NORTON ROSE FULBRIGHT

International Comparative Legal Guides

Practical cross-border insights into digital health law

Digital Health 2025

Sixth Edition

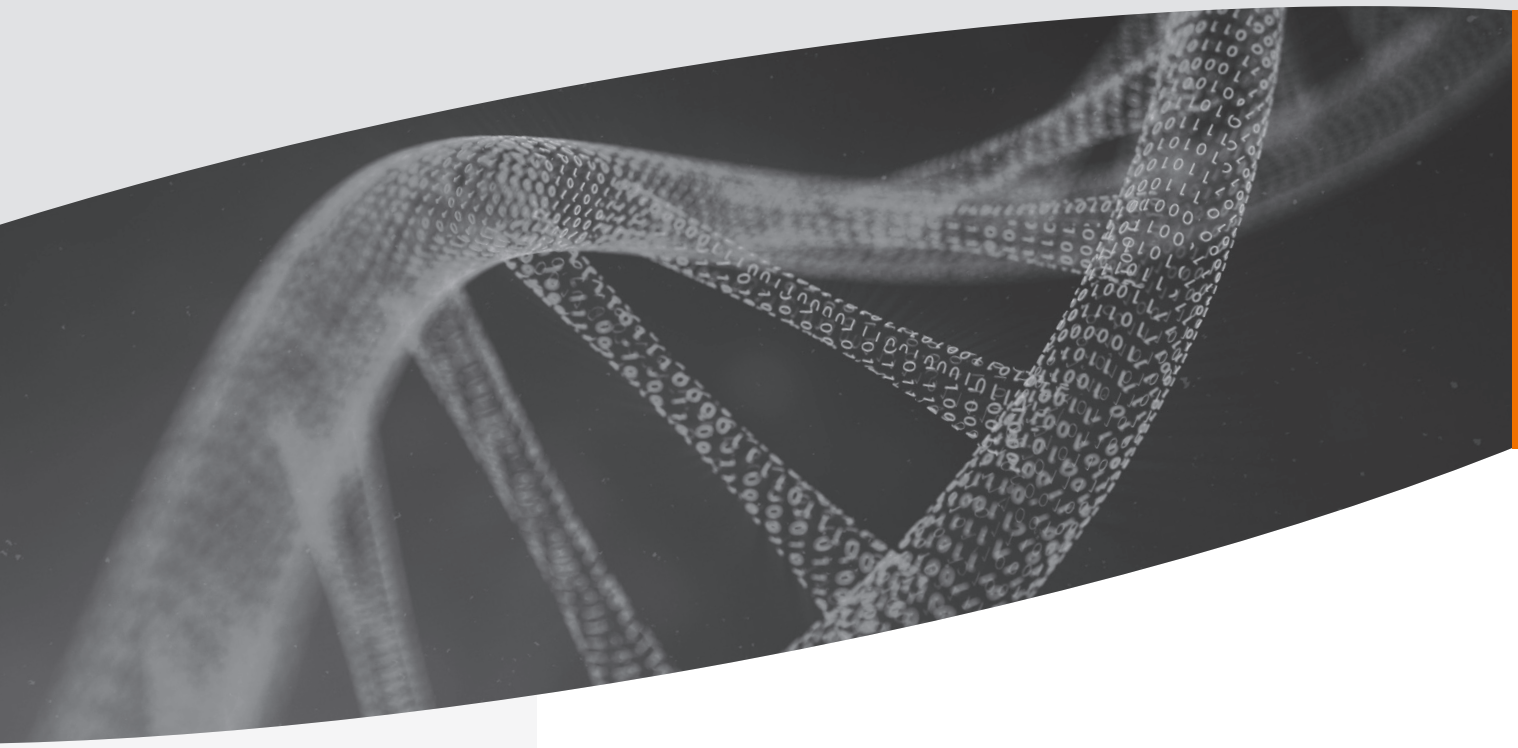
Contributing Editor

Roger Kuan

US Head of Digital Health and Precision Medicine Practice

Norton Rose Fulbright

iclg International Comparative Legal Guides



ISBN 978-1-83918-402-4
ISSN 2633-7533

Published by
glg Global Legal Group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
customer.service@glgroup.co.uk
www.iclg.com

Publisher
James Strode

Production Editor
Maya Tyrrell

Head of Production
Suzie Levy

Creative Lead
Wilfried Tshikana-Ekutshu

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

iclg International Comparative Legal Guides

Digital Health 2025

Sixth Edition

Contributing Editor:

Roger Kuan
Norton Rose Fulbright

Introductory Chapter

1 Introduction
Roger Kuan, Norton Rose Fulbright
David Wallace, Johnson & Johnson

Expert Analysis Chapters

7 Protecting Biotech's Data Frontier: A Guide to IP and Asset Strategy in the Age of AI
Jason Novak, Dr. Milad Alucozai & Q. Andy Guo, Norton Rose Fulbright

13 Artificial Intelligence Tools in Health Services – An Overview of Current and Evolving US Federal and State Health Regulatory Structures
Alexis Gilroy, Rebecca Martin, Jessica Tierney & Claire Castles, Jones Day

20 Data Protection and Cybersecurity in Digital Health
Stephen K. Phillips & Alicia Macklin, Hooper, Lundy & Bookman, P.C.

Q&A Chapters

28 **Argentina**
Diego Fernández & Martín J. Mosteirin, Marval O'Farrell Mairal

41 **Australia**
Bernard O'Shea & Rohan Sridhar, Norton Rose Fulbright

56 **Belarus**
Marina Golovnitskaya & Yauheni Budchanka, Alba LLP

68 **Belgium**
Olivier Van Obberghen, Pieter Wyckmans, Amber Cockx & Chaline Sempels, Quinz

83 **Canada**
Vanessa Grant, Véronique Barry, Manpreet Singh & Sarah Pennington, Norton Rose Fulbright

96 **France**
Catherine Mateu & Pierre Camadini, Armengaud Guerlain

105 **Germany**
Jana Grieb, Steffen Woitz, Dr. Claus Färber & Dr. Christian Lebrecht, McDermott Will & Emery Rechtsanwälte Steuerberater LLP

117 **Greece**
Evangelos Katsikis, Alexandra Asourmatzian & Filippos-Athanasios Misoulis, KKLegal

126 **India**
Manisha Singh & Dr. Pankaj Musyuni, LexOrbis

135 **Indonesia**
Marshall Situmorang, Andhitta Audria Putri, Mia Sari & Albert Barnabas, Nusantara Legal Partnership

144 **Israel**
Adv. Eran Bareket & Adv. Alexandra Cohen, Gilat, Bareket & Co., Reinhold Cohn Group

156 **Italy**
Sonia Selletti & Claudia Pasturenzi, Astolfi e Associati, Studio Legale

169 **Japan**
Masanori Tosu & Kenji Tosaki, Nagashima Ohno & Tsunematsu

178 **Korea**
Jin Hwan Chung, Eileen Jaiyoung Shin & Sungil Bang, Lee & Ko

187 **Mexico**
Carla Calderón, Marina Hurtado Cruz, Daniel Villanueva & Carlos Vela Treviño, Baker McKenzie

200 **Poland**
Michał Czarnuch, Dr. Paweł Kaźmierczyk & Julia Nowosielska-Łaskawiec, Rymarz Zdort Maruta

213 **Singapore**
Gloria Goh, Koh En Ying, Tham Hsu Hsien & Alexander Yap, Allen & Gledhill LLP

223 **Switzerland**
Dr. Tobias Meili, Dr. Carlo Conti, Dr. Martina Braun & André S. Berne, Wenger Plattner

234 **Taiwan**
Tsung-Yuan Shen, Rachel Chen & Nita Ye, Lee and Li, Attorneys-at-Law

243 **United Kingdom**
Pieter Erasmus, Emma Drake, Tristan Sherliker & Mario Subramaniam, Bird & Bird

256 **USA**
Roger Kuan, Jason Novak & Apurv Gaurav, Norton Rose Fulbright

Publisher's Note

Dear Reader,

The digital health market is experiencing explosive global growth and showing no signs of slowing down, with projected growth to result in an industry worth $600 billion by 2030. The industry is wide ranging, using digital tools and platforms to improve healthcare outcomes, whether by providing personalised patient care in person, expanding access to healthcare through mobile apps, or using neural networks to diagnose diseases. Notable areas of growth include remote monitoring, personalised healthcare services, and the use of data analytics for informed decision-making.

The growth is not limited to a specific region – digital health is becoming a global phenomenon. North America, particularly the U.S., leads in market share due to its advanced healthcare infrastructure, high adoption of technology, and supportive regulatory environment. Europe, particularly the U.K. and Germany, is also a significant player, with substantial investments in telemedicine and digital health startups. In Asia-Pacific, countries like Singapore and India are rapidly expanding their digital health initiatives, driven by large populations and increasing demand for affordable healthcare solutions.

Hot legal topics in this space revolve around data privacy and security, with regulations like HIPAA and GDPR setting stringent standards. Intellectual property protection, particularly patents related to health tech innovations, is another significant concern. Furthermore, the rise of AI in healthcare introduces legal challenges regarding liability, accountability, and medical malpractice. These complexities highlight the need for evolving global regulatory frameworks that balance innovation with patient safety.

All of the topics and regions mentioned above are covered in this year's edition of *International Comparative Legal Guide to Digital Health*. My thanks to our authors for their insights, which have resulted in the ability to navigate key topics within the industry for the year ahead.

James Strode
Publisher
Global Legal Group


iclg

Introduction


Roger Kuan


David Wallace

Norton Rose Fulbright
Johnson & Johnson

What is Digital Health?

Over the past 10 years, the rapid integration of digital technologies into healthcare has revolutionised the way medical services are delivered – even before the COVID-19 pandemic accelerated this shift. Digital health is transforming traditional, provider-centric healthcare – characterised by standardised "one size fits all" treatments and siloed information – into a patient-centric model that prioritises personalised care, data accessibility, and seamless communication.

This new approach leverages advanced information technologies (IT) to enhance coordination among patients, healthcare providers, insurers, researchers, and health data repositories. As a result, healthcare is becoming increasingly data-driven, enabling tailored treatments and more efficient delivery of therapeutics to patients.

According to a January 2025 report by *Fortune Business Insights*, the global digital health market is projected to grow at a compound annual growth rate of approximately 18.9%, reaching an estimated value of US$1.5 trillion by 2032.[1]

Digital Health Ecosystem

There are five primary constituents that make up the Digital Health Ecosystem.

Life Sciences Companies – are the companies that develop and make products such as therapeutics, diagnostics, medical devices and the like that are used to help treat a patient's health or wellness condition.

Pharmacies – are the supply chain, people and companies that sell the products that life sciences companies develop to end-users such as patients and providers.

Providers – are the doctors, clinics, hospitals and healthcare systems that provide healthcare services to patients by leveraging off the products produced by the life sciences companies.

Payors – are the group of entities (e.g., private insurance companies, government-sponsored insurance programmes, national healthcare systems, etc.) that pay for the products and healthcare services provided to patients.

Patients – are the people who all the collective entities (Life Sciences Companies, Pharmacies, Payors and Providers) try to serve as part of the Digital Health Ecosystem.

The Digital Health Ecosystem constituents sometimes struggle to transact in a seamless manner with each other; and Digital Health Solutions provide the key to building effective channels and improving efficiencies between them.

Traditional Healthcare Paradigm

"One size fits all" approach

Disease diagnosis and treatment have traditionally been based on efficacy validation models that neatly packaged patient populations into distinct buckets (often focused just on the disease state in question) that rarely allowed for differentiation between the individual constituents. This "one size fits all" approach did not enable true personalisation of patient diagnosis and treatment based on their innate individual characteristics (e.g., genome, epigenome, proteome, microbiome, metabolome, morphology, etc.) and exposome (e.g., lifestyle, environmental exposure, socioeconomic status, etc.).

One main reason why the healthcare industry adhered to the "one size fits all" paradigm for so long was the lack of capable and affordable tools and methodologies that could accurately monitor and determine all aspects of an individual's innate characteristics and then utilise that data to precisely tailor treatments or infer clinical outcomes for an individual. Because of recent digital health advances and availability of large volumes of relevant data, many of those technical hurdles have been overcome. The cost of generating and processing data that is indicative of an individuals' uniqueness (e.g., whole genome sequencing, proteomic analysis, high resolution imaging, etc.) has recently come down to such an extent that it is readily accessible to the masses and recent advances in artificial intelligence (AI) (more specifically machine learning (ML)) techniques have powered the analysis of large and complex datasets generated by these tools to make clinically relevant insights that can help guide the diagnosis and treatment of patients based on their individual uniqueness.

Provider-centric model

Until recently, healthcare services were delivered to patients primarily through a provider-centric model whereby patients seeking medical attention were required to go to a medical practitioner, clinic or hospital to be diagnosed and/or treated for their condition. This approach was largely driven by the healthcare industry's slow adoption of new IT (e.g., Internet of Things (IoT), wireless video communication, text messaging, electronic medical record systems, etc.) and the lack of digital health tools (e.g., wireless diagnostic medical devices, wearables, mobile apps, etc.) that allow for remote patient diagnosis and monitoring.

In the last few years, the healthcare industry's adoption of new IT technologies and other digital health tools has accelerated significantly, ushering in a new patient-centric paradigm (e.g., telemedicine, virtual healthcare, etc.) whereby healthcare services are delivered remotely, almost on-demand, to patients regardless of where they are. When the COVID-19 pandemic took hold of the world, a measure of urgency was also added as the provider-centric approach to healthcare now included a component of danger that patients would be exposed to COVID-19 if they visited their providers in person.

Siloing of health information and data

Data access and analytics are the fuel that drives digital health. Patient health information has traditionally been either stored as physical files at a provider site (e.g., doctor's office, clinic, hospital, etc.) or in electronic health record (EHR) management systems that are incompatible with one another. This resulted in health data being siloed where they were stored, which hindered the seamless communication and sharing of health data. This also prevented the use and aggregation of such data to power analytics tools (many of which are driven by AI/ML) that are used in a variety of different applications, including drug discovery, diagnostics, digital therapeutics, pre-surgical planning and clinical decision support.

Fragmentation of constituents

There is substantial fragmentation between the major constituents of the Digital Health Ecosystem, which makes it difficult for them to access, navigate or transact with each other. The inefficiencies caused by this fragmentation add unnecessary cost and delay to the delivery of care to patients. Further, it makes it difficult for patients to access the full range of products and services that are available to treat their health or wellness condition.

New Digital Technologies

A host of different digital technologies are helping to provide the infrastructure and know-how to drive the digital health revolution in healthcare.

Wireless connectivity and Internet of Medical Things (IoMT)

Wireless/mobile devices (e.g., mobile phones, wearables, medical devices, mobile applications, etc.) allow patients to access their healthcare providers and resources from anywhere around the world with wireless or Wi-Fi data connectivity. In turn, this also allows their healthcare providers to monitor their current health status and condition. This amalgamation of devices can all be connected to enterprise healthcare information systems using networking technologies to form an IoMT that allows for uniform transfer of medical data over a secure network.

Big Data analytics/storage

The voluminous quantity of medical data captured and transmitted through an IoMT is then stored and analysed using Big Data storage and analytics systems that manage, curate and process the data to generate predictive insights and/or visualise the data to aid analysts in quickly interpreting the data. A 2017 white paper from Stanford University School of Medicine estimates that 153 exabytes of healthcare data was generated in 2013, and that was projected to grow to 2,314 exabytes by the year 2020.[2] Analytics can be performed on the data using traditional statistical data analysis tools or more advanced AI/ML methodologies.

Enabling New Digital Health Solutions

The adoption of digital technologies in healthcare has given rise to a number of different categories of transformative digital health solutions.

Remote patient monitoring and delivery of care

Perhaps the most visible and impactful of the categories of digital health solutions are telemedicine/telehealth and virtual care. 2020 was a banner year for telehealth as the COVID-19 pandemic led to an exponential leap in the number of patient consults using telehealth platforms due to social-distancing measures and to minimise exposure.

A 2020 report by Amwell found that before COVID-19, fewer than 1% of all physician visits in the US were conducted via telehealth; in just over a month after the start of the pandemic, analysis of health claims data found that this number had increased to over 50%. Of those patients who used telehealth platforms, over 90% said that they planned to continue using those platforms post-COVID-19.[3] The digital technologies that enable telehealth are wireless/mobile devices and the applications that run on them.

Moving beyond virtual doctor's visits through telehealth platforms is the concept of virtual care, whereby healthcare providers remotely deliver the full range of health services to patients by remotely monitoring patient condition and vitals (remote patient monitoring) using IoMT-connected wearables and wireless medical devices; and communicate with patients to provide treatment advice and answer their questions using wireless/mobile devices that enable live and secure video, audio and instant messaging communication. This next step in the evolution of telehealth will truly change the traditional provider-centric model of healthcare delivery to patients to a patient-centric model where the wide range of healthcare services can be delivered virtually on-demand and remotely wherever the patient is located.

Big Data analytics and AI/ML-powered healthcare solutions

- **Personalised/precision medicine**
  Personalised/precision medicine is another digital health solution that has recently gained traction. These are healthcare models that are powered by Big Data analytics and/or AI/ML to ensure that a patient's individual uniqueness (e.g., genome, microbiome, exposome, lifestyle, etc.) factors into prevention and the treatment (e.g., therapeutics, surgical procedures, etc.) of a disease condition that the patient is suffering from. An example of this would be companion diagnostic tests that are used to predict a patient's response to therapeutics based on whether they exhibit one or more biomarkers. Large quantities of patient records, including measured data of one or more patient biomarkers, the therapeutic(s) the patient is taking and the patient's clinical

outcome, can be analysed using Big Data statistical software tools to determine the biomarker(s) associated with a particular clinical outcome when the patient is treated with a particular therapeutic; or be used to train AI/ML algorithms that can identify biomarker(s) of relevance and infer patient clinical outcomes when treated with a particular therapeutic.

- **AI/ML-enabled diagnostics**
  The application of advanced AI/ML algorithms and techniques to process healthcare data enables critical clinical insights that link previously unrelated data inputs (e.g., imaging features, genomic/proteomic/metabolomic/microbiome biomarkers, phenotypes, disease states, etc.) to disease conditions and progression. This has resulted in diagnostic tests that have a high degree of predictive accuracy for some previously difficult-to-diagnose health conditions such as dementia, depression, Alzheimer's, and also enabled more non-invasive methods to diagnose and monitor disease conditions (i.e., cancer) that previously required surgical biopsies or other more invasive techniques.
- **Intelligent drug design and discovery**
  The same data that is used to train AI/ML algorithms for personalised/precision medicine purposes can also be re-purposed to train algorithms that can be used for intelligent drug design and clinical cohort selection applications that aid in the discovery and the clinical study of new or novel therapeutics and re-purposing of existing therapeutics.
  For example, an AI/ML algorithm trained to predict biological target response and toxicity can be used to design novel (i.e., non-naturally occurring) chemical structures that have strong binding characteristics to a biological target with correspondingly low chemical and/or systemic toxicity. This ability to design a therapeutic compound "backwards" from looking at desired attributes (e.g., binding strength, toxicity, etc.) and then custom designing a therapeutic compound with those attributes, instead of traditional drug discovery methods that screen millions of compounds for the desired attributes, is potentially game-changing. Not only does it hold the promise to shorten the initial drug target discovery process as it moves away from looking for the proverbial "needle in a haystack" to a "lock and key" approach, but it will likely lead to drugs that have greater efficacy and fewer side effects for larger groups of patients.
  Those novel chemical compounds can then be administered to clinical cohorts selected using AI/ML algorithms trained to choose the most suitable patients to enrol for clinical trials used to study the efficacy and toxicity of the compounds. Currently, it takes an average 10–15 years and US$1.5–2 billion to bring a new drug to market with approximately half of the time and investment consumed during the clinical trial phases of the drug development cycle. One of the main stumbling blocks in the drug development pipeline is the high failure rate of clinical trials. Less than one third of all Phase II compounds advance to Phase III. More than one third of all Phase III compounds fail to advance to approval. One of the primary factors causing a clinical trial to fail is clinical cohort selection that fails to enrol the most suitable patients to a clinical trial.[4] Minimising errors in clinical cohort selection can potentially shorten the clinical trial phase and reduce the risk of clinical trial failures that are not attributable to the drug being studied.

Digital hospital

Traditional hospital workflows can be highly inefficient because of disorganisation in patient treatment workflows and difficulties that clinicians have in readily accessing or utilising patient medical information. Through the use of digital medical information management tools, much of this inefficiency can be eliminated by ensuring less workflow downtime and gaps in the way that a patient is diagnosed and treated once he/she is admitted to a hospital and allowing patient medical information to be accessed anywhere within the hospital through a multitude of different means (e.g., workstation terminals, mobile devices, etc.) and from information stored externally from the hospital.

EHR aggregation platforms

Large volumes of good quality patient EHR data is the fuel that drives many Digital Health Solutions. The old adage of "garbage in, garbage out" applies particularly well to ML technologies. Flawed or nonsense input data that is fed to even the most sophisticated ML algorithm will invariably produce nonsense outputs or predictions. The integration of cloud-based EHR databases with advanced data extraction tools (e.g., natural language processing, automated annotations, etc.) has enabled companies to aggregate large volumes of good quality EHR data from fragmented (i.e., unaffiliated) clinical sources (e.g., sole practitioners, clinics, hospitals, etc.) distributed throughout the US and the rest of the world.

Digital Health Legal Issues

There are many important legal issues that apply to digital health. These issues can be broadly divided into two categories: intellectual property rights (IPRs); and regulatory compliance.

IPRs

With respect to IPRs, there are registrable IPRs (e.g., patents, copyrights, etc.) and unregistered IPRs (e.g., data rights, trade secrets, know-how, etc.).

Patents and copyrights

With respect to digital health and patents, the most burning issue is subject-matter patentability (or what qualifies as patentable). A series of US Supreme Court cases in the past 10 years have cast a shadow over the patentability of software (see *Alice Corporation Pty. Ltd. v. CLS Bank International*) and diagnostic methods (see *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*[5] and *Association for Molecular Pathology v. Myriad Genetics, Inc.*).[6] Successfully navigating these patentability hurdles is often a critical part of protecting the substantial investments that companies make in bringing their digital health solutions into the marketplace. Some recent US Supreme Court and Federal Circuit cases have begun to chip away at the patentability hurdles for diagnostics innovation (see *Hikma Pharmaceuticals USA Inc. v. Vanda Pharmaceuticals Inc.*[7] and *CardioNet, LLC v. InfoBionic, Inc.*)[8] and the current expectation is that future cases will continue to swing toward protection of this important area of innovation. In other jurisdictions around the world, computational software-driven innovations face similar hurdles toward patentability.

Copyrights can be used to protect software, including code for learning platforms such as various machine and deep-learning models. Copyrights can also be used to protect databases and some types of data content that which is itself original (e.g., structured compilations of genomic sequencing data, structured compilations of images, audiovisual recordings, detailed diagrams, etc.), but cannot protect factual data (e.g., raw genomic sequencing data, metabolite data, proteomics data, etc.). However, there may be other legal mechanisms that can be used to protect factual data, such as contract law and trade secret protection.

Trade secrets

Because of the current limitations of patent law, trade secret protection plays an outsized role in protecting digital health innovation relative to other industries. However, trade secret law has inherent limitations that make it less protective of innovation than patents. For example, trade secret law does not protect against third parties independently developing identical solutions (i.e., digital health innovations) and it requires that the trade secret owner marks their trade secrets and demonstrates that they are taking active measures to ensure that their trade secrets are not misappropriated.

Data rights

Digital health solutions tend to both generate and utilise large quantities of health data; therefore, data rights are a vital component of digital health IPRs that need to be protected. This is particularly true for digital health solutions that are powered by AI/ML algorithms as the accuracy of their predictions are largely determined by their training using large quantities of quality training data.

As discussed above, raw factual data is generally not protectable under copyright law, so the primary means used to guard data rights is currently with contract and trade secret laws. As the value of health data rights increases, the expectation is that the body of law dealing with data rights protection will also evolve to more adequately safeguard the rights of data owners.

Regulatory Legal Issues

Moving beyond IPRs, compliance with state and federal regulations is also essential for digital health companies seeking to successfully develop, market or implement digital health solutions in the US.

Data privacy

Continued access to medical data relies on patient trust and the laws and regulations that underpin that trust. As data gathering and access are critical components of most digital health solutions, it is vital that digital health companies adopt data privacy policies and infrastructure that are compliant with the data privacy laws and regulations of the jurisdiction(s) in which they operate.

In the US, the most pertinent data privacy laws are the Health Insurance Portability and Accountability Act (HIPAA), California Genetic Information Privacy Act (GIPA), California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (CDPA). The jurisdictional boundaries of the HIPAA, GIPA, CCPA and CDPA are carved out based on both the entity gathering the data (HIPAA-Covered Entities and their Business Associates) and the legal residence of the individual whose data is being gathered. That is, the HIPAA only applies to a statutorily defined group of Covered Entities such as health plans (e.g., health insurance companies, Medicare, Medicaid, etc.), healthcare clearinghouses (e.g., billing service, community health information systems, etc.), and healthcare providers (e.g., physicians, clinics, hospitals, pharmacies, etc.) that are considered traditional healthcare data custodians. Importantly, this leaves a coverage gap for non-traditional healthcare data custodians such as the technology companies (e.g., Amazon, Apple, Facebook, Google, etc.) that have recently entered the healthcare marketplace through their IoT and mobile app product offerings that can diagnose and treat healthcare-related issues. The first state to attempt to fill the HIPAA coverage gap was California when it enacted the CCPA in 2018. The CCPA provides privacy rights and consumer protection for data obtained from residents of California irrespective of the type of business. The California GIPA came into effect in 2022 and it places data collection, use, security and other disclosure requirements on direct-to-consumer genetic testing companies and provides their customers with access and deletion rights. The Virginia CDPA came into effect in 2023 and is the most recent state-level data privacy law to come into effect. It lays out clear regulations for companies that conduct business in Virginia regarding how they can control and process data. It also gives consumers the right to access, delete and correct their data, as well as opt-out of personal data processing for advertising purposes.

Generally, the HIPAA, GIPA, CCPA and CDPA regulate how businesses collect, handle and protect an individual's personal information (PI) to ensure their privacy and give them control over the sharing (informed consent) of their PI with third parties.

US Food and Drug Administration (FDA) regulatory

Another set of regulations that digital health companies must consider are those that regulate the safety and efficacy of digital health solutions. The Federal Food, Drug and Cosmetic Act (FFDCA) and related laws are federal statutes that regulate food, drugs and medical devices. The FFDCA is enforced by the FDA which is a federal agency under the US Department of Health and Human Services.

Depending on whether the digital health solution is a device, system or software, the FDA may enforce a number of different regulations and programmes, including: 510(k) certification; Premarket Approval (PMA); Software as a Medical Device (SaMD); Digital Health Software Pre-certification Program (Pre-Cert Program); and Laboratory Developed Test regulated under the Clinical Laboratory Improvement Amendments programme. One technology area of focus for the FDA recently is AI/ML-powered digital health software, which is dynamic by design and thus poses particular challenges for the FDA as the current regulatory regime is based on software being static by design. The FDA recently launched a Digital Health Center of Excellence to further the advancement of digital health solutions and address the unique regulatory issues they pose.[9]

State-specific practice of medicine laws (telehealth and virtual health)

For telehealth and virtual health companies that provide physician consultations across state lines, the Interstate

Medical Licensure Compact Commission regulates the licensure of physicians to practice telemedicine in member states.

The Interstate Medical Licensure Compact (IMLC) speeds up the licensure process for physicians practising telemedicine as it eliminates the need for them to individually apply for licences in each state they intend to practise in by allowing them to obtain an IMLC licence that is valid in all states that have joined the compact. The following states have joined the IMLC: Alabama; Arizona; Colorado; Idaho; Illinois; Iowa; Kansas; Maine; Maryland; Michigan; Minnesota; Mississippi; Montana; Nebraska; Nevada; New Hampshire; Pennsylvania; South Dakota; Tennessee; Utah; Vermont; Washington; West Virginia; Wisconsin; and Wyoming; as well as the District of Columbia, and Guam.[10]

The Stark Law and Anti-Kickback Statutes (AKSs)

Telehealth and virtual health providers who enter into business arrangements with third parties that incentivise care coordination and patient engagement are also subject to federal Stark Law and AKSs.

The Stark Law (or physician self-referral law) prohibits referrals by a physician to another provider if the physician or his/her immediate family has a financial relationship with the provider. The AKSs, meanwhile, bar the exchange of remuneration (monetary or in kind) for referrals that are payable by a federal healthcare programme like Medicare.

These laws provide another necessary consideration for telehealth companies as they can hinder opportunities for large health systems and companies to work together and to help smaller systems and hospitals develop their own platforms or take part in a larger telemedicine network.[11]

State and federal medical reimbursement laws and regulations

2020 has been a banner year for telehealth. Even before the COVID-19 pandemic, the remote care delivery model had been gaining traction among patients, particularly those who have grown up with technology.

Currently, all 50 states and the District of Columbia now provide some level of reimbursement coverage for telehealth services for their Medicaid members. At the federal level, the Mental Health Telemedicine Expansion Act was passed as part of the Omnibus Appropriations and Coronavirus Relief Package and the CONNECT for Health Act of 2019 and has been introduced but not passed.

Conclusions

The digital health sector experienced explosive growth even before the COVID-19 pandemic accelerated its adoption by mainstream payors, providers and patients. With the continued rapid pace of change in digital health, the expectation is that the delivery of healthcare will continue to transform. Within this transformation there will be some common themes.

The ability to gather data, generate clinical insights and transform those insights into actionable clinical solution(s) will form the foundation of value creation within digital health. In this paradigm, data access becomes the new "oil rush" as data will fuel the analytics engines behind many future digital health solutions. As a result, traditional technology players such as Amazon, Apple, Facebook and Google, may create substantial competition for traditional healthcare providers. It remains to be seen whether those advantages will translate to success in the digital health marketplace.

Clinical adoption of digital health solutions will continue to be a challenge as there are significant clinician concerns about how to safely integrate these solutions into their day-to-day practice. Moreover, digital health companies must navigate the myriad of state and federal regulations/laws relating to data privacy, FDA regulatory, practice of medicine, and medical reimbursement in order for their solutions to even be accessible by clinicians in the first place.

Lastly, there are brewing geopolitical factors that may impact how well digital health companies succeed in the marketplace. Regional regulations on health data access and usage (e.g., General Data Protection Regulation, HIPAA, CCPA, etc.), reimbursement, and product approval are additional requirements to contend with for companies that are foreign to the jurisdiction. Also, many countries have begun to aggressively invest in the gathering of healthcare data (especially whole genome data) on a national level, which can potentially be leveraged to give domestic companies an edge over foreign ones. Examples of this are the UK Biobank Whole Genome Sequencing Project and Beijing Genome Institute (BGI) Million Chinese Genome Project. It is conceivable (and likely) that the UK and China will implement data-access policies that specifically benefit domestic digital health companies to give them a home-grown advantage.

Endnotes

1 "Digital Health Market Size, Share and Trends | Growth Report [2032]" https://www.fortunebusinessinsights.com, January 27, 2025.

2 Stanford University School of Medicine (2017). "Harnessing the Power of Data in Health, Stanford Medicine 2017 Health Trends Report". Retrieved from: https://med.stanford.edu/content/dam/sm/sm-news/documents/StanfordMedicineHealthTrendsWhitePaper2017.pdf

3 Amwell (2020). "From Virtual Care to Hybrid Care: COVID-19 and the Future of Telehealth". Retrieved from: https://static.americanwell.com/app/uploads/2020/09/Amwell-2020-Physician-and-Consumer-Survey.pdf

4 Harrer, *et al.* "Artificial Intelligence for Clinical Trial Design." *Trends in Pharmaceutical Sciences* 40.8 (2019): 577–591.

5 https://supreme.justia.com/cases/federal/us/566/66

6 https://supreme.justia.com/cases/federal/us/569/576/#:~:text=Assoc.,Justia%20US%20Supreme%20Court%20Center

7 https://www.scotusblog.com/case-files/cases/hikma-pharmaceuticals-usa-inc-v-vanda-pharmaceuticals-inc

8 https://law.justia.com/cases/federal/appellate-courts/cafc/19-1149/19-1149-2020-04-17.html

9 https://www.fda.gov/news-events/press-announcements/fda-launches-digital-health-center-excellence

10 https://intouchhealth.com/half-of-the-country-has-joined-the-telemedicine-licensure-compact

11 mHealth Intelligence (2020). "Stark Law Changes Should Benefit Telehealth, Remote Patient Monitoring". Retrieved from: https://mhealthintelligence.com/news/stark-law-changes-should-benefit-telehealth-remote-patient-monitoring

Roger Kuan is a Partner at Norton Rose Fulbright LLP and US head of the Precision Medicine and Digital Health Practice Group, where he counsels companies that are uniquely positioned in the convergence of the life/medical sciences and technology industries on how to successfully navigate the complexities of the intellectual property (IP), data rights and regulatory challenges they encounter.

Roger has extensive experience in IP strategy and portfolio management (utility/design patents, trademarks, copyrights, and trade dress), data rights strategy, licensing and technology transactions, freedom-to-operate clearances, enforcement, monetisation, IP due diligence, and dispute resolution. His practice is focused in the life sciences sector (e.g., research tools, analytical instrumentation/software, digital therapeutics, medical devices, diagnostics, biomanufacturing equipment, etc.) with an emphasis in emerging technologies such as precision medicine (e.g., genomic sequencing platforms, AI/ML, computational genomics/bioinformatics, molecular diagnostics, companion diagnostics, etc.), digital health (e.g., mobile apps, clinical decision support, software, AI/ML imaging diagnostics, wearables, etc.) and 3D printing/bioprinting.

Norton Rose Fulbright
1 Embarcadero Center, Suite 1050
San Francisco, California 94111-3698
USA

Tel: +1 628 231 6800
Email: roger.kuan@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/roger-kuan-1b5b824

David Wallace is a member of the Johnson & Johnson Law Department and is the Assistant General Counsel (AGC) of Patents for the Health Technology Team. In his role as AGC, David is primarily responsible for day-to-day activities regarding the patent aspects of the health technology initiatives across the Johnson & Johnson Family of Companies.

Johnson & Johnson
510 Cottonwood Drive
Milpitas, California 95035
USA

Tel: +1 408 273 5101
Email: dwalla34@its.jnj.com
LinkedIn: www.linkedin.com/in/david-wallace-957b24

Protecting Biotech's Data Frontier: A Guide to IP and Asset Strategy in the Age of AI


Jason Novak


Dr. Milad Alucozai


Q. Andy Guo

Norton Rose Fulbright

The healthcare and biotech industry is on the brink of a data-driven revolution, with artificial intelligence (AI) poised to transform drug discovery, personalised medicine, and healthcare delivery. However, this revolution brings a new array of data ownership, privacy, and security challenges. The following addresses these critical questions, exploring how biotech companies can navigate this complex landscape while safeguarding their intellectual property, driving innovation, and fostering trust. This discussion will examine strategies for balancing open collaboration with strong IP protection, ensuring data privacy and security, developing explainable and reliable AI, navigating regulatory uncertainties, and managing the risks tied to AI-driven healthcare solutions. Ultimately, it will underscore the essential role of leadership in cultivating a data-driven culture that views data as a strategic asset and encourages employees to use it responsibly to advance the healthcare and biotech industry.

Data Ownership, Access, and Corresponding IP Strategy Considerations

Building a successful AI program in the healthcare sector depends on collaboration, as merging scientific, operational, and business expertise is crucial for achieving both innovation and capital efficiency. Each area of expertise plays a vital role, and their integration often forms the foundation for long-term success.

In the world of AI, it is no longer enough to have *a lot* of data. The real game-changer lies in having the *right* data – high-quality, relevant to the specific problem, and easily usable. Think of it like this: a massive warehouse filled with random objects is not nearly as valuable as a smaller, well-organised workshop stocked with the precise tools and materials needed for a specific project. Similarly, a massive dataset of generic information is far less valuable than a carefully curated dataset containing the accurate information required to train an AI model for a specific task.

This shift in focus from quantity to quality has significant implications for businesses. Algorithms are rapidly becoming commodities, with open-source models and readily available tools levelling the playing field. Competitive advantages now hinge on exclusive access to high-quality, relevant data and the legal right to use it. Protecting this valuable data, often as trade secrets, is becoming more crucial than relying on patents to safeguard algorithms. Data-related agreements are the bedrock of any AI-driven company, and any weakness in these agreements or overall data governance can have devastating consequences. For instance, AI-based companies and programs must secure comprehensive data usage rights, covering both research and commercial applications, before even beginning to train their AI models. Failure to do so could leave them vulnerable to losing control over valuable insights they generate, handing leverage to data rights holders. Industry stakeholders recognise this crucial dynamic and expect developers to proactively address these challenges to inspire confidence in the long-term viability of an AI program.

A weak or unclear data strategy poses a significant red flag for stakeholders. AI-based companies and programs with a well-defined plan and robust data hygiene – encompassing data acquisition, storage, management, and usage – can outshine their competitors. This discipline not only minimises risks but also shows the operational maturity that stakeholders look for in a high-potential product opportunity.

Moreover, reconciling a data strategy with a sound IP strategy can become difficult for companies. As healthcare and biotech converge with AI, creators of data-driven business models often struggle to balance IP protection and data protection. However, these challenges can be alleviated through prioritisation and planning.

Patents and trade secrets do not safeguard the data underlying inventions; instead, they protect the insights derived from analysing that data. For instance, patents and trade secrets can be combined to cover methodologies used to generate clinical insights, such as processes for identifying new drug targets or biomarkers. Therefore, data analysis and insight generation are essential prerequisites for obtaining patent protection.

The healthcare and biotech industries must adopt a mindset of "asking for permission, not forgiveness" regarding data ownership and access. Attempting to rectify mistakes after they occur can be costly and should be avoided at all costs. Thus, the top priority for a data-driven business model is ensuring ownership or control of data assets to a degree that aligns with both the company's planned and actual uses. This should be established immediately through appropriate data use or collaboration agreements. Once data has been analysed and downstream insights generated (e.g., innovations in diagnostics), patents and trade secrets can be pursued to protect those insights.

A priority for this mindset includes defining the specific purposes for which the company intends to utilise its data. This involves articulating the scope of desired data rights before entering negotiations for data-sharing, collaboration, or co-development agreements. Failing to define these rights upfront can lead to complications later on. If broader rights are necessary after agreements are in place, renegotiating with the data holder may be unpleasant or even impossible, as the data holder would possess all the leverage. Although planning may

require time and financial investments, it simplifies execution and reduces expenses in the long run.

The consequences of seeking forgiveness can be devastating. For example, a company that lacks proper rights to just 2% of its training data after launching an AI-driven product might encounter significant setbacks. It could be compelled to remove the product from the market, disgorge that 2% of training data, retrain the AI, and/or resubmit it for regulatory approval, incurring delays and expenses. Thus, from a due diligence perspective, all stakeholders and developers must understand the importance of a robust data plan. This alignment ensures clear expectations and fosters continuous improvement over time.

A robust data plan also involves implementing a trade secret programme. This consists of a series of practical steps. First, companies must identify and define confidential information, including data, algorithms, processes, and know-how. This requires a thorough inventory of critical assets and precise documentation of their confidentiality. Next, access controls should be established to limit access to sensitive information on a need-to-know basis. This can involve physical security measures, such as restricted areas and secure data storage, and digital security measures, such as password protection, encryption, and access logs. Employee training is crucial to ensure everyone understands the importance of protecting trade secrets and their role in maintaining confidentiality. This includes educating employees on company policies, procedures for handling confidential information, and potential consequences of breaches, as well as implementing legally binding contractual obligations with employees, contractors, and partners. Finally, documenting all trade secret policies and procedures is essential for maintaining a consistent and enforceable system. This documentation should be regularly reviewed and updated to reflect changes in the company's operations and the evolving legal landscape.

By implementing a comprehensive trade secret system, healthcare and biotech companies can protect their valuable intellectual property and maintain their competitive advantage in the rapidly evolving landscape of AI-driven innovation.

Lastly, many healthcare innovations stem from research institutes and universities. Treating each AI-driven research project as a commercial venture from the outset is a valuable approach. This mindset encourages entrepreneurship-minded researchers to integrate planning and safeguards early, such as executing proper data strategies and securing necessary agreements. Preparing for commercialisation from the beginning can pave the way to market success. After all, it is always better to be prepared than to scramble later.

Data Privacy and Security

Breaches or non-compliant use of patient data and other sensitive information can severely damage a company's reputation and that of its stakeholders. More critically, such incidents have profound consequences for end-users, eroding public trust and potentially leading to significant legal liabilities.

Unfortunately, the healthcare and biotech industry is a prime target for cybercriminals due to the vast amount of valuable personal information it holds. Recent data breach incidents have heightened concerns among healthcare companies and organisations about collaborating with startups and third-party vendors due to perceived breach risks.

For any AI-centred product, demonstrating robust data security measures is essential to inspiring confidence in potential partners. Measures such as regular audits, maintaining detailed security records and data trails, and employing state-of-the-art encryption solutions can set a program apart. These practices demonstrate a commitment to data privacy and security, highlighting the program developer as a responsible partner who prioritises security over growth at all costs.

AI companies and programs must be prepared to answer critical questions about their AI-driven products, such as: Where will the product operate – on-premises or in the cloud? If in the cloud, is it a hybrid cloud or multi-cloud architecture? How is data stored? How will data governance evolve as the company scales? Providing clear and thoughtful answers to these questions boosts credibility with experienced stakeholders and potential partners and fosters a cultural shift in the industry driven by prioritising security and responsibility.

Awareness of protecting data, preventing breaches, and complying with privacy regulations – such as HIPAA and state laws in the U.S. that exceed HIPAA's requirements – has grown significantly. The real test, however, is whether AI companies and AI programs can translate this awareness into a robust, actionable data protection plan and execute it effectively.

As explicitly applied to startups, a small company with the same data protection infrastructure and commitment as a prominent organisation gains a tremendous competitive edge. Startups can argue that large entities are primary targets for hackers, not small companies. By proposing that the startup handle sensitive data analysis and protect insights within its infrastructure, entrepreneurs can underscore how this approach is safer for the data and its derived insights. The consequences of security breaches – whether for a large entity or a small company – are severe, encompassing financial losses, resource drains, legal liabilities, and possibly product injunctions. Startups can leverage this reality to present a compelling value proposition: they help large entities mitigate these risks.

Patients' growing concerns about data rights also drive demand for privacy-first solutions. AI companies and AI programs that prioritise patient privacy can unlock tremendous opportunities. One effective way to achieve this is by focusing on data minimisation – collecting only the data necessary for specific purposes. Unlike data hoarding, which collects excessive and unnecessary data and increases breach risks, data minimisation reduces risk and liability. AI companies and AI programs that adopt this approach and communicate their focused data needs are more likely to gain the trust of data holders and secure collaborations.

AI Explainability and Trust

Trust in AI-powered diagnostic and treatment tools can often be centred around the "black box" nature of AI algorithms. However, the "black box" nature should be considered acceptable because some algorithms are inherently complex and challenging to interpret. However, AI-driven biotech companies must still strive to understand their AI models and make them as explainable as possible.

Explainability is essential for building trust. The best developers articulate how their AI works in simple, straightforward language. Investors, in particular, value this transparency. They are also keen to understand AI's limitations, as every solution has biases, error rates, and scenarios where human oversight or intervention is necessary – or where AI may not apply.

The willingness of leaders or their technical teams to openly discuss these limitations demonstrates maturity and realism that can be pivotal in gaining an investor's trust. Transparency about the strengths and weaknesses of an AI solution positions a company as credible, trustworthy, and prepared to navigate the challenges of AI implementation effectively.

The tech industry often accepts AI's "black box" nature, which refers to the opacity of its internal workings. This is because the focus is usually on AI's functionality rather than a deep understanding of how it works. This lack of emphasis on transparency aligns with the open-source culture prevalent in the tech sector, which prioritises the sharing and modifying of code, even if the code's inner workings are not fully understood.

However, the healthcare and biotech industry demands a different level of transparency. Disclosure requirements for adoption and investment in healthcare are significantly higher than in tech, not to mention the additional regulatory approvals not present in tech. Healthcare providers and payers want to understand how and why an AI solution works before committing to it. Despite this need for clarity, companies should not have to disclose the mathematical formulas behind their AI algorithms to gain adoption from payers, as this often goes beyond the knowledge base of decision-makers and is usually objectively less critical than understanding the inputs (data, prompts, variables) and outputs (scoring, decision matrix, insights, etc.) of the AI.

Companies should focus on explaining how these inputs are used in the AI model and how they generate actionable outputs. They can avoid disclosing proprietary details, such as parameter weighting (e.g., biomarker weighting) or neural network configurations, as these are not typically critical to decision-making.

A company with a unique AI algorithm should protect it as a trade secret rather than disclose it. This is partly because AI algorithms, based on mathematical formulas, are likely not patentable and, even if patentable, are often difficult to reverse engineer in competitor products. The biotech market usually overvalues the AI "black box", even though many algorithms are off-the-shelf solutions or may soon be.

Over time, the value of the AI "black box" will likely diminish, with the focus shifting to factors like unique data sets, novel combinations of variables under investigation, and the clinical insights derived from such data. Ultimately, the actual value lies not in the algorithm itself but in the uniqueness and quality of the data and insights.

A company can make a compelling argument that the specific details of its AI model – whether a static algorithm or a neural network – are less relevant than the clarity of what goes into the model, what comes out of it, and the soundness of the methodology.

Patent law for AI-enabled diagnostic inventions supports this approach to disclosure. For instance, a company investigating a unique combination of five biomarkers using a proprietary data set could obtain patent protection by describing the biomarkers, the distinctiveness of the data, the questions addressed, and the novel insights gained (e.g., a unique biomarker combination). There is no requirement to disclose the precise mathematical steps (e.g., the weighting of biomarkers) used by the AI model. This strategy ensures the company protects its proprietary technology while meeting legal and commercial needs for transparency.

Regulatory Uncertainty and Innovation

Food and Drug Administration (FDA) clearance or approval holds significant value in the healthcare and biotech industry. Companies developing AI-enabled products are strongly encouraged to immediately schedule meetings with the FDA. Collaborating with the FDA throughout product development fosters trust and ensures alignment with regulatory expectations. The current regulatory framework prioritises data over innovation; the FDA will not grant clearance merely because an AI model is novel.

Encouragingly, the FDA has indicated a growing willingness to engage with these AI-enabled product companies. This presents an opportunity for these companies to advocate for more adaptive and flexible regulations, including more explicit guidance on regulatory expectations, accelerated approval pathways tailored to address unmet needs, and additional measures that support innovation without compromising safety or efficacy.

It is worth noting that the current regulatory framework faces several challenges, including a shortage of personnel and expertise at regulatory agencies, a limited deep technical understanding of AI technologies, and the influence of industry groups with various and sometimes conflicting incentives.

Analysing improvements to the regulatory framework requires examining what the FDA guidance scrutinises *versus* what it has not emphasised. For instance, the FDA places significant focus on change control, requiring AI companies to outline detailed plans for how their AI systems will learn and when updates will be implemented. While these strict versioning requirements may work for technologies like smartphone operating systems, they are less suited to the dynamic nature of AI platforms.

Conversely, the current guidance lacks requirements for regulatory due diligence regarding the source of training data. This gap poses risks if a company improperly uses (intentional or not) part of its training data to develop an AI-driven product. In such cases, the company might struggle to rectify the issue retroactively and be forced to relinquish the improperly used data. This scenario could render the AI model unusable, leading to the de-marketing of the product and significant consequences for customers and stakeholders alike. The Federal Trade Commission has already employed penalties such as algorithm disgorgement, which can negatively affect these AI-enabled products and corresponding companies.

Some may argue that the regulatory agency should adopt a more rigorous "gatekeeping" approach upfront. By asking the right questions during the approval process, the agency could place more significant pressure on companies at the front end. Once approval is granted, the agency can trust its processes and the companies that have cleared the approval threshold. For post-approval updates and changes, a reporting structure could replace the need for repeated upfront reviews. This front-end-heavy strategy would better align with the business models of AI-driven companies while demonstrating greater trust from the regulatory agency in its processes and in the companies it approves.

To foster innovation while ensuring safety and efficacy, regulatory sandboxes and pilot programs are gaining traction as valuable tools for AI-driven healthcare solutions. These controlled environments allow companies to test their technologies in a real-world setting with a limited scope, providing helpful feedback and data to inform regulatory decision-making. By offering a safe space for experimentation and collaboration with regulatory agencies, sandboxes can accelerate the development and validation of AI solutions while mitigating potential risks. Furthermore, international cooperation is crucial in harmonising regulatory approaches to AI in healthcare. By sharing knowledge, best practices, and regulatory frameworks, countries can work together to establish globally applicable standards, reducing barriers to

innovation and promoting the safe and effective adoption of AI technologies across borders. This collaborative approach can foster a more consistent and predictable regulatory landscape, enabling companies to navigate the complexities of AI regulation more efficiently and bring their innovations to patients worldwide.

This presents an opportunity for these companies to advocate for more adaptive and flexible regulations, including more explicit guidance on regulatory expectations, accelerated approval pathways tailored to address unmet needs, and additional measures that support innovation without compromising safety or efficacy. Initiatives like the National Security Commission on Emerging Biotechnology further underscore the increasing importance of biotech in national security. With Senator Todd Young at the helm, the Commission is poised to play a crucial role in shaping policies that balance innovation with national security concerns. This highlights the growing need for biotech companies to engage with policymakers proactively and contribute to developing a regulatory environment that fosters progress and security. However, the dense and complex regulatory landscape can favour established players.

IP Protection for AI Innovations

First, data is now a critical asset, no longer a "back office" matter that company leaders can afford to overlook. Company leaders must be resourceful and capital efficient, planning and implementing robust patent and trade secret strategies at every growth stage.

A secure and well-executed data asset strategy significantly enhances a company's appeal to stakeholders and investors, increasing the likelihood of securing funding or advancing a program within a larger company. Additionally, it boosts the company's attractiveness as a partner for collaborations. These advantages, in turn, strengthen the company's overall position by providing it with more assets to build.

The key to standing out lies in having a clear strategy, a detailed plan, and a compelling narrative about how the company has implemented both. Leaders who can demonstrate that they have secured their data assets from day one – backed by a thoughtful approach and consistent execution – are far more likely to differentiate themselves from the competition.

These datasets are generally protected as trade secrets, not patents. Patents may protect how data is used to discover insights, including the processes and methodologies employed and the outputs derived from AI analysis – such as biomarkers, quantitative diagnostic tests, drug targets, and other clinical insights. Other elements, including the datasets, are better safeguarded as trade secrets.

Regarding the "black box" issue discussed above, patent filings should avoid including AI algorithms or architecture. Algorithms themselves are not patentable under patent law, as mathematical formulas cannot be patented. However, neural network architectures may be patentable. In the sporadic cases where the company must disclose its neural network architecture to gain adoption, patent protection may be considered. If disclosure is unnecessary, which should often be the case, the architecture can remain a trade secret. If disclosure is required, the company should patent it for protection. Further, detecting infringement may pose challenges for enforcing a neural network patent, as competitors are unlikely to reveal their proprietary architectures. As such, the "black box" nature can complicate the enforcement of such patents.

Companies should establish a trade secret framework before ingesting datasets or generating output data to implement trade secret protection effectively. This framework can be relatively simple but still requires a well-thought-out strategy, proper education, and alignment across the organisation. Companies should incorporate trade secret terms into their data-sharing agreements, addressing critical aspects such as how data is used, audited, stored, and ultimately destroyed or returned.

In practice, CEOs typically do not negotiate or execute data-sharing agreements. This responsibility usually falls to corporate development professionals or contract managers, who must thoroughly understand these principles as an extension of the company's IP strategy. As a cautionary note, the most significant risks to innovations and trade secrets stem from human errors, often due to a lack of education. If employees fail to grasp disclosure requirements – what can and cannot be disclosed – any IP program, whether focused on patents or trade secrets, may ultimately fail.

In conclusion, patents are straightforward because they involve deliberately disclosing known innovations. Trade secrets are also straightforward because they involve deliberate non-disclosure. The real challenge is ensuring that every organisation member understands and aligns with these principles. Even the most robust IP strategies can fall apart without this unified understanding.

Leadership and Culture

There was a time when an entrepreneur or product leader could succeed simply by being a visionary with innovative research to transform into a product. However, the landscape has evolved. Today, successful companies typically merge diverse talents, including data scientists, engineers, and wet lab scientists. This shift requires leadership to adopt a product-centric mindset. To do this effectively, they must become fluent in the language of data assets, allowing them to make informed strategic decisions from the beginning. The best leaders are creating a new playbook for navigating this complex environment.

AI-driven biotech companies are expanding rapidly, with speed, disruption, and scalability at the forefront of leadership's priorities. Yet, leadership must remember that they operate within the healthcare and biotech industries, not purely in the tech ones. In this space, prudence cannot be sacrificed for speed. Increasingly, value is less about the algorithms themselves and more about their applications and the deep domain expertise that drives them.

The first principle for company leaders is understanding that a data strategy must precede both IP and employment strategies. A well-defined data strategy lays the foundation for aligning and informing these other critical strategies.

First, when negotiating for data rights, a clear data strategy enables a company to know precisely what it needs the data for and why. For instance, if a company focuses on liver, pancreatic, or lung cancer, a data strategy ensures the company secures the necessary rights to pursue these fields. A leader who prioritises data strategy from the start and provides the company with data for specific purposes with proper rights fosters the right transactional culture.

Second, once data is collected, a leader educated in data rights can proactively address potential regulatory concerns. This diligence allows the company to identify and resolve flaws early, avoiding situations where regulatory agencies uncover issues too late for the company to correct its course.

Third, alignment across the organisation is essential. If a company's culture emphasises education on data strategy, the execution of that strategy becomes more seamless. Alignment ensures everyone in the company understands and supports the strategy, minimising conflicts and missteps.

For example, imagine an internal company meeting where the head of Software Engineering, head of R&D, and IP Counsel discuss disclosing the company's new code. The head of Software Engineering, with experience in big tech, advocates for open-source sharing, viewing the code as non-innovative and part of a collaborative field. Meanwhile, the head of R&D and IP Counsel, guided by the company's data strategy, argue for protecting the code as a crucial component of their data-driven approach, emphasising its potential for generating proprietary insights and competitive advantage. This scenario highlights the importance of a shared understanding of the data strategy, ensuring that decisions are made in alignment with the company's overall goals.

In this data-saturated world, leadership transcends traditional scientific expertise. It demands the creation of a data-fluent organisation where every member understands the transformative power of data and is empowered to wield it responsibly. Leaders must:

- **Empower Data Citizens:** Invest strategically in training and development programmes that equip employees at all levels with the skills to interpret, analyse, and effectively utilise data. Foster a culture of intellectual curiosity and data-driven decision-making, transforming every employee into a valuable contributor in the data ecosystem.
- **Orchestrate Collaboration and Shatter Silos:** Actively break down information silos and cultivate cross-functional teams that seamlessly integrate diverse expertise – scientists, engineers, ethicists, and business leaders – to collaboratively tackle complex challenges. Encourage open communication and transparent data sharing across departments, creating a unified force for innovation.
- **Lead with Transparency and Forge Trust:** Communicate openly and honestly about the organisation's data practices, AI development processes, and ethical guidelines. Build unwavering trust with patients, partners, and the public by demonstrating an unwavering commitment to responsible data stewardship and ethical AI development.
- **Embrace Agile Experimentation and Drive Innovation:** Foster a dynamic culture of experimentation and iterative learning with data. Encourage employees to explore unconventional ideas, rigorously test hypotheses, and learn from both successes and inevitable setbacks. In this environment, failure is not feared but viewed as a valuable stepping stone on the path to groundbreaking discoveries.

The biotech leaders who not only survive but thrive in this AI-powered landscape will be those who build organisations that are not just data-rich, but truly data-driven – where every strategic decision is informed by actionable insights, every process is optimised by intelligent algorithms, and every member of the team is empowered to contribute to a future of healthier lives. These are the leaders who will define the future of biotech, not just reacting to the data revolution, but actively shaping it. They will be the architects of a new era of medicine, where data is not just a resource, but the very lifeblood of innovation.

Jason Novak's practice was specifically created to focus on advising entities, both large and small, on the various legal issues that can arise with emerging technologies in the healthcare, food and life sciences industries, with a particular and targeted focus on "convergence" technologies (e.g., digital health, personalised/precision medicine, alternative protein) that operate at the intersection of multiple industries.

Jason has extensive experience in IP and data rights strategy. For data rights, Jason advises clients on transactions, protection and general strategy. On the IP front, Jason's experience extends to patent portfolio management, preparation and prosecution, oppositions, counselling, licensing and technology transactions, in- and out-licensing, freedom-to-operate, various types of due diligence, IP training, risk recognition and management and dispute resolution.

Norton Rose Fulbright
555 California Street, Suite 3300
San Francisco, California 94104-1609
USA

Tel: +1 628 231 6811
Email: jason.novak@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/jason-novak-002102b

Dr. Milad Alucozai is an Afghan-American neuroscientist, entrepreneur, biotech executive and global investor with nearly two decades of experience in deep tech, primarily in life sciences. He pushes the boundaries of bioengineering and computational advancements, integrating machine learning and artificial intelligence into biology and medicine. With a strong commitment to commercialising transformative technologies and fostering startup ecosystems worldwide, he is a thought leader and mentor for entrepreneurs through organisations like Creative Destruction Lab and the Wyss Institute at Harvard University. Currently, Milad is the head of Bio and Deep Tech at BoxOne Ventures, where he spearheads the firm's investments in early-stage companies with breakthrough scientific ideas. With nearly 80 early-stage investments, they are recognised as one of North America's most active venture firms. He is also a Venture Partner at Entrepreneur First, a global fund that has built over 500 companies from scratch with an enterprise value of $10bn.

Wyss Institute
201 Brookline Ave
Boston, MA 02215
USA

Tel: +1 617 432 7732
Email: milad.alucozai@wyss.harvard.edu
LinkedIn: www.linkedin.com/in/miladalucozai

Q. Andy Guo has a Ph.D. in Translational Biology and Molecular Medicine, and his practice areas include IP transactions, patent prosecution and patent litigation.

Andy had a fruitful career in academic technology transfer for about six years before joining the firm. He is experienced with evaluating inventions and communicating with researchers, cultivating industry-academia partnerships and commercialising a wide variety of life science and healthcare inventions, such as therapeutics, diagnostics, medical devices and research tools. He understands the unique aspects of academic technology transfer. After joining the firm, Andy has experience advising research institutions on strategic IP transaction matters and complex commercialisation-related IP questions.

While in law school, Andy authored two award-winning papers on patent litigation and licensing topics, one of which was published in the *Houston Law Review*. While completing his Ph.D. degree, Andy conducted neuroscience research and published first-author and co-author peer-reviewed scientific papers.

Norton Rose Fulbright
1550 Lamar Street, Suite 2000
Houston, Texas, 77010
USA

Tel: +1 713 651 3638
Email: q.andy.guo@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/q-andy-guo-ab05b09a

Artificial Intelligence Tools in Health Services – An Overview of Current and Evolving US Federal and State Health Regulatory Structures


Alexis Gilroy


Rebecca Martin


Jessica Tierney


Claire Castles

Jones Day

Although various algorithm-driven capabilities within electronic health records, digital-based clinical protocols, and other technologies have long supported the provision of health services,[1] recent attention on artificial intelligence ("AI") has galvanized federal and state legislators and regulators who are keenly focused on advancing requirements aimed at AI tools involved in health services. Federal regulators at the US Food and Drug Administration ("FDA") have utilised agency discretion for some AI-supported clinical support tools and have grappled with regulatory processes for AI tools requiring approval, yet continue to demonstrate commitment to evolving their regulatory approaches for AI. State legislative efforts regarding AI are increasing rapidly and can apply to a wide variety of technologies that health care providers ("HCPs") use to support diagnostic capabilities, manage administrative tasks, engage with patients, and otherwise. At the same time, foundational health regulatory topics, such as practice of medicine definitions, licensure, corporate practice of medicine ("CPOM"), and medical necessity may also inform interpretations by regulators and impact operational capabilities for HCPs utilising AI.

For several years, industry organisations have advanced policy frameworks and educational materials regarding the use of AI in health services. In March 2024, the Consumer Technology Association published its "What is Health AI?" brief[2] with the goal of informing policy.[3] In May 2024, the Federation of State Medical Boards ("FSMB") published a report called "Navigating the Responsible and Ethical Incorporation of Artificial Intelligence into Clinical Practice", adopted by its House of Delegates with the goal of "recommending best practices for state medical boards in governing the use of Artificial Intelligence (AI) in clinical care".[4] Also in 2023 and 2024, respectively, the American Medical Association ("AMA")[5] and American Telemedicine Association[6] published policy principles for AI. Generally, these materials seek to advance the benefits of utilising AI within the delivery of health services, while identifying frameworks and possible areas of attention and concern for regulators.

The AMA's president said, "[i]t is clear to me that AI will never replace physicians, but physicians who use AI will replace those who do not",[7] and many believe AI holds great promise for reducing health costs, advancing diagnostic capabilities, and elevating the standard of care (especially across geographies and previously disadvantaged communities). Yet, given the often high stakes of health services, legislators and regulators will no doubt impact these innovations. Given the rapidity of AI development alongside the slow pace of regulation, stakeholders should stay abreast of the evolving regulatory requirements, design operational practices and approaches for integrating new requirements (as appropriate), and participate in educating their legislators and regulators to balance the benefits with the real potential impacts of AI.

US Federal – FDA's Approach to AI in Health Services

FDA is tasked with ensuring the safety and effectiveness of medical products, including some that incorporate AI; however, this rapidly changing technology presents unique risks and complexities that challenge FDA's historic approach to regulating medical devices. While FDA's approach is still evolving, the agency has demonstrated its commitment to consider innovative, flexible, and adaptive approaches to the oversight and regulation of AI.

FDA's first approval of an AI-enabled device was in 1995, when the agency approved PAPNET Testing System, a software that used neural networks to aid in the rescreening of cervical Papanicolaou smears previously reported as negative to prevent misdiagnosis of cervical cancer.[8] While FDA has yet to authorise any generative AI-enabled devices – a type of AI that creates new content and ideas – it has authorised over 1,000 AI-enabled devices to date.[9]

FDA considers AI-enabled software to be a medical device if it has one or more medical purposes, which are purposes that are intended to treat, diagnose, cure, mitigate, or prevent disease or other conditions.[10] Software intended for one or more medical purposes that function independently are considered software as a medical device ("SaMD"). Most medical products that incorporate AI and machine learning ("ML") are considered SaMD. Examples of SaMD include software that analyses the electrical activity of the heart from an electrocardiogram signal to diagnose heart conditions, computer-aided diagnosis software that processes images to assist in detecting breast cancer, and continuous glucose monitoring software that analyses data from glucose meters and provides real-time information on blood glucose levels to help patients with diabetes make informed decisions about their health.

FDA ultimately takes a risk-based approach when determining whether to regulate AI-enabled devices – considering the product's intended use, technological characteristics, and risks to patient health. For example, while AI models that support healthy behaviour, general wellness, and administrative functions (e.g., a smart watch that tracks an individual's steps) are not regulated, AI models embedded in traditional medical devices are FDA regulated. Somewhere in the middle lies clinical decision support ("CDS") software; regarding CDS tools, FDA's regulatory oversight expands or condenses depending on the degree of risk. For example, where the

software provides sufficient transparency and information forming the basis for a diagnosis or treatment recommendation such that the HCP would not primarily rely on the tool, but instead their own judgment to make clinical decisions, then FDA typically does not exercise regulatory oversight.

Over the years, FDA has developed and applied innovative approaches to the regulation of AI-enabled devices. Some recent efforts include releasing the agency's five-part action plan in January 2021 to advance AI/ML-based SaMD, which included a commitment to developing a total product lifecycle-based regulatory framework for AI-enabled devices.[11] An initial outcome of this effort was a draft (and now final) guidance that provided a pathway for manufacturers to plan for AI's inherent learning capabilities and resulting changes to a product without having to request additional approvals from FDA with anticipated evolutions of the technology.[12] In 2022, FDA published its final CDS software guidance,[13] which is one of a handful of guidances that outline FDA's policies regarding its oversight of certain device software excluded from "device" as defined in federal statute (most recently in 2016 as a result of the 21st Century Cures Act).[14] FDA also created an advisory committee (holding its inaugural meeting in 2024) to provide guidance and recommendations for regulating digital health technologies, including AI-enabled devices.[15] Most recently in January 2025, FDA continued its efforts by issuing a draft guidance providing recommendations for the content of marketing submissions as well as the design, development, deployment, and maintenance for AI-enabled devices.[16]

The rapid development, advancement, and adoption of AI in health care suggests that the agency will continue to accelerate and adapt its approach to regulating tools across the spectrum of those integrating AI – the industry should expect and be prepared to adapt to robust FDA oversight through policies, frameworks, guidance documents, and initiatives for the foreseeable future.

US States – New Legislative Focus on AI in Health Services

In the 2024 legislative session, the majority of US states introduced AI-related proposed legislation with an increasing focus on AI in the health care space.[17] Notably, California and Colorado passed AI legislation both directly and indirectly impacting HCPs, underscoring requirements and prohibitions relating to transparency, anti-discrimination and bias, and HCP review and determination – categories likely to form models for future state laws and regulations.

Transparency

Recent AI-health legislation focuses on transparency through disclosures from (i) providers to patients, and (ii) further up the chain, developers of generative AI systems to providers utilising the systems.

California's AB 3030 requires health facilities, clinics, physicians' offices, and offices of group practices using generative AI in the creation of written or verbal communications to patients regarding clinical information to provide disclosures about the use of AI supporting the clinical information.[18] Specifically, disclosures to patients must (i) identify that such communications involved generative AI, and (ii) present clear instructions describing how a patient can contact a HCP or other appropriate person.[19] Notably, health organisations can forgo the required disclosure if a HCP reviews the AI-generated communication before it is distributed to a patient.[20]

Regarding disclosures from AI system developers to HCPs, California also passed AB 2013 and SB 942 in 2024, requiring that certain developers make disclosures regarding the training data, sources of data, and AI detection tools.[21] Under AB 2013, such developers must disclose (without limitation) the sources or owners of data sets, a description of how utilised datasets furthered the intended use of the AI, and the number of data points included in data sets.[22,23] Such disclosures are crucial for HCPs' operational teams as they assess the appropriateness of onboarding vendors with AI-powered tools, and associated risks the provider may "inherit" based on the developer's approach to data and training of the tool. Unique to SB 942, the California AI Transparency Act, developers of AI systems must implement contractual provisions with third-party licensees, which may include HCPs, to maintain data source disclosures.[24] Violators of California's AI Transparency Act, including HCP-third party licensees, can face enforcement from the California Attorney General ("AG").[25]

Protections against discrimination and bias

Some state laws focus on risks of discrimination to certain individuals from AI systems. For example, Colorado's Artificial Intelligence Act ("Colorado's Legislation") requires deployers of "high-risk artificial intelligence systems" ("High-Risk Systems")[26] to use "reasonable care" in protecting consumers from any known, or reasonably foreseeable risks of algorithmic discrimination.[27]

Deployers of High-Risk Systems that proactively implement certain practices may assert a rebuttable presumption that they took "reasonable care" to protect against prohibited discrimination.[28] Such practices focus on risk assessments and related policies, consumer notifications and rights, and public and governmental disclosures.[29]

While Colorado's Legislation offers an exemption for certain HCPs, the exemption only applies if the HCP is a Health Insurance Portability and Accountability Act-covered entity delivering health care recommendations that: (i) are generated by an AI system; (ii) require a HCP to take action to implement the recommendations; and (iii) are not considered "high risk".[30] Providers that do not fit squarely within the exemption may still be subject to Colorado's Legislation.

Provider over program – prioritising provider determinations over AI decisions

Recent AI-related health legislation also underscores the importance of provider decision-making over AI-enabled determinations. California's SB 1120 reflects this, prohibiting health care service plans (i.e., insurers) from improper uses of AI, algorithms, and other software tools when assessing medical necessity in claims for reimbursement. Specifically, SB 1120 explicitly prohibits insurers from using AI to "supplant" a HCP's decision regarding medical necessity, and instead must base its assessment on the enrollee's: (i) medical or other clinical history; (ii) individual clinical circumstances as presented by the requesting provider; and (iii) other relevant clinical information within the enrollee's medical or other clinical record, as applicable.[31]

Consistent with other legislation focused on anti-discrimination and transparency described above, SB 1120 prohibits insurers from discrimination and "directly or indirectly caus[ing] harm to [] enrollee[s]".[32] Further, health plans must implement disclosures regarding their use and oversight

of AI systems, algorithms, and software tools in written policies and procedures, and make such programs and tools available for government audit and inspection.[33]

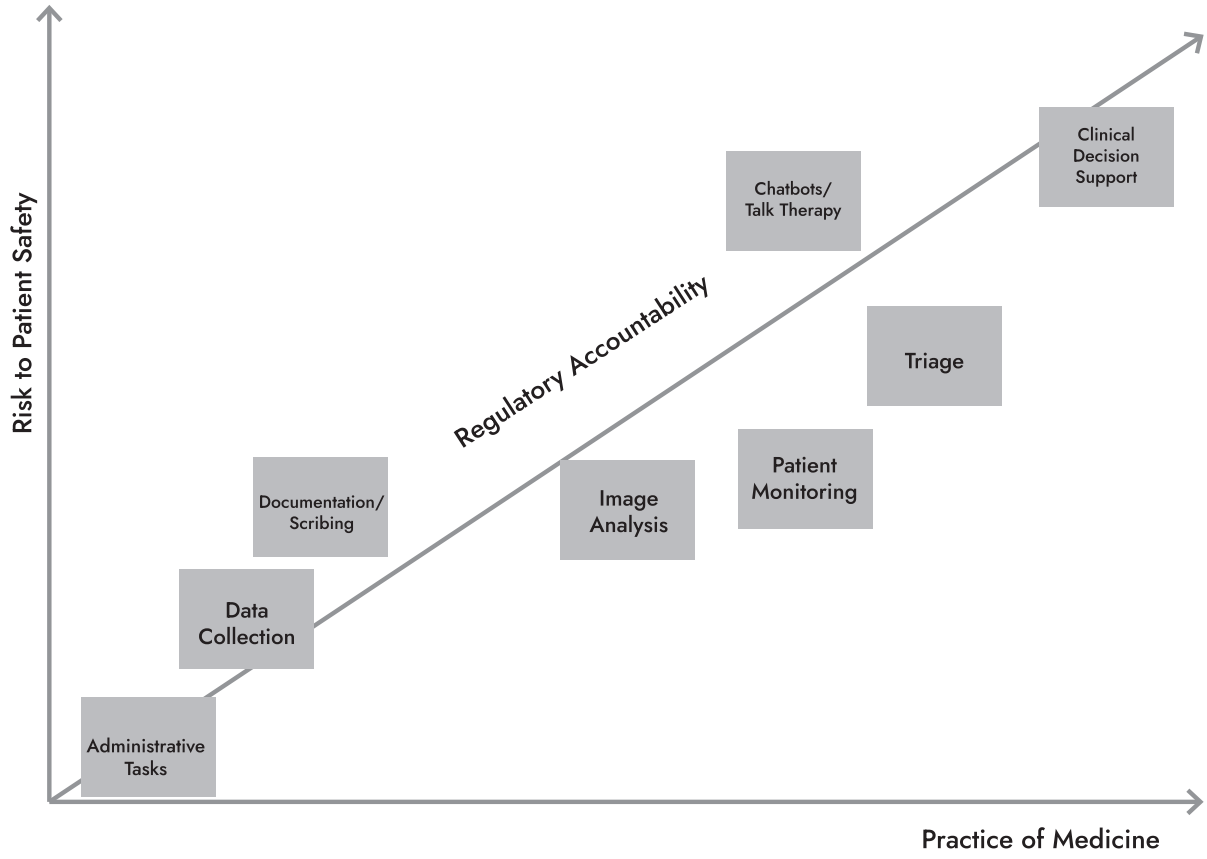
Although state legislators are increasingly active at the intersection of AI and health care, legislation to date focuses on specific use cases and risks. While states have attempted – and will likely continue to attempt – broader legislation, the industry should expect an increasingly complex patchwork of state AI legislation for specific settings and protections in the health care industry.

US States – Impacts of "Traditional" Health Laws and Regulations

While new legislation and guidance on AI in health services emerges at the federal and state levels, interpretations of existing state laws and regulations governing the provision of health services may also impact the use, deployment, and ultimate incorporation of AI tools in the health care setting.

State medical boards are responsible for licensing, regulating, and disciplining individual physicians who engage in the practice of medicine for patients located in the state, which is typically broadly defined to include activities such as diagnosing, treating, and prescribing.[34] As the FSMB acknowledged in its report on "Navigating the Responsible and Ethical Incorporation of Artificial Intelligence into Clinical Practice", "[s]tate medical boards do not regulate tools or technologies, only the licensed physicians that use those tools" and, according to FSMB, the more that AI tools perform functions that look like the practice of medicine, the higher the scrutiny by regulatory bodies should be.[35]

Figure 1 – Modelling Risk *v.* Function[36]



The majority of US states also prohibit or restrict CPOM (or other professions) or make it unprofessional conduct for a physician to aid in the unlicensed practice of medicine by individuals or entities unlicensed to do so.[37] At a high level, the CPOM doctrine restricts non-professional persons or entities from controlling, influencing, or interfering with clinical judgment by a licensed HCP. To preserve the clinical discretion and independence of licensed HCPs, organisations developing and deploying AI functionalities may benefit from careful consideration of provider involvement and oversight within development, training, and on-going utilisation of AI tools with clarity that licensed providers are responsible for the act of practising medicine, whether or not the provider is supported by an AI tool.

Some states are starting to explicitly address this issue in legislation or regulations on AI, such as by requiring that AI tools be used only when the clinical provider deems it is appropriate after reasoned judgment and organisations like the AMA and American Nursing Association have expressed similar sentiments.[38] There are also several existing regulatory concepts in the health care space that could offer a useful framework for states to consider for regulating the use of AI by HCPs while allowing providers to take advantage of novel tools to improve patient outcomes.[39] For example:

- Many states have exemptions to licensure requirements for certain "consultations" or even second opinions by out-of-state providers,[40] which could potentially be applied to AI as a "second opinion" of sorts supporting an in-state licensed provider.
- State professional boards require varying degrees of supervision and oversight over non-physician ancillary providers, such as nurses or medical assistants (typically viewed as unlicensed personnel).

- Most states and DC have addressed telemedicine (the use of digital tools to enable HCP and patient engagement when not in-person), such as by requiring specific informed consent (e.g., identifying risks specific to the use of telemedicine),[41] implementing additional record-keeping and privacy/security standards, and providing the patient with clear directions regarding potential follow-up care.

In the absence of a clear legal framework, HCPs and developers of AI technology performing functions consistent with the practice of medicine – diagnosing, treating, or prescribing – may benefit from structuring AI technologies and workflows as tools and not substitutes for the clinical judgment and discretion of licensed HCPs. Contractual documentation between HCPs and developers regarding AI tools should consider the roles and responsibilities of each party and, in certain circumstances, support and protect the independence and integrity of the judgment of licensed HCPs.

Early Enforcement Activities at the US Federal and State Levels

Just as the deployment of AI has spurred legislative activities, it has also started to prompt regulatory scrutiny and enforcement at both the federal and state level. These actions have targeted a range of conduct, using various theories, such as misrepresentations or false claims to the government under the False Claims Act ("FCA"), unfair bias in violation of state and federal non-discrimination laws, and false and misleading statements about AI under state and federal consumer protection laws.

Federal

Throughout 2024, AI captured the attention of the Department of Justice ("DOJ") at the highest levels. In February 2024, DOJ launched its "Justice AI Initiative" to further its understanding of the "promise of AI and the perils of its misuse".[42] At the same time, and with an emphasis on AI's "perils", Deputy AG Lisa Monaco instructed the DOJ's Criminal Division to seek stiffer penalties for criminal offences "made significantly more dangerous by the misuse of AI".[43] In July 2024, DOJ updated its "Evaluation of Corporate Compliance Programs" guidance,[44] which is used by prosecutors and compliance professionals alike, to include guidance for evaluating the potential misuse of AI by corporations. Some of these changes specifically implicate processes that can lie at the heart of health care business operations: "[P]rosecutors will consider whether the company is vulnerable to criminal schemes enabled by new technology, such as false approvals and documentation generated by AI. If so, we will consider whether compliance controls and tools are in place to identify and mitigate those risks, such as tools to confirm the accuracy or reliability of data used by the business."[45] In August 2024, the Justice AI Initiative issued recommendations to the US Sentencing Commission to codify a sentencing enhancement applicable to cases in which AI was used.[46] In its report, DOJ suggested that the pre-existing enhancement provisions do not adequately address the harms associated with AI, which purportedly included making "crimes easier to commit", amplifying their harms and enabling "offenders to delay or avoid detection".[47]

The Federal Trade Commission ("FTC") has also been active in enforcement concerning AI-related claims[48] and notably, a member of Congress has expressed concerns to the FTC and DOJ's Antitrust Division that "the use of algorithms that collect and process data" should not be used "to allow competitors to collude to make healthcare more costly for patients".[49] DOJ and the FTC have highlighted similar concerns in various Statements of Interest that have been filed over the last year in private price-fixing litigation, emphasising their view that the use of common algorithms for pricing could result in antitrust violations.

The potential of civil enforcement may also pose risk as the legal landscape evolves. For instance, DOJ and relators have also turned to the FCA to assert claims based on the allegedly improper use of algorithms in health care delivery and payment. In 2020, for example, DOJ filed an FCA complaint against a Medicare Advantage Organisation ("MAO") alleging that the MAO ran algorithms designed to identify diagnosis codes that could generate more revenue while failing to write an algorithm to find inaccurately reported diagnosis codes, even though its data team could have done so.[50] Further, in 2023, the Second Circuit left open the possibility of a "worthless services" argument under the FCA relating to the use of AI systems.[51]

State

Investigations and enforcement by state AGs have also signalled that AI is on the radar at the state level. In 2022, the California AG launched a novel investigation into potential racial and ethnic biases in health care algorithms used by hospitals and health systems, requesting information from 30 hospitals and health systems.[52]

Regulators are also increasingly focused on enforcing consumer protection laws, including unfair and deceptive acts and practices statutes, against businesses that allegedly make false, inaccurate, or misleading statements about their use of AI technology. For example, in September 2024, the Texas AG's Office ("AGO") announced it secured a "first-of-its-kind" settlement with Pieces Technology, an AI health care technology company, regarding alleged misrepresentations of the accuracy of its product.[53] The company had partnered with several major Texas hospitals, receiving health care data to "summarise" patient conditions and treatment for hospital staff. Pieces Technology represented that its product was highly accurate and advertised a low "critical hallucination rate" and "severe hallucination rate" of only "<.001%" and "<1 per 100,000", respectively. The Texas AGO asserted these metrics likely violated the Texas Deceptive Trade Practices – Consumer Protection Act, as they were "false, misleading, or deceptive". As part of the settlement, the Texas AGO required Pieces Technology to make accurate disclosures regarding its products' reliability, testing, and monitoring procedures, the definition or meaning of any metrics referenced, training data, and known or reasonably knowable harms or misuses of its products. The Pieces Technology case highlights the potential for enforcement against AI companies under existing laws that are not specific to AI and the importance of exercising caution in developing claims about an AI product's efficacy or performance.

Acknowledgments

The authors would also like to acknowledge and thank Ryan Blaney, Harrison Farmer, Rachel Page, and Maxine Thomas of Jones Day, whose efforts and contributions were significant in the development of this chapter.

Disclaimer

The views and opinions set forth herein are the personal views or opinions of the authors; they do not necessarily reflect views or opinions of the law firm with which they are associated.

Endnotes

1 Thomas Davenport and Ravi Kalakota, *The Potential for Artificial Intelligence in Healthcare*, 6 F.H.J. 2, 94–98 (2019), https://www.sciencedirect.com/science/article/pii/S2514664524010592?via%3Dihub; Adam Bohr and Kaveh Memarzadeh, *Chapter 2: The Rise of Artificial Intelligence in Healthcare Applications*. Artificial Intelligence in Healthcare, 25–60 (2020), https://www.sciencedirect.com/science/article/pii/B9780128184387000022?via%3Dihub

2 Consumer Technology Association ("CTA"), *Support the Thoughtful Application of Trustworthy AI in Healthcare,* https://cdn.cta.tech/cta/media/media/pdfs/cta_ai_healthcare.pdf (last visited Jan. 15, 2025).

3 CTA, Press Release, *Consumer Technology Association Convenes Health Care Stakeholders on Artificial Intelligence* (Mar. 13, 2024), https://www.cta.tech/Resources/Newsroom/Media-Releases/2024/March/Consumer-Technology-Association-Convenes-Health-Ca

4 FSMB, News Release, *FSMB Releases Recommendations on the Responsible and Ethical Incorporation of AI into Clinical Practice* (May 2, 2024), https://www.fsmb.org/advocacy/news-releases/fsmb-releases-recommendations-on-the-responsible-and-ethical-incorporation-of-ai-into-clinical-practice; FSMB, *Navigating the Responsible and Ethical Incorporation of Artificial Intelligence into Clinical Practice* (Apr. 2024), https://www.fsmb.org/siteassets/advocacy/policies/incorporation-of-ai-into-practice.pdf (hereinafter "FSMB Report").

5 AMA, *Principles for Augmented Intelligence Development, Deployment, and Use* (Nov. 14, 2023), https://www.ama-assn.org/system/files/ama-ai-principles.pdf (hereinafter "AMA AI Principles").

6 American Telemedicine Association ("ATA"), *The ATA's Artificial Intelligence (AI) Principles* (Oct. 2023), https://www.americantelemed.org/wp-content/uploads/2023/10/ATA-AI-Principles-23-v2.pdf

7 Erin Schumaker *et al.*, *AMA President: AI Will Not Replace Doctors*, Politico (Jul. 10, 2023); https://www.politico.com/newsletters/future-pulse/2023/07/10/ai-will-not-replace-us-ama-president-says-00105374

8 FDA, *Premarket Approval (PMA) Database: PAPNET (R) TESTING SYSTEM*, https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpma/pma.cfm?id=P940029 (last updated Jan. 13, 2025).

9 FDA, *Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices*, https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-aiml-enabled-medical-devices (last updated Dec. 20, 2024).

10 21 U.S.C. § 201(h).

11 FDA, *Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan* (Jan. 2021), https://www.fda.gov/media/145022/download?attachment

12 FDA, *Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence-Enabled Device Software Functions* (Dec. 2024), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial-intelligence

13 FDA, *Clinical Decision Support Software* (Sept. 28, 2022), https://www.fda.gov/media/109618/download

14 FDA, *Guidances with Digital Health Content*, https://www.fda.gov/medical-devices/digital-health-center-excellence/guidances-digital-health-content (last updated Jan. 6, 2025).

15 FDA, *Digital Health Advisory Committee*, https://www.fda.gov/advisory-committees/committees-and-meeting-materials/digital-health-advisory-committee (last updated Dec. 10, 2024); FDA, *November 20–21, 2024: Digital Health Advisory Committee Meeting Announcement*, https://www.fda.gov/advisory-committees/advisory-committee-calendar/november-20-21-2024-digital-health-advisory-committee-meeting-announcement-11202024 (last updated Jan. 14, 2025).

16 FDA, *Artificial Intelligence-Enabled Device Software Functions: Lifecycle Management and Marketing Submission Recommendations* (Draft Jan. 7, 2025), https://www.fda.gov/media/184856/download

17 *See* National Conference of State Legislatures, *Artificial Intelligence 2024 Legislation*, https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation (last updated Sept. 9, 2024).

18 Cal. Health & Safety Code § 1339.75(a).

19 *Id.*

20 *Id.* § 1339.75(b).

21 Under AB 2013, developers of certain generative AI systems or services must make documentation regarding training data available on their websites. Cal. Civ. Code § 3111.

22 *Id.* § 3111(a).

23 California's SB 942 similarly requires certain generative AI system developers to, among other things, disclose the origin of the generative AI audio, video, or image content through latent and, upon request, manifest disclosures. Cal. Bus. & Prof. Code § 22757.3.

24 *Id.* § 22757.3(c).

25 *Id.* § 22757.4(c).

26 "High-Risk Systems" are systems that "when deployed, make[], or [are] a substantial factor in making, a consequential decision" such as those that have a "material legal or similarly significant effect" on the provision or denial of, or the cost or terms of, health care services. Colo. Rev. Stat. § 6-1-1701(9)(a), (3).

27 *Id.* § 6-1-1703(1).

28 *Id.*

29 *See id.*

30 *Id.* § 6-1-1705(5)(d).

31 Cal. Health & Safety Code § 1367.01(k).

32 *Id.*

33 *See id.*

34 *See, e.g.*, Colo. Rev. Stat. § 12-240-107(1)(b) (defining the "practice of medicine" to include "[s]uggesting, recommending, prescribing, or administering any form of treatment, operation, or healing for the intended palliation, relief, or cure of a person's physical disease; ailment; injury; condition; or behavioral, mental health, or substance use disorder").

35 FSMB Report, at 5.

36 *Id.* at 6 fig.1.

37 *See, e.g.*, 225 Ill. Comp. Stat. 60/3 ("No person shall practice medicine, or any of its branches, or treat human ailments without the use of drugs and without operative surgery, without a valid, active license to do so…."); Cal. Bus. & Prof. Code § 2052 (same).

38 *See* 30 Miss. Code R. § 2635-13.2-13.3; N.C. Med. Board, Position Statement 3.2.1, *Medical Records – Documentation, Electronic Health Records, Access, and Retention* (amend. Nov. 2024), https://www.ncmedboard.org/resources-information/professional-resources/laws-rules-position-statements/position-statements/medical-records-documentation-electronic-health-records-access-and-retentio; Amer. Nurses Assoc., Position Statement, *The Ethical*

Use of Artificial Intelligence in Nursing Practice (2022), https://www.nursingworld.org/globalassets/practiceandpolicy/nursing-excellence/ana-position-statements/the-ethical-use-of-artificial-intelligence-in-nursing-practice_bod-approved-12_20_22.pdf; AMA AI Principles.

39 *See, e.g.*, FSMB Report, at 3.

40 *See, e.g.*, 225 Ill. Comp. Stat. 60/49.5; Ind. Code § 25-22.5-1-1.1(a)(5); S.C. Code Ann. § 40-47-37.

41 Some states have already started requiring special informed consent for the use of AI. *See* 30 Miss. Code R. § 2635-13.4 (requiring special informed consent for the use of AI and other "alternative therapies" that includes "[a]n accurate description of the benefits and risks of treatment or intervention, based on scientific evidence, as well as an explanation of alternatives to treatment or an intervention, and the right to withdraw from treatment or an intervention without denial of standard of care to patients").

42 DOJ, Speech, *Deputy Attorney General Lisa O. Monaco Delivers Remarks at the University of Oxford on the Promise and Peril of AI* (Feb. 14, 2024), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-university-oxford-promise-and

43 *See* DOJ, Press Release, *Readout of Deputy Attorney General Lisa Monaco's Participation in the 2024 Munich Security Conference* (Feb. 19, 2024), https://www.justice.gov/opa/pr/readout-deputy-attorney-general-lisa-monacos-participation-2024-munich-security-conference

44 DOJ, Crim. Div., *Evaluation of Corporate Compliance Programs* (Sept. 2024), https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl

45 DOJ, Speech, *Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the Society of Corporate Compliance and Ethics 23rd Annual Compliance & Ethics Institute* (Sept. 23, 2024), https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-nicole-m-argentieri-delivers-remarks-society

46 DOJ, Crim. Div., *Annual Report to U.S. Sentencing Commission* (July 15, 2024), at 12–13, https://www.justice.gov/criminal/media/1362211/dl

47 *Id.* at 13.

48 FTC, Press Release, *FTC Announces Crackdown on Deceptive AI Claims and Schemes* (Sept. 25, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes

49 *See* Letter from Amy Klobuchar, U.S. Sen., to Jonathan Kanter, Asst. AG, DOJ Antitrust Division, and Lina M. Khan, Chair, FTC (Apr. 29, 2024), https://www.klobuchar.senate.gov/public/_cache/files/4/4/4463fdf7-457e-4e48-b885-9dca394c57d4/7F84E808973057BD75668746A378A06B.4.29.2024-letter-to-doj-ftc-re-multiplan-insurance-payments.pdf

50 Complaint, *U.S. v. Anthem, Inc.*, 1:20-cv-02593 (S.D.N.Y. Mar. 26, 2020), Dkt. 1, https://www.justice.gov/usao-sdny/press-release/file/1262841/dl?inline=

51 *Doe 1 v. EviCore Healthcare MSI, LLC*, No. 22-530-CV, 2023 WL 2249577 (2d Cir. Feb. 28, 2023), at *2–3 (upholding the district court's dismissal on Rule 9(b) grounds and not reaching the merits of the worthless services argument).

52 CA DOJ, Press Release, *Attorney General Bonta Launches Inquiry into Racial and Ethnic Bias in Healthcare Algorithms* (Aug. 31, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-launches-inquiry-racial-and-ethnic-bias-healthcare

53 TX AGO, Press Release, *Attorney General Ken Paxton Reaches Settlement in First-of-its-Kind Healthcare Generative AI Investigation* (Sept. 18, 2024), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-reaches-settlement-first-its-kind-healthcare-generative-ai-investigation; Assurance of Voluntary Compliance, *Texas v. Pieces Technologies Inc.*, No. DC-24-1346 (Tex. Dist. Ct., Dallas Cty. Aug. 21, 2024), https://www.texasattorneygeneral.gov/sites/default/files/images/press/Petition%20for%20Approval%20of%20AVC%20Pieces%20File%20Stamped.pdf

Alexis Gilroy, a national leader in the digital health industry, advises on complex transactional and health regulatory issues with an emphasis on virtual health methods, such as telemedicine, telehealth, and mobile health. With more than two decades in digital health, her experience supports various regulatory counselling and transactional needs for health AI, digital health product development, and life sciences organisations, including novel virtual clinical trial offerings. Alexis is co-leader of the Firm's Health Care & Life Sciences Practice. Focused on transactions across the health care, life sciences, and digital health sectors on innovative technologies and methods, Alexis pairs practical experience with a keen understanding of often novel and still evolving federal and state regulatory requirements.

Jones Day
51 Louisiana Avenue, N.W.
Washington, D.C. 20001-2113
USA

Tel: +1 202 879 5552
Email: agilroy@jonesday.com
LinkedIn: www.linkedin.com/in/alexisgilroy

Rebecca Martin is a 15-year veteran of the U.S. Attorney's Office for the Southern District of New York (SDNY), with decades of experience in investigations and litigations involving the federal False Claims Act (FCA), New York and other state false claims acts, Anti-Kickback Statute (AKS), Stark Law, FDCA, and other regulatory and privacy matters. She regularly represents clients facing *qui tam* complaints and in other matters before the Department of Justice (DOJ), state Attorney General Offices, and local regulatory bodies.

Jones Day
250 Vesey Street
New York, New York 10281-1047
USA

Tel: +1 212 326 3410
Email: rcmartin@jonesday.com
LinkedIn: www.linkedin.com/in/rebecca-martin-54887511

Jessica Tierney has more than 10 years of experience working with U.S. Food & Drug Administration (FDA) regulations and enforcement activities. As a former attorney with the FDA, Jessica brings valuable perspective to clients seeking advice in matters before the agency. Jessica regularly advises clients on bringing to market novel food, tobacco, medical device, and drug products. Clients frequently look to Jessica when engaging with the FDA, particularly in matters involving regulatory compliance such as recalls and withdrawals, responses to FDA 483 violation forms and warning letters, and matters regarding marketing and good manufacturing practices.

Jones Day
51 Louisiana Avenue, N.W.
Washington, D.C. 20001-2113
USA

Tel: +1 202 879 3474
Email: jtierney@jonesday.com
LinkedIn: www.linkedin.com/in/jessica-tierney-03543b2a

Claire Castles advises clients on complex health care and life science regulatory compliance issues in transactions, investigations, and litigation matters, including issues that are international in scope, relate to significant regulatory enforcement, and present potential reputational concerns. Claire helps clients implement response strategies for novel and emerging public health threats, including COVID-19. She assists clients in regulatory waiver strategies and impact on corporate practice of medicine, HIPAA/HITECH, and other state and federal regulations and guidance.

Jones Day
555 South Flower Street
Fiftieth Floor
Los Angeles, California 90071-2300
USA

Tel: +1 213 243 2629
Email: ccastles@jonesday.com
LinkedIn: www.linkedin.com/in/claire-castles-36b155142

Jones Day is a global law firm with more than 2,400 lawyers in 40 offices across five continents. The Firm is distinguished by: a singular tradition of client service; the mutual commitment to, and the seamless collaboration of, a true partnership; formidable legal talent across multiple disciplines and jurisdictions; and shared professional values that focus on client needs.

www.jonesday.com

Data Protection and Cybersecurity in Digital Health


Stephen K. Phillips


Alicia Macklin

Hooper, Lundy & Bookman, P.C.

Introduction and Summary

Digital health products and services are typically accessible over the Internet. Many digital health companies seek to leverage the near universal access of the Internet to offer products and services to a mass market and achieve economies of scale. The health care information that these companies collect, create, and use, however, is among the most highly regulated categories of data under data protection and cybersecurity laws.

Data protection laws regulate health care data at the continental, national, and state/provincial level. Continental and national privacy laws usually establish minimum levels of privacy protection that allow national and state/provincial laws to establish stronger privacy protections. In addition, privacy laws often differentiate among various categories of health information, with stronger protections afforded categories of health information whose misuse or wrongful disclosure can cause more harm.

Compliance with different privacy rules based on jurisdiction and category of health information is the primary privacy and security challenge for digital health, with the following being the most significant challenges that digital health faces:

1. The ease of electronic data transmission exacerbates cybersecurity challenges.
2. Cybersecurity threats continually increase, with health information among the most targeted categories of data.
3. The accelerated pace of technological innovation compared to legislative and regulatory rulemaking creates regulatory vacuums and unclear legal requirements.
4. Differences in data protection requirements based on local jurisdiction and health information category preclude universal data protection and cybersecurity rules.
5. Digital health companies tend not to design products to comply with local privacy and security laws or laws relating to specific categories of health information.

Without laws keeping pace with technologies and threats, the tension between security, functionality, and efficiency increases. Industry best practices and certification programmes hold promise as an increasingly important means of filling the gap between technological innovation and regulation for digital health.

The Historical Regulation of Health Care Privacy and Security

The statutory protection afforded health information has existed for over 40 years. California, a bellwether jurisdiction for the regulation of businesses and the protection of consumers, enacted its landmark privacy law, the California Medical Information Act, in 1981.[1] The Health Information Portability and Accountability Act of 1996, commonly known as "HIPAA", followed 15 years later.[2] The General Data Protection Regulation ("GDPR"), enacted on April 27, 2016, came into force May 25, 2018.[3]

The Tradition of Local Autonomy

In the U.S. Constitution, the concept of "federalism" has long reserved to the states the regulation of human activity not otherwise determined to be in the national interest. States regulate most issues of crime, health, and safety, including the protection of health information. Where federal laws encroach upon domains historically regulated by state laws, they often do so through a preemption scheme that attempts to balance national interests with state autonomy by allowing stronger state protections to persist.[4]

HIPAA is no exception. From its inception, and with the promulgation of its administrative regulations containing detailed rules regarding health privacy and security requirements, HIPAA follows a preemption doctrine that sets minimum standards of privacy protection and allows state privacy laws to establish heightened privacy protections. HIPAA privacy rights co-exist with stronger state privacy rights, preempting only state laws affording weaker privacy rights to individuals.[5]

Similarly, the GDPR establishes privacy protections throughout the European Union, but preserves autonomy to its member nations to impose stronger national privacy protections, which then co-exist with GDPR standards. As with HIPAA, the GDPR preempts weaker national privacy protections while allowing member nations to enact, without threat of preemption, national laws providing stronger privacy protections.[6]

The deference to local autonomy by continental and federal privacy standards is unlikely to change; if anything, efforts to create global governmental standards appear to be dissipating. For example, the United States has no national comprehensive data privacy law and has none on the horizon, but it has seen a proliferation of state consumer data protection laws modelled after the GDPR. California led the way with passage of its California Consumer Protection Act of 2018 ("CCPA"), as amended by its California Privacy Rights Act ("CPRA") and followed by regulations specifying more detailed requirements for protecting personal information.[7] By the end of 2024, 23 states had adopted similar but not identical personal information privacy laws. In most cases, these statutes exempt health information protected under HIPAA from their ambit but otherwise protect individuals' health information.[8]

HIPAA does not apply to business-to-consumer ("B-C") digital health companies, because HIPAA regulates only "covered entities" and their "business associates".[9] Digital health care providers who receive pay for services from patients, rather than patient health insurers, are not covered entities. Digital health companies providing administrative (*i.e.*, non-treatment) services are only business associates if they service covered entities. State consumer data privacy laws, however, apply to B-C digital health companies. Although the state consumer data laws typically follow a common template for protecting health data, the variation among state statutes affords less consistency regarding privacy and security requirements than under HIPAA, even with HIPAA's accommodation of stronger state privacy protections. Thus, at least in the United States, for B-C digital health companies, cybersecurity and privacy requirements have become more localised than for traditional health care companies or digital health companies subject to HIPAA.

Laws Providing Additional Protection for Sensitive Health Information

Another feature of data protection laws is the higher level of privacy protection afforded certain categories of health information considered more sensitive (*i.e.*, having the potential to cause more harm from misuse and unauthorised disclosure). The GDPR and analogous state personal information or consumer data laws in the United States generally treat health information as "sensitive" personal information and thus accorded higher levels of privacy protection.[10] In the United States, there are additional long-standing heightened protections to specific categories of health information. These categories include behavioural and sexual health information, as well as genetic information. At the federal level in the United States, substance abuse information is accorded special protection under what are commonly known as the Part 2 regulations.[11] HIPAA has, since the enactment of the Privacy Rule, also provided stronger protection to psychotherapist notes[12] and added special protection for genetic information under the Genetic Information Non-discrimination Act of 2008.[13] More recently and effective December 2024, HIPAA provides special protections for reproductive health information.[14]

In addition to the U.S. federal laws, state laws provide special protection for sensitive health information. Various states, with California again being the most noteworthy, have afforded special protections for specific health information. In California, the Lanterman-Petris Short Act[15] provides special protections for certain behavioural health information, and various provisions of the *California Health & Safety Code* afford heightened protection to information regarding HIV status,[16] immunisation,[17] and substance use disorder treatment.[18]

Some of the more recent state laws regulating sensitive health information mandate not only specific privacy practices, but also specific security practices that impact the design of health information systems. On January 1, 2024, California's Assembly Bill No. 352 ("AB 352") became law, and requires, by July 1, 2024, certain businesses that electronically store or maintain medical information related to gender-affirming services, abortion and abortion-related services, and contraception ("reproductive health information"), to develop capabilities, policies, and procedures, that (a) limit user access privileges to reproductive health information, (b) prevent the sharing of reproductive health information to persons and entities outside of California, (c) segregate reproductive health information from the rest of the patient's record, and (d) provide the ability to automatically disable access to segregated reproductive health information from individuals and entities outside of California.[19] Also effective January 1, 2024, California Assembly Bill No. 254 ("AB 254") revised the definition of medical information under the Confidentiality of Medical Information Act ("CMIA") to include reproductive or sexual health application information, defined to mean information about a consumer's reproductive or sexual health collected by a reproductive or sexual health digital service, which includes mobile applications or websites collecting reproductive or sexual health application information from individuals. AB 254 subjects such businesses to CMIA, including the new CMIA requirements under AB 352.[20]

Unique Data Protection and Cybersecurity Challenges for Digital Health

The privacy and security laws apply fully to uses and disclosures common in digital health, and in certain cases, such as the limitation of the HIPAA Security Rule to electronic health information, apply specifically to digital health. There are characteristics of digital health that make compliance with health data privacy and security laws far more challenging than with health care information in paper form; some of those challenges, in fact, have driven the enactment of health care privacy and security laws.[21]

Digitalising Data Increases the Potential Severity of Security Breaches

First, the ease of electronic data disclosure increases the potential severity of security breaches. When paper records were the norm for maintaining health information, one factor mitigating the severity of a security breach was the limited amount of health information that could be misappropriated. Because the penalties associated with violations of privacy and security obligations under HIPAA and analogous state laws correlate to the number of individual health records involved, a misappropriation of paper records often produces relatively small penalties.[22] Correlating to relatively small penalties are relatively low insurance premiums for such incidents. With electronic health information, a security breach can misappropriate enormous amounts of data – equivalent to a truckload – and very quickly.[23]

Virtually all security breaches of electronic health information – exfiltration, alteration, denial of access, destruction, *etc.* – are potentially exponentially greater in scope and thus severity than security breaches of paper records. The privacy and security laws make no allowance for such disparate impacts in the digital health realm; quite the opposite, the potential damage from breaches of electronic health information is often a justification for stronger privacy and security requirements and thus greater penalties.[24]

Electronic Information and the Criminal Opportunity

A second area where digital health presents challenges different than the world of paper information relates to criminal activity. It is relatively rare for health care providers to be subject to concerted efforts to steal large amounts of paper health information. On the other hand, cybersecurity threats advance unabated, with digital health information among the most targeted categories of data by criminals. Because of the wealth of information that can be stolen in digital form,

criminals, with typical alacrity and ingenuity in the adoption of technology to their criminal endeavours, have developed a vibrant black market for health information and increasingly clever and advanced methods of stealing electronic health information. Fraudulent billing, identify theft, extortion and other crimes have all found fertile soil in electronic health information systems.[25] Financial opportunity and poor security practices within the health industry have attracted criminal attention, resulting in an ever-increasing range of cyber-threats, from advanced malware, phishing expeditions and penetration attacks.

A stressed health care provider community, where economic and budgetary forces increasingly squeeze margins from health care providers, presents an easier target for cyber-attack than, for example, financial institutions, which operate in a culture attuned and better prepared and resourced for cyberattacks. At the same time, federal regulatory policy in the United States, as exemplified by the 21st Century Cures Act ("Cures Act") and its requirements for enhanced patient access to individual health information, have pushed health care providers, ready or not, to digitise health information and make it readily available to patients and their designated third parties. The Cures Act, signed into law on December 13, 2016, is designed to help patients quickly and easily access their electronic health information to make informed decisions about their care. It requires health care organisations to have the capability to release electronic health information, such as clinical notes and test results, to patients as soon as the information is finalised. The Act includes a provision requiring that patients be able to electronically access all of their electronic health information, structured and/or unstructured, at no cost, and outlines penalties for non-compliance or "Information Blocking".[26] Health information technology developers and health information exchanges and networks violate the prohibition if they engage in a practice that they know or should know is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; a health care provider violates the prohibition if it engages in a practice that it knows is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.[27] Thus, the digitisation of health information is a general requirement of the health care industry in the United States.

The Time Gap Between Technological Innovation and Rulemaking

A third distinct privacy compliance issue for digital health relates to the speed of technological innovation and the sluggishness of legislative and regulatory rulemaking.[28] Technological innovation happens fast and with increasing velocity.[29] By contrast, the development of the law, whether by legislation, common law judicial rulings or administrative rulemaking, evolves ponderously, often by design. In the case of the common law under the judicial systems in the United Kingdom and the United States, the law intentionally evolves slowly and with deliberate caution through holdings in specific lower court cases, which must then be approved by higher courts before becoming the law of the land. Administrative rulemaking is slowed by design through notice and comment periods required for proposed rules, which are then followed by final rules. Final rules typically then have a further period before requiring compliance. The process-oriented culture of bureaucracies slows down the rulemaking process further. It is not uncommon for rulemaking to take years from the enactment of legislation authorising regulation to the issuance of final regulations and still further to regulatory compliance and active enforcement of regulations.

Taking HIPAA as an example, it became law in 1996. As a statute, it provides little detail. Its implementing regulations were issued over the next 13 years by the U.S. Department of Health and Human Services ("HHS"), beginning on December 28, 2000, with the publication of the Privacy Rule and ending in March 2009 with the issuance of the Omnibus Rule. In between, HHS published the Security Rule in February 2003, the Enforcement Rule in February 2006, and the Breach Notification Rule in February 2009. Enforcement of HIPAA did not begin until early 2009,[30] with enforcement beginning in earnest later that year through HHS's Office of Civil Rights ("OCR").[31] In the digital health industry, by contrast, the period from 1996 to 2013 saw an entire, massive industry transformed by digital health. The period from 2013 to the present has seen equally if not greater changes created by digital health, notably the explosion of telehealth as a modality for delivering health care and the proliferation of B-C telehealth companies.

The slow pace of regulatory reforms compared to industry innovations creates a vacuum where the law struggles to adapt and conform to digital health-driven threats to the privacy and security of health information with clear and effective rules. As but one example, not until December 2024 have proposed amendments to the HIPAA Security Rule been proposed (not finalised) that would mandate the use of encryption and two-factor authentication in the storage and transmission of electronic health information. Compared with HIPAA, state privacy laws and regulations have evolved even more slowly. As of 2025, there are many states without any laws regulating health information with any specificity approaching the HIPAA Privacy Rule or Security Rule. Many states only have vague patient privacy laws and breach notification laws. Many have no cybersecurity laws. California, one of the few states with a health information security law, as opposed to a privacy or breach notification law, provides only a very general security requirement that: "Every provider of health care shall establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information. Every provider of health care shall reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use, or disclosure."[32] By comparison, the HIPAA Security Rule establishes a comprehensive set of security safeguards and implementation standards.[33]

Challenges to Administrative Rulemaking

Another impediment to cybersecurity and privacy laws in the United States keeping pace with technology stems from a recent fundamental challenge to federal rulemaking. Under the seminal U.S. Supreme Court case of *Chevron USA v. National Resources Defense Council*, the federal judiciary has, for 40 years, followed a practice of deferring to federal agencies' reasonable interpretations of, and rulemaking under, ambiguous federal laws.[34] On June 28, 2024, the Supreme Court overturned *Chevron* and the policy of deference to agency rulemaking. In overturning *Chevron*, moreover, the Supreme Court provided little guidance to lower courts deciding agency rulemaking challenges, thus inviting a chaotic regulatory environment with much less certainty and more variation as to the enforceability of federal regulations.[35] The demise of *Chevron* presages a more chaotic and uncertain ability of administrative agencies to regulate digital health and for the industry to have clear guidance regarding cybersecurity and data protection practices.[36]

Political Polarisation

As with any Internet-based business, digital health would benefit enormously from universal cybersecurity and privacy rules, or at least a greater movement towards the harmonisation of national and cross-border rules. The U.S. government has promoted such an approach through HIPAA, the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Office of the National Coordinator, the harmonisation of the Part 2 substance treatment rules with HIPAA, and the Cares Act, among other initiatives. The European Union and its adoption of the GDPR embodies a similar effort to create near-universal rules. Strong political currents, however, have arisen that threaten to derail efforts towards universal data protection standards. Although analysing such political trends is beyond the scope of this chapter, it is also impossible to ignore the impact of events such as Brexit, the rise of anti-establishment political movements in the United States and Europe, and a worldwide backlash against the comprehensive regulation of industries by national and continental administrative agencies (derided as the "administrative state"). The overturn of *Chevron* is a manifestation of rising scepticism towards federal regulation and a strong headwind against which federal efforts to establish national data protection and cybersecurity rules must contend.

Political polarisation promises to lead to greater gridlock at the federal and international level, as well as disparities in state-level regulation. Such effects are occurring with the protection of reproductive health information, with challenges to federal rules by states underway and conflicts between mega-states like California and Texas in the initial stages. As noted above, in April 2024, the OCR issued a Final Rule to protect reproductive health information under HIPAA.[37] The Texas attorney general sued in September 2024 to invalidate not only the 2024 Final Rule, but also elements of the HIPAA Privacy Rule that had previously gone unchallenged for over 20 years.[38] A separate suit by a Texas physician against the HIPAA Final Rule resulted in an injunction against the rule by a Texas Federal Court.[39] Meanwhile, California enacted a series of laws to protect abortion providers from states like Texas that have criminalised abortion. AB 352, discussed above regarding state protection of sensitive information, reacted to the efforts of Texas and other states recently prohibiting or greatly restricting abortion by exempting a provider of health care from liability for damages or from civil or enforcement actions relating to cooperating with, or providing medical information to, another state or a federal law enforcement agency.[40]

Digital health cannot avoid the repercussions of political conflict, touching as it does on issues of privacy, reproductive health and local autonomy. The stage is set for more conflict and chaos in the regulation of digital health by governments, leading to more difficulty establishing universal and consistent rules for data protection and cybersecurity.

"HIPAA Compliant" as the Beginning and End of Cybersecurity and Privacy

Because of the variances in health privacy and security laws based on jurisdiction and type of health information, privacy restrictions are complex and inconsistent. Digital health companies and customers with broad market reach are, therefore, required to comply with numerous discrete privacy requirements that reflect local customs and political processes, as well as higher sensitivities for different types of health information. For both the digital health developer and consumer, the privacy and security requirements become exceedingly complex and expensive to accommodate. Developers with limited capital to develop products and services nuanced enough to comply with local privacy and security requirements, and limited knowledge or resources to develop or acquire the requisite expertise for compliance, often produce products and services designed to meet national or continental privacy and security requirements while overlooking local requirements.

Within the digital health vendor community, few companies develop products and services to address the variances in the legal landscape for health information. The developers of digital health solutions and applications typically stop short of designing products with state and national privacy requirements in mind, despite, as discussed above, the existence of state privacy laws prior to HIPAA and the GDPR and despite the explicit allowance in HIPAA and the GDPR for state and national variation in privacy requirements. The prevalence of the legally meaningless term "HIPAA compliant" to digital health products connotes an industry mindset that treats U.S. health care privacy and security requirements as beginning and ending with HIPAA, even though such has never been the case. From a legal and compliance perspective, HIPAA and the GDPR are only the beginning points of legal analysis and compliance practices.

Adding to the challenge, in the fast-evolving world of digital health, where much innovation is driven by startup and early-stage private companies, capital is scarce. The failure of the digital health industry to develop products built to comply with local laws requiring greater privacy requirements than national/continental law reflects the primacy of research, development and marketing imperatives of vendors over compliance requirements of customers. The result from the competition for capital, driven in part by investor demands for capital efficiency, is that digital health technologies often lack the functionality to segment different categories of health information and facilitate compliance with disparate requirements for health information. The health care providers who are customers of digital health products, along with their patients, are left to navigate the privacy and security requirements of local law with digital health products developed to enable compliance with only national or continental requirements.

The segmentation of health information into different categories of sensitive information and jurisdiction, each often with its own specific restrictions on use and disclosure, ideally is addressed by digital health solutions recognising, properly categorising and allowing the ready segmentation of sensitive health information and health information subject to different jurisdictions. Thus, health information of a sensitive nature (*e.g.*, reproductive health, behavioural health) would be flagged by a digital health system and segmented into specific data silos as needed for compliance. The same recognition and segmentation would be performed for health information subject to different requirements based on geographical jurisdiction. Meeting the needs of health care providers for such segmentation, as well as for state/national-driven stronger privacy requirements, remains an important challenge for the digital health industry.

Industry Standards and Best Practices

One approach to the various challenges to digital health outlined above is to embed universal conceptual frameworks rather than rigid rules into laws and regulations. The HIPAA Security Rule and Breach Notification Rule adopt such an

approach to a limited extent by establishing implementation rules for encrypting and destroying electronic health information that reference standards issued by the National Institute of Standards and Technology ("NIST").[41] There is promise that more comprehensive reliance on standards issued by the Office of the National Coordinator for Health Information Technology, a part of HHS, will promote an approach to rulemaking that will be more adaptive to technological innovation within digital health.[42] Government standards, however, remain subject to the sluggishness of governmental bureaucracies and, in the wake of *Chevron*'s demise and increased political polarisation, are less authoritative.

Reliance on private industry standard-setting organisations may be a more promising way to close the gap between governmental laws and regulations and technological innovation. Within digital health, private certification programmes such as Service Organization Control 2 ("SOC 2"), International Organization for Standardization ("ISO") 27001, the Payment Card Industry ("PCI") Data Security Standards and the Health Information Trust Alliance ("HITRUST") have already done much to promote cybersecurity. The SOC 2 programme from the American Institute of Certified Public Accountants provides a report on information controls at a service organisation that can certify security, availability, processing integrity, confidentiality, and privacy standards. SOC 2 reports have become widely used by U.S. digital health companies to attest to their cybersecurity safeguards meeting industry best practice. ISO 27001, which has considerable overlap with the SOC 2 criteria, is popular internationally and was established by the ISO to fulfil a similar need.[43]

PCI Security Standards, developed and maintained by the PCI Security Standards Council, are specific to the protection of payment data throughout the payment lifecycle. The different PCI Standards support different stakeholders and functions within the payments industry. Some of the PCI Standards are intended for use by health care providers involved in payments, including digital health companies, to use within their own environments. PCI Standards support the implementation of secure practices, technologies, and processes within the organisation. The PCI Security Standards Council has developed other PCI Standards that digital health companies can use to demonstrate that their product or service was designed with security in mind and meets a defined set of security requirements.[44]

Finally, HITRUST is a private company that provides businesses a control framework designed to provide comprehensive guidelines on managing risk, particularly in the health care industry. HITRUST certification enables covered entities and their business associates to demonstrate compliance to HIPAA requirements based on a standardised framework. The HITRUST Common Security Framework assurance programme combines aspects from common security frameworks like ISO, NIST, PCI, and HIPAA.[45]

These and other private, industry-led certification and compliance programmes hold great potential for promoting cybersecurity in digital health. Nor are they limited to health care. A counterpart exists in the world of tax regulation, where tax rules reference general accounting and audit principles developed by the Financial Accounting Standards Board. These industry standards and accreditations can then be supplemented by more informal industry standards or best practices.[46] Such private programmes, however, would need to expand in reach and ambition to provide guidelines for complying with the privacy requirements of local laws and health information subcategories to fill the need created by the data protection challenges discussed above. As it stands now, the industry certification and compliance programmes are focused on cybersecurity standards and much less so than on privacy requirements.

Conclusion

Digital health would greatly benefit from universal and comprehensive rules governing the privacy and security of health information. Designing and using digital health products and services to comply with continental, national and state privacy and security rules, as well as rules governing specific categories of health information, is daunting, especially for digital health companies seeking to introduce their products and services simultaneously to a national or even worldwide customer base via the Internet. Adding in the challenges presented by cybercriminals, the pace of technological change, movements to promote direct patient access to health information, judicial challenges to administrative rulemaking and increased political polarisation, the compliance requirements become overwhelming and the possibility of regulatory relief remote.

The promotion of industry standards and best practices offers perhaps the most practical and realistic means of addressing the cybersecurity and privacy challenges of digital health through near-universal standards. Industry standards are currently far from universal, and rudimentary at best regarding privacy requirements, but they promise a more agile and uniform set of standards that digital health can coalesce around in the absence of cohesive government regulation. The enormous potential of digital health to improve health care requires the industry to adapt its culture and practices for a differentiated, nuanced and rapidly changing landscape of cybersecurity and privacy requirements, one that develops products and services adaptable to local requirements and differences among customers. The development of industry standards will hopefully play a vital role in that evolution.

Endnotes

1 *See* Cal. Civ. Code §§ 56 *et seq.* The Information Practices Act of 1977 (Cal. Civ. Code §§ 1798–1798.78) preceded CMIA and protects "personal information", including medical history that "identifies or describes an individual", but only when maintained by state agencies. Cal. Civ. Code §1798.3(a).

2 HIPAA, Pub. L. No. 104-191, 42 U.S.C. §§ 1320d–d(9). HIPAA became law on August 21, 1996.

3 Regulation (EU) 2016/679 of the European Parliament and Council for 27: GDPR.

4 U.S. Constitution, Article I, Section 8. Article I, Section 8 of the Constitution lists the powers of Congress, limiting them to those listed and those that are "necessary and proper" to carry them out. The states retain all other lawmaking powers. The Supremacy Clause in Article VI of the U.S. Constitution is the source of federal preemption.

5 45 C.F.R. Part 160, Subpart B of HIPAA, specifically § 160.203, outlines the general rule regarding preemption of state laws by HIPAA regulations and implements § 1178 of the Social Security Act, which is the statutory basis for HIPAA preemption. *See* https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html for HHS's detailed explanation of HIPAA's preemption rule.

6 GDPR Article 3 and Recitals 22–25.

7 Cal. Civ. Code §§ 1798.100–199 codify the CCPA and CPRA. The CPRA became effective January 1, 2023. Regulations under the California Privacy Protection Agency, created by the CPRA, published regulations implementing the CCPA and CPRA at Title 11 of the California Code of Regulations, §§ 7000–7600.

8 *See* Ieuan Jolly, *US Privacy and Data Security Law: Overview,* Practical Law Data Privacy & Cybersecurity (2024).

9 *See, e.g.*, 45 C.F.R. §§ 160.102, 160.105, 160.300, 164.304, & 164.501. Covered entities includes health insurers (including self-insured employer health plans), health care clearinghouses and those health care providers who transmit electronic health information in connection with a transaction for which HIPAA has established standards. The standard electronic transactions in which providers typically engage are health care claims, health plan eligibility inquiries, requests for referral authorisation, and health care claim status inquiries. *See generally*, 45 C.F.R. Part 162. Business associates are persons or entities who use protected health information to provide non-treatment services to covered entities. *See* 45 C.F.R. § 160.103 for definitions of "covered entities", "business associates" and "protected health information".

10 GDPR, Article 4(15), GDPR, Article 9(2), Recitals 51 and 56 (classifying as "sensitive" and subject to specific processing requirements the following personal data: (i) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; (ii) trade-union membership; (iii) genetic data, biometric data processed solely to identify a human being; (iv) health-related data; and (v) data concerning a person's sex life or sexual orientation).

11 The Part 2 statute (42 U.S.C. 290dd-2) protects "[r]ecords of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance use, disorder, education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States". Confidentiality protections help address concerns that discrimination and fear of prosecution deter people from entering treatment for SUD. The regulations are at 42 C.F.R. Part 2 (§§ 2.1–2.67).

12 42 C.F.R. §§ 164.501, 164.508(a)(2).

13 Public Law 110–233; 42 U.S.C. § 2000ff.

14 89 Fed. Reg. 32976 (April 26, 2024).

15 Cal. Welf. & Instit. Code §§ 5000, *et seq*. The Lanterman-Petris Short ("LPS") Act protects information and records created by certain mental health providers obtained in the course of providing health care services. Cal. Welf & Instit. Code § 5328, protects the health information of persons receiving mental health services, and Cal. Welf & Instit. Code § 4514 protects information of persons receiving services for developmental disabilities. The LPS Act went into effect in 1972, three years before the Part 2 Federal regulations.

16 Cal. Health & Saf. Code § 120975 protects HIV test results from unauthorised disclosure.

17 Health & Saf. Code § 120440(d).

18 Cal. Health & S C § 11845.5 (the identity and records of patients in alcohol or drug abuse programmes must be kept confidential, except in limited specified circumstances). In addition, California Medicaid (*i.e.*, Medi-Cal) records are protected by Cal. Welf. & Instit. Code §14100.2(a) and 22 Cal. Code Regs §51009. Records of public officers and agencies concerning individuals participating in other public social services for which California receives grants-in-aid from the federal government are similarly protected by Cal. Welf. & Instit. Code § 10850(a).

19 Cal. Civil Code § 56.101(c).

20 Cal. Civil Code §§ 56.05(i) (revised definition of medical information), (p) (definition of "reproductive or sexual health application information"), (q) (definition of "reproductive or sexual health digital service") and 56.06 (subjecting reproductive or sexual health apps and websites to CMIA).

21 The HIPAA Transaction Rule, for example, establishes a set of standards to govern the electronic exchange of patient health information, based on electronic data interchange standards. 45 C.F.R. Part 162. The HIPAA Security Rule, as noted above, establishes security requirements only for electronic protected health information. 45 C.F.R. § 164.302.

22 *See* 45 C.F.R. §§ 160.406 (addressing how HIPAA violations are counted) and 160.408(a)(1) (establishing the number of individuals affected as a factor in determining HIPAA civil penalties).

23 *See* Paul M., Maglaras L., Ferrag M.A., Al Momani I., *Digitization of Healthcare Sector: A Study on Privacy and Security Concerns. ICT Express.* 2023 doi: 10.1016/j.icte.2023.02.007 for an excellent analysis of the increased risks of data breaches in a digital *versus* paper world.

24 *See, e.g., Sharif M.H.U., Mohammed M.A. A literature review of financial losses statistics for cyber security and future trend. World J. Adv. Res. Rev.* 2022; 15:138–156. doi: 10.30574/wjarr.2022.15.1.0573.

25 *See* Saqib Saeed, *Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations* (2023) at https://pmc.ncbi.nlm.nih.gov/articles/PMC10422504 for a systematic review of the scholarship the digital transformation and its cybersecurity implications, including the adaptation of cybercriminals to the digital world.

26 Public Law 114-255,130 Stat 1033; 45 C.F.R. Parts 170 and 171.

27 45 C.F.R. § 171.103.

28 *See* Adam Thierer, "The Pacing Problem and the Future of Technology Regulation", (August 8, 2018) at https://www.mercatus.org/economic-insights/expert-commentary/pacing-problem-and-future-technology-regulation, citing Wendell Wallach, *A Dangerous Master: How to Keep Technology from Slipping beyond Our Control* (2015) and other scholars on this phenomenon, which Thierer dubs "the Pacing Problem".

29 *See, e.g.*, The World Economic Forum, Our World in Data republished at https://www.weforum.org/stories/2023/02/this-timeline-charts-the-fast-pace-of-tech-transformation-across-centuries (Feb. 27, 2023).

30 The Privacy Rule, 45 C.F.R. §§ 160.101 and 164.501 *et seq.*, became effective on April 14, 2001, with a compliance date of April 14, 2003, for most covered entities. The Omnibus Rule implemented provisions of the HITECH Act that strengthened HIPAA's privacy and security protections. The Security Rule, 45 C.F.R. §§ 160.101 and 164.302 *et seq.*, had a compliance date for most covered entities of April 20, 2005. The Enforcement Rule gave HHS the authority to investigate and penalise HIPAA-regulated entities for non-compliance. The HITECH Act established four categories of HIPAA violations and set penalty amounts and broadened the definition of the law to digital health vendors through an expansion of the term "business associate" to include entities, such as Internet hosting or cloud companies, a key cornerstone of the digital health revolution. On January 16, 2009, HHS entered into its first settlement for HIPAA violations, levying a $2.25 million fine against CVS Pharmacy for improperly dumping patient health records.

31 The OCR of the HHS is responsible for enforcing HIPAA. OCR became responsible for enforcing the Security Rule on July 27, 2009. *See* https://www.hipaajournal.com/hipaa-history for an excellent history of HIPAA.

32 Cal. Health & Saf. Code § 1280.18(a).

33 45 C.F.R. §§ 164.302–164.318.

34 467 U.S. 837 (1984).

35 *Loper Bright Enterprises v. Raimondo*, 603 U.S. 369 (2024).

36 The Fifth Circuit Court of Appeals ruling in *University of Texas M.D. Anderson Cancer Center v. U.S. Department of Health and Human Services,* 985 F.3d 472, 478 (5th Cir. 2021), holding that a covered entity can meet its encryption obligations under the HIPAA Security

Rule by implementing a mechanism to do so, without regard for the effectiveness of the implementation of that mechanism, motivated the recent HIPAA proposed rule, "HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information", 90 Fed. Reg. 898 (Jan. 6, 2025).

37 89 Fed. Reg. 32976 (April 26, 2024).

38 *State of Texas v. United States Department of Health and Human Services et al.*, Case 5:24-cv-00204-H (Sept. 4, 2024) (Paragraphs 24—35 state Texas's objections to the Privacy Rule as exceeding HHS's authority, rendering it invalid).

39 *Purl v. United States Department of Health and Human Services*, 2:24-CV-228-Z (N.D. Tex. Dec. 22, 2024).

40 Cal. Civil Code § 56.108. *See also* https://www.gov.ca.gov/2023/09/27/california-expands-access-and-protections-for-reproductive-health-care for a list and summary of the recent California reproductive rights legislation.

41 Specifically, NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*; NIST Special Publication 800-88 *Guidelines for Media Sanitation*; Federal Information Processing Standards (FIPS) 140-2; NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; NIST Special Publication 800-77, *Guide to IPsec VPNs*; and NIST Special Publication 800-113, *Guide to SSL VPNs as cited in OCR's* "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable" (2009).

42 *See* https://www.healthit.gov/topic/about-astponc

43 *See* https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2 and https://www.iso.org/standard/27001

44 *See* https://www.pcisecuritystandards.org

45 *See* https://hitrustalliance.net

46 *See* https://www.fasb.org

Stephen K. Phillips's practice includes facilitating advancements in health care information technology and effectively addressing corresponding challenges with patient privacy and data security. Also handling a wide range of business and compliance matters for providers and technology vendors, Steve has a depth of knowledge and diversity of experience to deliver reliable, actionable, and accurate counsel efficiently. With both private practice and in-house experience, Steve counsels clients on all transactional, operational, or regulatory issues that intersect with health care technology and patient privacy. He drafts and negotiates health care technology agreements of all kinds, including those involving SaaS products, data sharing agreements, software licences, business associate agreements, HIE licensing, and participation and data sharing agreements and policies.

Steve plays a critical role in helping providers protect patient privacy, secure data and systems from evolving threats, and navigate an ever-changing regulatory and compliance landscape. His work includes drafting internal privacy and security policies and programmes, breach investigation, remediation, and reporting, and addressing related data compliance issues. His compliance counselling also covers fraud and abuse investigations and self-disclosures, telemedicine and web-based service design, and medical, dental, and other professional practice act restrictions.

In transactional matters, Steve leverages his combination of health care and technology experience to structure arrangements between technology and health care providers that address corporate practice, fraud and abuse, and other health care licensing compliance requirements. He provides counsel on mergers, acquisitions, strategic partnerships, outsourcing agreements, and corporate governance matters that help his clients achieve their business objectives and facilitate continuing innovation in health care delivery.

Before joining HLB, Steve was the general counsel and compliance programme chair for Neoforma, a public health care supply chain management outsourcer, and the chief operating officer and general counsel for eCliniq, a provider of web-based clinical solutions for heart care physicians.

Hooper, Lundy & Bookman, P.C.
44 Montgomery Street, Suite 3500
San Francisco, CA 94104
USA

Tel: +1 415 875 8508
Email: sphillips@hooperlundy.com
LinkedIn: www.linkedin.com/in/steve-phillips-848694

Alicia Macklin is a trusted advisor to a range of inpatient and outpatient behavioural health care providers, along with hospitals and health systems. She has counselled many of California's hospitals on unsettled areas of law, with an emphasis on compliance with the Emergency Medical Treatment and Labor Act (EMTALA). A former litigator with a Master of Public Health from UCLA's Fielding School of Public Health, Alicia brings her unique perspective and experience to her clients' most nuanced regulatory problems.

Alicia's work with behavioural health providers includes advising on licensing and accreditation, Medicare and Medi-Cal reimbursement, federal and state privacy and confidentiality requirements, and operational issues. She also helps California providers navigate voluntary and involuntary treatment under the Lanterman-Petris-Short Act (LPS Act). In addition to providing guidance and counsel on current legal issues, Alicia also provides her clients with insights into broader behavioural health policy trends that could affect them in the future, including both federal and state-level initiatives to reform behavioural health care.

For her hospital and health system clients, Alicia similarly advises on a broad range of compliance, reimbursement, and operational issues, including those involving behavioural health treatment. She specialises in EMTALA, and her work with hospitals in this space involves reviewing and revising EMTALA policies, providing in-service education for physicians and staff, managing investigations and surveys, and advising on EMTALA's intersection with state laws, including state involuntary civil commitment laws.

Alicia has a deep commitment to issues affecting health equity and public health education. She has studied, written, and presented in this area for nearly a decade, first as a student earning her Master of Public Health, and now as a practising health care attorney and lecturer at the University of California, Los Angeles Fielding School of Public Health, where she co-teaches Legal Environment of Health Services Management.

Hooper, Lundy & Bookman, P.C.
1875 Century Park East, Suite 1600
Los Angeles, CA 90067
USA

Tel: +1 310 551 8161
Email: amacklin@hooperlundy.com
LinkedIn: www.linkedin.com/in/aliciamacklin

Argentina

Diego Fernández

Martín J. Mosteirin

Marval O'Farrell Mairal

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no formal or legal definition of digital health in Argentina. Nevertheless, it can be defined as the use of information and communication technologies (ICT) in healthcare for the purposes of prevention, diagnosis, treatment and monitoring of diseases (according to the WHO definition).

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Recently, there has been growth in the development and implementation of different health technologies such as apps, wearables, telemedicine, electronic health records and electronic prescription platforms across the healthcare industry.

1.3 What is the digital health market size for your jurisdiction?

According to Statista,[1] the revenue in the digital health market is projected to reach USD1.129b in 2025 and is expected to show an annual growth rate (CAGR 2025–2029) of 7.47%, resulting in a projected market volume of USD1.506b by 2029.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

According to Statista, as of January 2025, the five largest digital health companies in Argentina are Fitbit, Calm, Polar, Withings and Meditopia.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

This information is not publicly available.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The National Ministry of Health (MoH) is the main health authority in Argentina. The MoH is responsible for promoting the progressive implementation of electronic or digital prescriptions and of healthcare tele-assistance platforms, and to regulate the interoperability of such platforms (Decree 98/23, which regulates Law 27,553 (Law on Electronic Prescriptions).

The National Agency of Medicines, Food and Medical Technology (ANMAT), created by Decree 1,490/92 (amended by Decree 1,271/13), is an independent agency responsible for regulating the safety and efficacy of medical devices, including those with digital technologies.

In addition, each province has its own health authority that works jointly with ANMAT and can issue regulations.

Lastly, the Agency of Access to Public Information (AAIP), Argentina's data protection authority, oversees personal data compliance (although it does not specifically oversee nor enforce regulatory schemes related to digital health). The AAIP is entitled to enforce the Data Protection Regime (as defined in question 2.2), which applies to any digital health matter, as long as it involves the processing of personal data.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

The Argentine sanitary regulatory framework is fragmented and divided according to the services or product categories that are related to digital health, such as:

- Telemedicine: At the Federal level, Regulatory Decree 98/23 of Law 27,553 on Electronic or Digital Prescriptions sets forth the following definition of "tele-assistance": "*Provision of remote healthcare services through information and communication technologies in a synchronous or asynchronous manner (...), by a healthcare team, for the promotion, prevention, diagnosis, treatment and rehabilitation (...).*"

- Electronic prescription: Since July 1, 2024, the use of electronic prescriptions and/or digital prescriptions is mandatory in Argentina for prescribing: (i) medications; (ii) medical studies; (iii) procedures; and (iv) any other indications that healthcare professionals (HCPs) consider pertinent for their patients (Law on Electronic Prescriptions, as amended by Decree 70/23).
  Additionally, MoH Regulation 1,959/24 created the National Registry of Digital Health Platforms (ReNaPDiS) and the Registry of Electronic Prescriptions, where information systems and digital health platforms must be registered.
- E-commerce of medicinal products: The sale and dispensing of prescription medicinal products must be carried out from the pharmacy in the presence of a responsible pharmacist and their sale and delivery to the patient may be arranged through electronic channels determined by the pharmacy (Regulatory Decree 7,123/68 of Law 17,565, as amended by Decrees 345/24, and 1,024/24). This latter mechanism is innovative and will allow a progressive implementation of the electronic channels at a federal level.
  Additionally, each province can issue its own regulations for pharmacies, which may differ from the modifications in Law 17,565 and its Regulatory Decree 7,123/68.
- Digital licence for HCPs in the City of Buenos Aires: the digital health professional licence replaced the physical professional licence, thus becoming the only mandatory professional licence (MoH Regulation 3,320/2024, as amended by MoH Regulation 4,827/24).

The protection of personal data is governed by the Personal Data Protection Law 25,326 (DPL), its Regulatory Decree 1558/2001, Convention 108 for the Protection of Individuals with respect to Automatic Processing of Personal Data (ratified by Law 27,483), its Amending Protocol (approved by Argentine Law 27,699), also known as "Convention 108+"[2] and by the complementary rules issued by the AAIP (collectively, the "Data Protection Regime").

Lastly, there is no general artificial intelligence (AI) regulation yet, nor specific regulation for AI and digital health matters. Although certain bills have been submitted to Congress in the last years, Argentina lacks a dedicated legal framework for AI. Nevertheless, general regulations – covering areas such as labour, consumer rights, intellectual property (IP), and data protection – provide a foundational framework for the use of AI tools within the country.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

One of the key and emerging areas in Argentina related to digital health is the digitalisation of the healthcare system. In 2023, the MoH created a unified digital medical record system that is expected to significantly improve the accessibility, accuracy, and efficiency of patient information. However, the new administration has not issued any regulation for its implementation.

In addition, as mentioned above, the MoH also stipulated that authorised HCPs can issue electronic or digital prescriptions and treat patients through telemedicine platforms. This is a major step forward for digital health, as patients can now access healthcare services from their homes, which is very beneficial as in Argentina there are many rural or remote areas.

From a data protection standpoint, regardless of the industry, there is a tendency for the AAIP to sanction particularly the following behaviours: (i) processing personal data in an unlawful manner or in disregard of the principles and guarantees set forth in the Data Protection Regime; (ii) failure to comply in due time and form with the request of the data subjects for the rights of access, rectification or suppression, when legally applicable; and (iii) failure to comply with the duty of confidentiality and security.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

Software as a medical device (SaMD) is mainly governed by ANMAT Regulation 64/2025, which defines medical devices as *"[a]ny instrument, device, equipment, implant, in vitro diagnostic product, software, material or other article, intended by the manufacturer to be used, alone or in combination, in human beings, for any of the following specific medical purposes, when the main intended action is not achieved by any pharmacological, immunological or metabolic means in the human body, but may contribute to its intended action: (i) diagnosis, monitoring, treatment or relief of a disease; (ii) diagnosis, monitoring, treatment or repair of an injury or disability; (iii) investigation, replacement or modification of anatomy, physiological or pathological process or state; (iv) sustaining or supporting life; (v) monitoring or supporting conception; and (vi) obtaining information by in vitro examination of specimens from the human body, including organ and tissue donations"* (Section 6, Appendix I, Annex I).

If software is considered a medical device, the following regulatory framework applies:

- Law 16,463 (Law on Medicines) and its Complementary Decree 9,763/64.
- ANMAT Regulations: No. 2,319/02 (as amended by ANMAT Regulation 3,433/04); No. 6,052/13 (as amended by ANMAT Regulation 7,802/21); No. 3,266/13; No. 4,980/05; No. 9,688/19 (as amended by ANMAT Regulation 8,671/21); No. 2,096/22; No. 8,194/23; No. 11,419/24; No. 11,467/24; and No. 64/25.
- MoH Regulation 2,175/13 (as amended by ANMAT Regulation 2,303/14).

Additionally, members of CADIEM (Argentine Chamber of Medical Devices) use its Code of Ethics (CADIEM Code) as a guideline for cases where regulations are ambiguous (mainly, regarding the interaction between medical devices companies and HCPs).

From a data privacy perspective, the Data Protection Regime applies to the processing of personal data (including sensitive data) through SaMD, which may also entail automated decision-making.

Lastly, there are no specific IP regulations regarding SaMD; however, general copyright regulations – in respect of the corresponding software – apply to its development and use.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

From a sanitary regulatory perspective, there are no specific regulations applicable to AI/machine learning (ML)-powered digital health devices or software solutions and their approval for clinical use. If devices or software solutions are classified as medical devices, general provisions governing medical devices will apply.

Given that Argentina's digital regulatory landscape is evolving, it is likely that special regulations will be developed in the future.

Lastly, regarding data privacy matters, IP and automated decision-making, please refer to our answer to question 2.4.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

ANMAT is committed to the development of regulatory principles for AI-based medical devices and is currently participating in an International Medical Device Regulators Forum's project regarding AI medical devices.[3]

ANMAT has submitted to public opinion a bill that aims to provide technical considerations and regulatory aspects related to the design and manufacturing processes of AI- and ML-based software to all actors involved. In response, stakeholders have been expressing their opinions regarding the bill.[4]

Regarding the AAIP, we note a tendency to issue broad and general recommendations on the use of AI, without currently focusing on a particular industry. In this context, the AAIP has introduced some resolutions to promote the responsible and ethical use of AI. The AAIP issued Resolution 161/2023,[5] which established the Program for Transparency and Personal Data Protection in AI Use (Program). Recently, and within the context of the Program, the AAIP also issued the "Guide for Public and Private Entities on Transparency and Personal Data Protection in Responsible AI Use" (AI Guide), providing further guidance for organisations navigating AI implementation.[6] It is expected for the AAIP to have a relevant role in the use or deployment of AI systems in the future, and therefore it may issue certain industry-specific regulations.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Although there are no regulations specifically regarding AI/ML-based digital health solutions, as previously mentioned, the AAIP has issued the AI Guide, which establishes several recommendations for AI use and development, including that the developed models should be trained with accurate, valid and exact data, to take accurate decisions and outcomes.

From a sanitary regulatory perspective, this matter is not regulated yet by the health authority in Argentina.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Argentina is a federal country that is divided into 23 provinces and the City of Buenos Aires. There are a variety of (federal, provincial, and municipal) laws and regulations in diverse fields such as electronic prescriptions, e-commerce of medicines and medical devices, regulation of the medical profession, as well as medicines and medical devices. Health is considered to be a social right with constitutional recognition; thus, Argentine legislation regulating medicines and medical devices primarily serves to protect public health.

Thus, both federal and local regulations must be considered when analysing the requirements that apply to each digital health product and solution. For example, while National Law 27,553 established the mandatory use of electronic and/or digital prescriptions, the City of Buenos Aires Law 6,439 allows the coexistence of paper and electronic prescriptions in such jurisdiction.

Most provisions of the DPL are of public interest and apply nationwide. However, provinces are permitted to establish their own regulations on specific matters, such as the creation of their own data protection authority, establish sanctions and regulate data protection procedures.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Please refer to our answers to questions 2.1 and 2.2.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

From a data privacy and cybersecurity perspective, there are no specific regulations for digital health technologies. Therefore, the processing of personal data through such technologies must follow the general existing regulations.

- **Telemedicine/Virtual Care**
  Law 27,553 sets forth the possibility of using tele-assistance platforms in health. Please refer to the definition of "tele-assistance" in question 2.2 above. Similarly, Article 2 *bis* of Law 17,132 enables telecare for the practice of medicine, dentistry and their collaborative activities. Moreover, MoH Regulation 3,316/23 approved the Guidelines for the Organisation and Operation of Teleconsultation, whose objective is to "*contribute to improving the accessibility, equity, efficacy, effectiveness and efficiency of health services, in order to promote an adequate level of quality of care and patient safety (…)*" (Annex, Section 1).
  One of the main issues is regarding the implementation of tele-assistance platforms and services for vulnerable populations and those remote areas that may have connectivity issues. It should be further assessed whether the anew administration will enforce or take measures to promote access to digital health.
  From a data privacy perspective, some of the core legal issues would include compliance with patient confidentiality obligations, cybersecurity matters, and compliance with the Data Protection Regime, which would entail ensuring, among others: (i) the existence of a lawful basis for processing (likely to be consent); (ii) implementation of adequate safeguards for the processing of sensitive data; (iii) compliance with the duty of information owed to the data subjects regarding the processing of their personal data; and (iv) implementation of necessary security and confidentiality measures.
- **Robotics**
  Depending on the intended use, robotic technologies may be classified as medical devices. This should be assessed on a case-by-case basis.
  With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above.

- **Wearables**
  Depending on the intended use, wearables may be subject to the medical devices' regulatory framework. Wearables may also be governed by consumer product legislation. This should be assessed on a case-by-case basis.
  With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above.
- **Virtual Assistants (e.g. Alexa)**
  If a virtual assistant provides diagnostic, therapeutic, preventive, contraceptive or rehabilitation advice, it may be classified as a medical device and will be subject to the regulatory framework described in our answer to question 2.4. The main issues are connected to liability claims, if the virtual assistant has a role in the decision-making process in which there is an adverse health outcome.
  With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above.
- **Mobile Apps**
  According to Annex XI of ANMAT Regulation 9,688/19, mobile applications (apps) are considered software as medical devices when they meet the definition provided by said regulation (please see next point for further reference). This should be assessed on a case-by-case basis.
  With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above.
  Regarding IP rights, general regulations apply to the development and use of mobile apps.
- **Software as a Medical Device**
  Although ANMAT provides some rules for the classification and registration of SaMD, we suggest seeking regulatory advice to properly assess on such classification.
  With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above, and in our answer to question 2.4.
  Regarding IP rights, please refer to the issues mentioned in the Mobile Apps section above.
- **Clinical Decision Support Software**
  Software intended to support clinical decision-making and treatment may be regulated as a medical device if it meets the definitions provided by ANMAT Regulation 64/25 and ANMAT Regulation 9,688/19. The main issues are connected to liability claims, if the virtual assistant has a role in the decision-making process in which there is an adverse health outcome.
  With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above, and in our answer to question 2.4.
  Regarding IP rights, please refer to the issues mentioned in the Mobile Apps section above.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  Software that is powered by AI/ML and that meet the definition of SaMD will be governed by the regulatory framework applicable to SaMD.
  Regarding tele-assistance platforms, Decree 98/23 set forth limitations to the use of AI. In this sense, AI-powered digital health solutions can only be used as a support of professional decision-making of HCPs, and AI should be always supervised by HCPs.
  With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above, and in our answer to question 2.4.
  Regarding IP rights, please refer to the issues mentioned in the Mobile Apps section above.
- **IoT (Internet of Things) and Connected Devices**
  With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above.
- **3D Printing/Bioprinting**
  Bioprinting is not regulated yet in Argentina.
  With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above, and in our answer to question 2.4.
  Regarding IP rights, please refer to the issues mentioned in the Mobile Apps section above.
- **Digital Therapeutics**
  Digital therapeutics may be subject to the medical devices' regulatory framework if it meets the definition of medical device.
  With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above.
- **Digital Diagnostics**
  Digital diagnostics may be classified as medical devices as they meet the definition provided by ANMAT Regulation 64/25. The main issues are connected to liability claims, if the digital diagnostics are used in the decision-making process in which there is an adverse health outcome.
  With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above.
- **Electronic Medical Record Management Solutions**
  Law 27,706 and Decree 393/23 introduced electronic health records to ensure the access to data and documents by both patients and HCPs.
  With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above.
- **Big Data Analytics**
  Currently, there are no regulatory guidelines.
  With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Currently, there are no regulatory guidelines. With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above.
- **Natural Language Processing**
  Natural language processing has not yet been discussed by the sanitary authorities in Argentina. However, depending on the intended use, it may be subject to the medical devices' regulatory framework.
  With regard to data privacy and cybersecurity, please refer to the issues mentioned in the Telemedicine/Virtual Care section above.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

According to MoH Regulation 1,959/24, the following information systems and digital platforms linked to digital health must be registered with the ReNaPDiS: (i) prescription platforms and systems; (ii) digital prescription repositories; (iii) digital dictionaries of medicines; (iv) telecare systems; (v) medicine validation systems; (vi) pharmacy administration systems; and (vii) any other system involved in the processes covered by digital health. Furthermore, individuals responsible for such platforms and/or systems are obliged to register

with the ReNaPDiS, in accordance with the technical requirements issued by the applicable authority.

Additionally, platforms and/or prescription systems using electronic and/or digital prescriptions, medicines, study orders, practices and/or any other indication must be registered with the Registry of Electronic Prescriptions, included in the ReNaPDiS. Such platforms and/or prescription systems must allow access to the prescriptions stored to all those pharmacies in the national territory, authorised by the competent sanitary authority, where the patient requires their dispense.

Lastly, data protection regulations and, specifically those governing collecting, processing and transferring sensitive data (*i.e.*, health-related data) must be followed.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

As previously explained, in Argentina there are no regulations specifically regarding healthcare technologies, but the processing of personal data is generally governed by the Data Protection Regime. Under this regime, the following issues must be considered when processing personal data: (i) complying with the duty of information owed to the data subjects regarding the processing of their personal data; (ii) following principles of transparency, lawfulness and fairness, minimisation, purpose limitation, and proportionality; (iii) registering databases before the AAIP registry, as well as the data controllers; (iv) establishing a lawful period of data retention; (v) ensuring data processors' compliance with their obligations; (vi) having a lawful basis for data processing (including, where applicable, obtaining data subjects' consent to enable data controllers to process their personal data); (vii) implementing adequate safeguards for the processing of sensitive personal data (as further described below); (viii) implementing safeguards for the international data transfer to non-adequate countries; (ix) ensuring data subjects' rights of access, rectification and elimination of their personal data; (x) complying with duty of confidentiality; and (xi) implementing security measures.

Furthermore, the platforms through which tele-assistance is managed or prescriptions are carried out must comply with the following requirements as set forth in Decree 98/23, which regulates the Law on Electronic Prescriptions:

(i) Be appointed in Argentina as a data processor, ensuring to do so in a confidential and secure manner and complying with the applicable regulatory requirements.
(ii) Provide mechanisms that safeguard the credentials and access of the stakeholders involved, to guarantee the security, privacy, purpose, timeliness, veracity and inviolability of the data.
(iii) Host platform servers in a secure location, in accordance with applicable practice and regulatory requirements, establishing safeguards to preserve the security, availability, inviolability, inalterability and confidentiality of personal data.
(iv) Comply with the provisions of Law 25,326 (Law on Personal Data Protection) and guarantee users of the healthcare system access to their registered data, as well as its update, in accordance with Law 26,529 (Law on Patient's Rights). In this sense, mechanisms for safeguarding or backing up personal data must be ensured for the time set forth in the applicable regulations.
(v) Ensure timely access to health data, guaranteeing its privacy, purpose, integrity and confidentiality.
(vi) Adopt all measures necessary to guarantee the security, availability, inviolability, inalterability and confidentiality of personal data to prevent their adulteration, loss, or unauthorised consultation or processing, as well as to detect deviations of information.
(vii) Ensure its technology meet the standards for health information systems set forth by the regulatory authority and the security and cybersecurity protocols for the inviolability of the information. For the use of simultaneous audio and video transmission, up-to-date systems with encryption and encoding that ensure the highest security standards must be implemented.
(viii) Those responsible for health information systems must establish mechanisms that ensure users' compliance with the regulations on the protection of personal data in electronic communication and privacy in the telecommunications sector, as well as with the competent authorities on e-commerce, consumer protection, crimes against public health and cybersecurity.
(ix) Owners of such platforms must comply with the regulatory framework applicable to the medical profession and to pharmacy.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

As indicated in question 2.8, most of the DPL's provisions are of a public interest, meaning they cannot be overridden by provinces in Argentina (with certain exceptions). In this regard, obligations related to sensitive data (which include personal heath data) apply nationwide.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The considerations explained above do not change either depending on the nature of the entities or the nature of the data, as the DPL applies equally to public and private entities.

4.4 How do the regulations define the scope of personal health data use?

The DPL defines personal health data as sensitive data and provides for stricter obligations for the data controller to comply with.

When processing sensitive data, data controllers should abide by the following guidelines: (i) providing personal sensitive data cannot be mandatory; (ii) data subjects should be informed about and specifically consent to the processing of their sensitive data; and (iii) data controllers should adopt the recommended security measures with respect to sensitive data, which are listed in DPA Regulation 47/18.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

Under the Data Protection Regime, data controllers may have to enter into different contractual provisions based on the parties involved in the processing of personal data. On the one hand, data controllers must ensure compliance with their employee's duty of confidentiality. On the other hand, when engaging data processors, data controller must enter into data processing agreements, which will have to follow the provisions of section 25 of the DPL. The sharing of personal data with other data controllers does not require the implementation of specific contractual provisions, although it is customary for data controllers in Argentina to do so. Lastly, if personal data is transferred to non-adequate jurisdictions, then data controllers must implement adequate safeguards, which include the implementation of standard contractual clauses (SCCs) and binding corporate rules (BCRs).

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Regarding personal data inaccuracy, the DPL establishes the obligation for data controllers to inform the data subjects of the consequences of providing inaccurate data, to promote the accuracy of IT.

Moreover, the DPL establishes certain principles such as transparency, minimisation, purpose limitation, and proportionality, which root against bias and discrimination.

In addition, the AAIP's AI Guide also establishes anti-discrimination principles for the use and development of AI systems.

Lastly, the Anti-discrimination Law 23,592 protects people from discrimination based on race, gender, social status, religion and political opinions, among others.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

Please refer to our answer to question 4.1.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The DPL establishes as a general principle of data sharing/transfer that personal data subject to processing may only be assigned to a new data controller for the fulfilment of purposes directly related to the legitimate interest of the assignor and the assignee, with the prior consent of the data subject (with certain exceptions), must be informed of the purpose of the assignment and provided with information that identifies the assignee or with elements that make it possible to do so. The DPL further establishes that the data subject's consent will not be necessary when the assignment concerns personal data related to health, and such assignment is necessary for public health reasons, emergency or for the performance of epidemiological studies, as long as the identity of the data subjects is preserved by means of appropriate dissociation mechanisms.

Moreover, when transferring personal data to a data processor, the parties must implement data processing agreements with such processors, which should establish that: (i) personal data cannot be used or applied to purposes other than those provided for in the contract for the provision of processing services; (ii) personal data cannot be transferred to other third parties, not even for storage purposes; (iii) the data processor shall act only on instructions from the data controller; (iv) the data processor shall comply with the obligations relating to the security and confidentiality of personal data provided for in the DPL; and (v) upon completion of the contractual performance, or upon termination of the contract for the provision of processing services for any cause or reason, data processors must destroy or delete the personal data processed.

Furthermore, in case of transferring personal data to non-adequate jurisdictions – according to the list approved by the DPA – such transfers must be based, at least, in one of the following safeguards: (i) the data subject's consent to the transfer; (ii) contractual clauses (as international data transfer agreements); or (iii) systems of self-regulation (as BCRs).

Lastly, Decree 98/23, which regulates the Law on Electronic Prescriptions, provided that in the event of a transfer, the recipient must comply with the same obligations lying on the individual who originated it. In addition, as dissociated health data is not considered sensitive data, it may be used for scientific research or for statistical, epidemiological or health policy purposes.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Please refer to our answer to question 4.2.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Please refer to our answer to question 4.3.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Please refer to our answer to question 5.1.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Please refer to our answer to question 5.1.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Under the Argentine Patents Law 24,481 (Patents Law), patents are granted for products or processes that meet patentability

requirements, *i.e.*: novelty; inventive step; and industrial applicability. While there are no specific provisions dealing with digital health technologies, section 6 of the Patents Law specifically excludes from patentability methods of treatment and methods of diagnosis applicable to the human body.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

The Argentine IP Law 11,723 (IP Law), which is of general application to all copyrightable works, protects scientific, literary and artistic works and software. As a general principle, the IP Law provides copyrights originally vest in the author. As an exception, the IP Law expressly provides that any software developed by employees belongs to the employer, without the need of executing an assignment, if employees were specifically hired to develop such software. If works are developed in circumstances that do not involve employment relationships, like those developed by contractors, the proprietary rights over such works belong to their authors, unless otherwise agreed by the parties.

Although there are no specific provisions regarding copyright protection for digital health technologies, depending on the digital health technology, it could be protected as a scientific work, as software, or as both, and thus, the general provisions outlined above would apply.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

The Confidentiality Law 24,766 establishes that any person may prevent information that is legitimately under their control from being disclosed to third parties or from being acquired or used by third parties without their consent, as long as such information meets the following conditions: (i) it is secret in the sense that it is not, as a whole or in part, known or easily accessible to persons in that area of expertise/practice; (ii) it has a commercial value because it is secret; and (iii) the person in its control took reasonable measures to keep it secret.

Moreover, it provides that those persons who, by means of their labour or business relationship, have access to information that may be considered trade secrets or is intended to be kept confidential, must refrain from using and disclosing it without legal basis or the consent of the owner of such information. The breach of this confidentiality obligation constitutes a criminal offence according to Section 156 of the Criminal Code.

Appropriate non-disclosure measures must be implemented to protect such information (*i.e.*, marking information as trade secrets, implementing IT security measures, particularly access restriction, and concluding NDAs).

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Since there are no specific regulations applicable to academic technology transfers, the general regulations apply. As per the Transfer of Technology Act 22,426 and Argentine Patent and Trademark Office (AR PTO)'s Resolution P-117/14, registration of technology transfer agreements is handled by the Transfer of Technology Department at the AR PTO.

Furthermore, regarding academic transfers, in Argentina, the National Scientific and Technical Research Council of Argentina (CONICET) is the main government agency that promotes science and technology in the jurisdiction. Thus, its agreements with third parties and any of its decisions assigning its IP rights to third parties must be made following certain legal and formal procedures and under reasonable commercial conditions.

Applicable regulations to employees of CONICET and other research institutions determine that the result of their activities will be owned:

(a) solely by CONICET, when such results arise from CONICET's activity only;
(b) jointly by CONICET and a participating entity, when such results arise from an agreement between CONICET and said entity and co-ownership was agreed upon, or when participating employees are dependent from both CONICET and the relevant entity; or
(c) solely by third parties, when such results arise from specific agreements wherein ownership by a third party was agreed upon.

CONICET shall have the right to receive royalties, a lump sum, or shares, or any combination thereof, when such results are exploited or an agreement is signed, subject to the conditions of the relevant agreement.

Employees will have the right to: (i) be recognised as the inventors of the patented invention on the Letters Patent issued in favour of the institutions; and (ii) receive a share of CONICET's economic benefits arising from patent exploitation according to CONICET internal regulations.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Please refer to our answer to question 6.2.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

Under current regulations, only natural persons can be listed as inventors. Therefore, an AI device cannot be named as an inventor of a patent in our jurisdiction.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

In the case of patents, there are no rules that regulate government-funded inventions. Patent rights belong to the patent holder.

Moreover, both the Patents Law and the Labor Contract Law regulate employee inventions through public law provisions, which cannot be waived by the parties. As per these provisions, in principle, inventions developed by employees hired to invent are owned by the employer, while inventions developed by employees outside their scope of work might be owned by the employee.

With regard to copyrights, please refer to our answer to question 6.4.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

As mentioned in our answer to question 6.1, there are no specific patent regulations dealing with digital health innovations. There are not any precedential legal cases or decisions involving patent nor copyright protection of digital health innovations.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

From a copyrights perspective, the contract should clearly determine who is the owner of the IP rights, to prevent future disputes on ownership rights. While not mandatory, it is also advisable to register copyrights assignments and works with the Copyright Office, to be enforceable *vis-à-vis* third parties. If works are licensed, the scope of the licence should also be clearly determined, as licence agreements tend to be interpreted in favour of the author.

As to patents, under the Patents Law, the patent holder is/are the person/s or entity/ies in whose name the Letters Patent is issued, and that it is possible to apply for co-ownership between several parties, and in different proportions. Further, since agreements between parties are of a private nature, changes in ownership must be recorded with the AR PTO to be enforceable before third parties. Documentary evidence must be submitted to obtain such recordal.

Moreover, the Patents Law provides that licensing agreements must not include restrictive commercial terms affecting the licensee's production, marketing or technological development, nor any other conducts that may be deemed anti-competitive. If included, such provisions will be considered void and unenforceable.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

From a sanitary regulatory perspective, regarding agreements between healthcare and non-healthcare companies, it is important to recognise the different regulatory environments each party operates within. As the healthcare industry is highly regulated, the stakeholders must ensure compliance with local health regulations and adhering to standards set by regulatory authorities like MoH and ANMAT.

Consideration should be taken if a device or product using digital health technology may be considered as a medical device. In these cases, compliance with ANMAT's regulations is needed. On the other hand, if agreements between healthcare and non-healthcare companies involved the use of personal data, the parties must fully comply with the Law on Personal Data Protection and Law on Patient's Rights. The agreement should also explicitly address obtaining patient consent for the use of their data.

From a data protection perspective, personal data processing compliance should always be considered, especially when dealing with healthcare companies, where it is most likely that there is processing of sensitive data. Considerations explained in our answers to questions 2.4 and 5.1 would apply.

As regards patents and copyrights, there are no specific considerations related to healthcare and non-healthcare companies. Considerations for agreements in general – see our answer to question 7.1 – apply.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Please refer to our answers to questions 5.1, 7.1 and 7.2.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

The AAIP's AI Guide includes several recommendations on AI matters, which should be considered when dealing with the use of generative AI in the provisioning of digital health solutions. Among others, the AI Guide recommends the application of transparency and data protection principles, specifically mentioning compliance with the DPL. Compliance with these principles and the data protection regulations should be ensured by including all necessary provisions into agreements.

Furthermore, the use of generative AI in digital health solutions must align with healthcare regulations. It is advisable to seek guidance from legal professionals experienced in Argentina's health law framework before introducing such technology into the local market to evaluate whether the solution requires specific regulatory authorisation or oversight. On the other hand, healthcare services in Argentina can only be provided by licensed medical professionals. While generative AI can serve as a valuable tool to support professionals by analysing data or offering suggestions, it cannot replace or independently deliver medical care.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

From a sanitary regulatory perspective, there is no specific regulatory scheme dedicated exclusively to AI/ML technologies. However, if a device/product uses AI or ML that meets the definition of medical device or SaMD set forth in ANMAT Regulation 9,688/19, then it would be considered a medical device or SaMD and subject to the regulatory framework and oversight of ANMAT.

As to data protection matters, the AAIP, which is the Argentine data protection authority, is the enforcement body of the DPL. Although there is no specific regulation regarding AI matters, if there were any data privacy issues regarding AI/ML, which may include automated decision-making, for instance, the AAIP will oversee enforcing compliance with the DPL.

Regarding consumer protection, the national enforcement authority, the National Direction for Consumer Protection and Consumer Arbitration, as well as local authorities under the jurisdiction of provincial or municipal governments, are responsible for safeguarding consumer rights and enforcing the applicable regulations.

Among their main objectives is the oversight of advertising, particularly advertisements that may be misleading. This is especially relevant in the digital sphere, where the use of algorithms cannot only create a lack of transparency but also employ covert persuasion techniques based on AI to influence consumers' purchasing or contracting decisions. Furthermore, the use of AI may lead to biases that violate the principle of equal treatment.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

Currently, from a sanitary regulatory perspective, Argentina does not have a regulatory framework in the healthcare sector dedicated exclusively to AI/ML technologies. Consequently, such technologies are regulated under existing frameworks applicable to medical devices and related technologies, such as ANMAT Regulation 9,688/19 if such devices or products meet the definition of medical devices.

As to data protection, please refer to our answers to questions 2.2 and 8.1.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

The ownership of the IP rights to algorithms that are improved by AI/ML without active human involvement in the software development is still under discussion in Argentina, as there are no regulations that cover this topic, neither in the IP Law, nor in an existing individual specific AI regulation.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Licensing data for use in AI/ML requires careful attention to several commercial and strategic considerations, particularly in the healthcare sector, where data is highly sensitive. Thus, key aspects include ensuring compliance with data protection laws such as the DPL, where applicable, obtaining valid legal basis for the processing, and implementing measures to protect the data from unauthorised access or breaches. Licences must clearly define the scope of use, including the specific purposes for which the data can be processed, and include clauses addressing data anonymisation or pseudonymisation to minimise privacy risks. Licensed data must be accurate, and the licensee should ensure that the licensed data is used only for the purposes described in the licence agreement.

Parties must also account for obligations related to data retention, destruction, and transfer across jurisdictions. Healthcare data licences should also address restrictions on using data to train AI/ML models for commercial purposes, as well as ensuring the licensed use aligns with ethical principles for AI development.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Legislation in Argentina does not currently differentiate between standard AI and generative AI technologies or products. AI/ML-based solutions, regardless of their specific category, are assessed under existing frameworks applicable to their intended use, such as medical device regulations for healthcare applications. For instance, the AAIP, in its AI Guide, does not differentiate between standard AI and generative AI.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

The main legal issue regarding IP rights and generative AI technologies is the ongoing discussion on who owns the IP rights on the outcomes provided by the generative AI system. Discussions are ongoing regarding whether AI models can own IP rights. Furthermore, another legal issue unique to generative AI technologies is the use of images of third parties without their authorisation to create "deepfakes", especially circulating through social media. To address these issues, there have been some draft bills published seeking to regulate these matters – but these have not yet advanced to congress submission.

From a sanitary regulatory perspective, no initiative has been launched to directly address these generative AI-specific issues within healthcare.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

Please refer to our answers to questions 2.2 and 2.6 regarding AI legal framework in Argentina.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

In Argentina, adverse outcomes in digital health solutions are primarily addressed through consumer protection laws and civil liability, particularly under the Consumer Protection Law 24,240, the Civil and Commercial Code (CCC) and related regulations. The following theories of liability are relevant:

- Strict liability: Digital health solutions are often classified as products or services under consumer law. Suppliers, developers, and intermediaries can be held jointly and severally liable for harm caused to consumers by defective products or services, regardless of fault. This includes software malfunctions, inaccurate health data, or misleading results from digital health tools.
- Defective product or service: If a digital health solution fails to meet safety standards or performs below reasonable expectations, it may be deemed defective. Liability arises if the defect causes harm, even if the defect was not intentional or known to the provider.
- Breach of duty to inform: Providers are required to supply clear, accurate, and detailed information about the functionality, limitations, and potential risks associated with digital health solutions. Failure to do so can

lead to liability if the lack of information contributes to adverse outcomes.

- Misleading advertising: If a digital health solution is marketed with claims that it cannot fulfil (*e.g.*, exaggerated accuracy of diagnostic tools), liability may arise for misleading or false advertising under consumer protection law.
- Violation of data protection rights: Providers are required to comply with the DPL when processing personal data. In this regard, the AAIP Resolution 126/24 establishes penalties for non-compliance with the Data Protection Regime, which are limited to: (i) warnings; (ii) fines; (iii) suspensions; (iv) closure; or (v) cancellation of the database.

Moreover, the AAIP maintains a public registry of individuals and legal entities that have been sanctioned due to a violation of the DPL. Therefore, the infringer could additionally face reputational damage.

In addition, there may be claims for damages by data subjects based on the general principles of civil liability established in the CCC, including through class actions.

Courts in Argentina emphasise the principle of full compensation (*reparación plena*) for damages, including compensatory, moral, and, in some cases, punitive damages. Consumers are afforded a lower burden of proof in these cases, and suppliers must evidence they were not at fault or that the harm was not related to their product or service.

Lastly, from a sanitary regulatory perspective there are no explicit or specific rules applicable to product liability for adverse outcomes caused by these technologies. Therefore, the general rule of tort liability set forth in the CCC and consumer protections liabilities rules apply. In addition, from a liability perspective, potential claims may occur from patients who have received inaccurate treatments or diagnosis defined through the use of digital health tools, if such use had a causal relationship with an injury suffered by the patients. This liability should be also analysed together with the professional liability of the HCPs that used such digital health device.

9.2 What cross-border considerations are there?

From a regulatory standpoint, digital health solutions intended for use in Argentina must comply with local laws, including those governing medical devices and healthcare services. As a general rule, the CCC allows parties to international contracts to select the laws that will govern their agreement. However, the CCC limits party autonomy by providing that the principles of public policy and internationally mandatory rules of Argentine law will apply to the agreement, regardless of the law chosen by the parties (Articles 2599 and 2651, paragraph I CCC). Therefore, it is relevant to set forth clear governing law and dispute resolution contractual provisions to avoid any dispute regarding such clauses.

Regarding data protection, the DPL prohibits the international transfer of personal data to countries that do not have an adequate level of data protection and security, according to the AAIP's standards, unless the data subject consents to it or the data controller implements appropriate safeguards (SCCs or BCRs, as explained above).

Furthermore, it should also be considered that most of the provisions of the DPL are of a public nature (imperative regulation) and cannot be disregarded by any of the parties and will apply notwithstanding any contractual provision on the contrary. As to the relationship of the parties to an agreement themselves, they should be free to choose the venue (*i.e.*, local or foreign courts, arbitration, among others); however, based on the public order nature of the DPL, even if the parties choose a foreign law as applicable law, there exist chances that the courts or arbitrators may still need to resort to the DPL when it relates to their obligations for the processing of personal data.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Firstly, healthcare providers must ensure that any AI/ML system used has been thoroughly validated and tested, ensuring its clinical effectiveness and safety before being used in clinical settings. HCPs should also maintain their responsibility for patient care, ensuring that AI/ML tools are used as support rather than as replacements for clinical judgment. It is essential that healthcare providers understand the limitations of AI/ML tools and continuously monitor and assess their recommendations. Additionally, patients should be made aware of the role AI/ML tools play in their care, including any potential risks, and their consent should be obtained before using these tools. It is also recommended that healthcare providers consult with legal experts to determine whether a specific digital health solution triggers a regulatory framework and requires prior authorisation from health authorities. This is relevant when entering Argentina's market, where regulatory requirements may vary depending on the nature of the solution/device and its intended use. Finally, data protection and security must be prioritised, ensuring compliance with the DPL, particularly regarding the collection and processing of sensitive health data used by AI/ML systems. Regular audits of AI/ML systems for bias, transparency, and data security could most likely further mitigate legal risks.

Furthermore, it is advisable to include a compliance legal team in charge of ensuring that the company is complying with all legal obligations.

Lastly, the AAIP's AI Guide includes a set of recommendations for AI use, such as evaluating the user's experience to ensure the highest level of accessibility and usability standards, publishing a Privacy Policy, and securing information on the following: protection of personal data; transparency; traceability; and auditability. In this regard, when focusing on transparency, the AI Guide highlights the importance of always acting with data subjects' consent, and protecting confidentiality through robust security measures.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Please refer to our answer to question 9.1.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

A key concern in digital health is protecting sensitive health data. In Argentina, cloud providers must comply with strict data privacy laws to ensure secure storage and transmission, with encryption and access controls in place. Data breaches could lead to legal and reputational consequences and, therefore, it is essential to include in data processing agreements

strong provisions governing the implementation of security measures to safeguard the data stored in the cloud.

Moreover, the lack of efficient implementation of sanctions – such as those being inopportune or inadequately enforced – could undermine trust in digital health systems and increase the risk of data misuse or mishandling, compromising patient privacy and data security.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

As Argentina is a federal country, both federal and local regulations must be considered when entering the digital healthcare market. Companies will need to navigate varying regulatory frameworks, ensuring compliance with both national and provincial rules regarding regulated products (such as medical devices, SaMD, etc.).

From a data privacy perspective, the Data Protection Regime is of general application, regardless of the industry and thus, non-healthcare companies should consider the same key issues described in our answer to question 4.1.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Investing in digital health ventures in Argentina requires careful evaluation, particularly given the sector's emerging nature and lack of regulation. Early-stage assessments are crucial to ensure the venture has a solid grasp of regulatory demands and an informed approach to operating in a highly controlled environment like the healthcare industry.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The absence of standardised regulations for digital health is the main barrier to its widespread adoption in clinical settings, which may hinder a full integration of digital health technologies in practice. The decentralised and fragmented nature of Argentina's healthcare system adds another layer of complexity that may make coordinating the adoption of digital health solutions difficult.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

There is no specific certification body exclusively for digital health solutions in Argentina. However, the clinical adoption of digital health technologies could be influenced by certain professional organisations and regulatory agencies bodies that govern healthcare practices in the country. ANMAT is the authority that can grant marketing authorisations for digital health tools that may classify as medical devices.

In addition, the National Commission for Health Technology Evaluation and Clinical Excellence (CONETEC) was created through Decree 344/23 under the Secretariat of Access to Health of the MoH, which: (i) carries out evaluations of health technologies, according to criteria of quality of evidence, clinical benefit and economic impact on equity and public health; and (ii) issues technical recommendations on the incorporation, disinvestment, form of use, financing and coverage of the health technologies used in the health system. These technical recommendations will be binding for the MoH and decentralised agencies (*i.e.*, ANMAT, Superintendence of Health Services, National Cancer Institute and the Argentine Coordinating Institute for Organ Transplantation, among others) and deconcentrated agencies (*i.e.*, the National Institute of Social Services for Retirees and Pensioners, companies and entities of the national public sector).

In addition, HCPs in Argentina are regulated by professional associations such as the Argentine Medical Association and provincial medical professional associations. These organisations ensure that HCPs adhere to professional, ethical, and legal standards and its main objectives are specialisation, improvement and professional updating, although they do not specifically endorse or certify digital health tools.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

In Argentina, the Mandatory Medical Program (PMO) set forth the basic treatment coverage that social security and public/private healthcare insurance providers must guarantee. Reimbursement percentages and amounts are dependent on whether a medical practice is included in the PMO list. Values or practices that exceed those established in the PMO list are considered optional and covered either by private/public healthcare insurance providers. The PMO guarantees basic health coverage in the areas of preventive care, diagnosis, medical treatment, dental care, and medicine. However, there are no specific reimbursement processes for digital health services.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Argentina lacks a specific regulatory framework tailored to evaluating digital health solutions, particularly those relying on data-driven technologies such as AI and ML. However, if these health solutions qualify as medical devices, they may be subject to the evaluation of the CONETEC, as described in our answer to question 10.5.

Moreover, besides Data Privacy Impact Assessments – which are not currently mandatory in Argentina – there are no standardised legal mechanisms or protocols in place to assess the safety, efficacy, and ethical considerations of these tools before their implementation in clinical practice. As a result, the integration of AI- and ML-based health solutions remains limited and fragmented across the healthcare ecosystem.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

On June 27, 2024, the Argentine Congress approved a law denominated as "*Bases and Starting Points for the Freedom of the Argentinians*" (Basis Law), which entered into force on July 8, 2024.

The Basis Law is a wide-ranging law, including changes in legal, commercial, regulatory, and social relationships, with the aim of simplifying rules and obstacles to promote free market and competition, and limit state intervention.

One of its most relevant features is the creation of an Incentive Regime for Large Investments (RIGI), which provides for a comprehensive and very attractive system of tax, customs, and foreign exchange incentives, as well as guarantees and stability for foreign and local investments.

The RIGI will be applicable in the entire Argentine territory and the deadline for joining the regime is two years as of the entry into force of the Basis Law (July 2026). Such term may be extended for one additional year by the Executive Branch. The term of the benefits under the regime is 30 years.

Adhesion to the RIGI must be structured through a single project vehicle registered in Argentina holding a project that qualifies as a "Large Investment" (*i.e.*, a project involving a long-term investment equal to or higher than USD200m up to USD900m, depending on the promoted productive sector) in certain promoted productive sectors. Those sectors are mining, energy, oil and gas, steel, technology, agroforestry, tourism, and infrastructure.

Regarding the technology sector, it is focused on activities whose main purpose is the production of technological goods and services, both in their basic and applied aspects, of an innovative nature in different industries, including biotechnology and nanotechnology, software, robotics and AI, among others. The minimum investment for this sector is USD200m.

Moreover, the RIGI is compatible with other promotional regimes existing in Argentina, such as the promotional regime of the knowledge economy or the promotional regime for the development of biotechnology and nanotechnology.

The RIGI is generating large expectation in the market, since it is expected to be the driving force that channels all much-needed local and foreign investments for the development of certain strategic sectors in Argentina.

From a sanitary regulatory perspective, a particularly relevant issue in Argentina's digital health landscape is the ongoing debate surrounding the e-commerce of medicines. While online sales of pharmaceuticals have gained traction globally, in Argentina, they remain a highly contested and partially regulated area. The traditional pharmaceutical sector, including pharmacy associations and professional bodies, has expressed strong resistance to online medicine sales, citing concerns about patient safety, the risk of counterfeit drugs, and the lack of professional oversight in digital transactions. These concerns have led to ongoing litigation, creating legal uncertainty for platforms and providers attempting to operate in this space.

Despite these challenges, regulatory authorities have begun to cautiously authorise certain forms of online pharmaceutical sales under strict conditions, signalling an emerging recognition of the potential benefits of regulated e-commerce channels. This trend reflects an effort to balance innovation with patient safety and aligns with broader global shifts towards digital accessibility in healthcare services. Moving forward, it is likely that Argentina will see the development of a more robust regulatory framework specifically addressing the online sale and distribution of medicines, with clearer guidelines for compliance, traceability, and quality control. Such developments could significantly shape the evolution of digital health and improve access to essential medications, particularly in underserved regions.

Endnotes

1 https://www.statista.com/outlook/hmo/digital-health/argentina

2 Convention 108+ is not yet enforceable.

3 https://www.argentina.gob.ar/anmat/relacionesinternacionales/convergencia-regulatoria/participacion-ejecutiva

4 https://opinionpublica.anmat.gob.ar/DetalleProyecto.aspx?pno_id_proyecto=5293

5 https://servicios.infoleg.gob.ar/infolegInternet/anexos/385000-389999/389231/norma.htm

6 https://www.argentina.gob.ar/sites/default/files/aaip-argentina-guia_para_usar_la_ia_de_manera_responsable.pdf

Diego Fernández is a partner in the IP, AI & privacy practice group at Marval O'Farrell Mairal, Argentina. He is a technology expert, with 20 years' experience with a wide range of expertise that includes cybersecurity, data protection, RegTech (including Fintech, Insurtech and HealthTech), software protection and licensing, and criminal law in connection with technology. He regularly advises clients on IT and privacy-related matters, as well as IP and IT in M&A transactions. He has extensive experience advising clients on IP matters, including litigation. He is a former foreign associate in the IT & Privacy group at Foley & Lardner, Chicago. In 2013, he earned an LL.M. degree in IT & Privacy Law from the John Marshall Law School, Chicago, where he participated as the international student's ambassador and acting vice president of the Privacy & IT Law Society.

Diego is the vice president of ITechLaw, a member of the Research Advisory Board of IAPP and Co-Chair of its KnowledgeNet Chapter Buenos Aires, member of the Data Protection Committee of INTA, and member of the Technology Committee of IBA. Diego is also the president of the Privacy & M&A Committee of the Latin America Privacy Association (ALAP) and editorial board member of the Global Privacy Law Review. Diego has been recently appointed by Universidad Torcuato Di Tella as the new director of their Technology, Law and Corporations postgraduate course and continues to co-direct the Data Protection course as well as a course on AI & Law. He is also a professor at the John Marshall Law School, Chicago (United States) in its online course on Global Privacy.

Marval O'Farrell Mairal
Av. Leandro N. Alem 882
Buenos Aires
Argentina

Tel: +54 9 11 3462 8254
Email: dfer@marval.com
LinkedIn: www.linkedin.com/in/diego-fern%C3%A1ndez-97837a1b

Martín J. Mosteirin joined Marval O'Farrell Mairal in 2003 and is a partner of the Life Sciences and Healthcare departments. His areas of expertise are bio-pharmaceutical, healthcare, health-tech, medical devices, dental products, cosmetics, toiletries and perfumes, households cleaning products, food industry, animal health and food, food contact products, and agribusiness (seeds, agrochemicals, herbicides, insecticides, fungicides, fertilisers, growth regulators, GMOs and other related products), among other industries.

He provides both contentious and non-contentious legal advice to leading global companies on regulatory strategies and compliance matters ranging from the client's day-to-day business to complex cross-border transactions, start-ups, joint ventures, M&As, spin-offs, product liability and recalls, contracts, compliance training, monitoring, audits and investigations, (trial and pre-trial) administrative proceedings and litigation, and civil and commercial advice in general. Martín helps his clients by delivering sophisticated, high-quality and multi-practice work in cross-discipline matters for complex projects, enhancing the outcome for the client.

Marval O'Farrell Mairal
Av. Leandro N. Alem 882
Buenos Aires
Argentina

Tel: +54 11 4310 0100 ext. 1901
Email: mjmo@marval.com
LinkedIn: www.linkedin.com/in/martin-mosteirin

Australia

Bernard O'Shea

Rohan Sridhar

Norton Rose Fulbright

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

Digital health is an umbrella term referring to a range of technologies that can be used to treat, diagnose and monitor patients and collect and share a person's health information.

Similar to other jurisdictions, the term 'digital health' is still developing as technologies evolve. At one end of the spectrum, the term includes the delivery of telehealth services, while at the other end, the term connotes mobile apps and software as a medical device ('SaMD') used to deliver personalised and individualised medicine, with digital medical devices lying somewhere in between. The Therapeutic Goods Administration ('TGA') has also highlighted what they term Digital Therapeutics, which they characterise as being health software intended to treat or alleviate a disease, disorder, condition or injury, that works by generating and delivering a medical intervention that has a demonstrated positive impact on a patient's health. This can stretch to companion 'apps' that are an adjunct to other treatments.

While digital health is not a defined legislative term, the Government has taken steps to define telehealth in order to include these services under the subsidised Medicare arrangement during the COVID-19 pandemic, and the national regulator, the TGA, regulates some digital health technologies as medical devices.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

The key emerging digital health technologies in Australia are:

- Genetic guidance of treatment: Use of genomic testing to guide treatment pathways for a range of illnesses, including cancer and mental health issues. This is attendant with issues regarding the regulatory requirements of the testing process, as well as the end output, which typically informs decision-making by a healthcare professional.
- Use of AI: The application of AI to the mass of available health data, to enhance treatment pathways, aid diagnostic processes, find efficiencies in terms of treatment costs and timelines, and assist in tailoring individual treatments.
- Predictive technology: The use of algorithmic or data-driven software to guide further preventive or diagnostic testing for patients.
- Telehealth: Which is now an established part of the healthcare delivery landscape. It is readily available on a reimbursed basis where there is an established patient relationship, with multiple additional categories to cover emergencies or things like COVID-19 infections. It is also widely used on a non-reimbursed basis.
- My Health Record: Digitisation of health records to improve the quality and availability of health information. New legislation is proposed to mandate, subject to opt out, the pushing of a wide range of personal health information into the My Health Record system.
- eScripts: Digitisation of pharmacy prescriptions to allow easier access to certain medicines and ease processing on pharmacists. This fundamentally changes the long-standing requirements that all prescriptions must be provided physically and in writing.
- Adjunctive apps: Which might sit alongside an existing treatment, or be a sort of 'minder' app to encourage some activity. These challenge the limits of the existing regulatory dividing lines.
- Secure messaging: Facilitating the secure, encrypted exchange of information between health professionals.

1.3 What is the digital health market size for your jurisdiction?

The market for digital products and services in the healthcare sector is growing rapidly, especially post-COVID. Although the exact figure is not confirmed, in 2023, it was estimated that Australia's digital health market will be worth approximately A$3.16 billion (see https://www.statista.com/outlook/hmo/digital-health/australia?currency=AUD).

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

Public information in relation to private companies is difficult to find. As such, it is necessary to consider publicly listed companies which typically report to the market. To our knowledge, the five largest (by revenue) digital health companies in Australia are Pro Medicus, MedAdvisor, Cogstate, Austo Healthcare and OneView Healthcare.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Likewise, it is difficult to ascertain the five fastest growing

digital health companies by revenue in Australia. To our knowledge, 4D Medical is the fastest growing, followed by heraMED, Respiri, Austo Healthcare and Pro Medicus.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The TGA, which is part of the Australian Government Department of Health, is Australia's regulatory authority for therapeutic goods. Broadly, the TGA is responsible for regulating the registration of therapeutic goods in Australia. The TGA regulates therapeutic goods through pre-market assessment, post-market monitoring and enforcement of standards, and through the licensing of Australian manufacturers. The TGA can issue conformity assessment documents in respect of manufacturers of medical devices, though given the limited Australian manufacturing industry, many manufacturers rely on overseas certification of quality management systems, including notified bodies or Medical Device Single Audit Program certification.

Most digital health solutions are medical devices, and many are software based. The diversity of digital health solutions has challenged the regulatory dividing lines, which traditionally were either caught or not. Apart from the ability to prescribe things that are or are not medical devices (which has been utilised a lot in the digital health space), there is now a category of 'you are not regulated, but we want to know about it', which requires notification that an exemption is being relied upon. It is notable that the claims made in respect of a digital health product, as opposed to its essential function, may well be determinative of whether it is regulated as a medical device or not.

The TGA can essentially pursue anyone involved in the manufacture, importation, supply or promotion of therapeutic goods. It has broad information gathering and inspection powers, and a range of civil and criminal sanctions that it can enforce. Under the *Therapeutic Goods Act 1989* (Cth) ('TG Act') and the Therapeutic Goods Regulations ('TG Regulations'), the Secretary of the Department of Health can make decisions in relation to individual sponsors, manufacturers and advertisers. Some of these decisions are made in the event of non-compliance with regulatory requirements and others are made at the request of the sponsor or manufacturer. Regulatory requirements for which sponsors, manufacturers and advertisers can face liability for breaching include failure to properly label or advertise goods, or the importation of goods that are not registered correctly.

There are privacy laws at both the federal level and in various states, which typically are quite relevant to digital health, with a focus on the collection and use of health information. In general terms, their focus is on consent and security. The Office of the Australian Information Commissioner ('OAIC') is responsible for federal laws and the administration of the privacy provisions contained in the My Health Record Act and the *Healthcare Identifiers Act 2010* (Cth).

Additionally, the Australian Competition and Consumer Commission ('ACCC') is responsible for enforcing the *Competition and Consumer Act 2010* (Cth) ('CCA') and the Australian Consumer Law ('ACL'), which is set out in Schedule 2 of the CCA. The ACL includes a national law guaranteeing consumer rights when buying goods and services and a national product safety law and enforcement system. This includes the principal oversight of recalls of products, though often these are left to the TGA in relation to medical products.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

As noted above, the TGA is the primary regulatory authority, and in most cases the only one where approval is required to provide a digital health product. Two other agencies have an impact on some digital health offerings. Specifically, the Australian Digital Health Agency ('ADHA'), which primarily oversights software connected to and accessing My Health Record, and the National Prescription Delivery Service, which in conjunction with the ADHA oversights electronic prescribing software, which includes an approval process.

The ADHA also provides a guidance framework for what it terms mHealth apps, but this has no legislative support, and specifically excludes TGA-regulated SaMDs. Nonetheless, it contains some useful guides for the development of unregulated digital health products.

Other regulatory regimes that may apply to digital health products are, in contrast, regimes for which there are compliance obligations, with possible consequences at the hands of relevant regulators, and in some cases, recourse by consumers. Foremost among these is the *Privacy Act 1988* (Cth) ('Privacy Act') (and various State and Territory counterparts), which can apply to digital health in a number of ways. For example, the Privacy Act contains provisions that will apply if the digital health function uses, collects or distributes personal information. Personal information is any information that identifies, or is likely to identify, a person. If a digital health function uses personal information, it must ensure that it displays a privacy policy, notifies users that it is collecting their personal information and the purpose for which this information is being collected. Several State and Territory Governments have also enacted privacy legislation directed specifically to health records and other health information, whether held by healthcare professionals or by digital health applications. This legislation typically restricts transfer out of the particular State, and certainly Australia, making cloud and other offshore storage problematic.

If the digital health function collects health information, such as disability or specialist reports, then this will attract additional privacy protections compared to personal information. For example, any data in relation to the My Health Record scheme must be stored in Australia and under no circumstances is to be disclosed to cross-border entities.

Australia's consumer regulatory scheme, the CCA, may also apply to digital health. The CCA establishes a national law that governs how all businesses in Australia must deal with their competitors, suppliers and customers. The CCA is designed to enable all businesses to compete on their merits in a fair and open market, while also ensuring businesses treat consumers fairly.

Under the CCA, any acts undertaken by digital health companies that are viewed as promoting an anti-competitive business strategy can face severe penalties. Further, any digital health products that are likely to cause consumers to be misled, or make misrepresentations about the quality, purpose or efficacy of the product can face regulatory action pursuant

to the CCA. The penalties that the regulator can seek range from injunctive action and pecuniary penalties, to prison sentences for serious cartel conduct.

There are presently limited anti-kickback restrictions in Australia. These typically apply to doctors, pathology and diagnostic imaging services, and prevent certain payments being made between these professionals. These provisions apply where primary payments are made through Australia's public health system and the need to limit unnecessary referrals.

Australia has recently introduced an independent agency, the National Anti-Corruption Commission, which is targeted at detecting, investigating and reporting on serious or systemic corrupt conduct in the public sector. This power is limited to corruption involving public officials, though the National Anti-Corruption Commission can investigate others if their conduct might cause a public official to carry out their role in a dishonest or biased way.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The primary areas that regulatory authorities are targeting are:

- Classification of devices, to exclude or include categories of devices within the regulatory framework or to up-classify devices.
- Virtual prescribing, where online consultations occur, typically closely aligned with some supply pathway.
- Ensuring digital health products are advertised in a TG Act-compliant manner.
- Protecting privacy and data security of personal and sensitive health information housed in data centres of digital health organisations. This is expected to become even more important following a number of significant data breaches, which have led to substantial increases in applicable penalties.
- The digital economy, including consumer data issues in digital health, is an area of priority for the ACCC.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

If the SaMD is captured by the medical device definition in the TG Act and is not within one of the exemptions or exclusions, it will need to conform to the typical medical device clinical requirements. This involves registering the medical device in the Australian Register of Therapeutic Goods ('ARTG'), which is managed by the TGA. The device will need to be classified according to the TG Regulations, which is closely aligned with the classification system used by the EU. The quality management system will also need to be certified as compliant with the relevant conformity assessment procedures, again closely aligned with the EU system.

Further, an Australian sponsor will need to be appointed, and a Declaration of Conformity must be submitted. The Sponsor must then submit various certifications and applications to the TGA for review. In making its assessment, the TGA will assess the device against the Essential Principles contained in the TG Regulations. If the TGA approves the application, an ARTG listing number will be issued to the device, and it will be visible on the ARTG database on the TGA website. The SaMD may then be legally supplied.

It is also necessary to note that the sponsor of a therapeutic good, in Australia, is the person who imports the product into, or manufactures the product in, Australia. This creates a number of issues for software-based medical devices, since they are often made available by way of download from a central repository. In such a case, the download of the product may be considered the importation of the product in Australia, leaving the relevant 'downloader' as technically satisfying the sponsor definition. The TGA is concerned about this issue, particularly where consumers may be acting on recommendations generated by such software, but as yet it has not proposed a concrete solution.

As noted above, there is also a new category, namely SaMDs that have the benefit of an exemption, but which need to be notified to the TGA to validly qualify for the exemption. Presently this only applies to clinical decision support software ('CDSS').

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

There are presently no special regulations applying to artificial intelligence ('AI')/machine learning ('ML')-powered digital health devices or software solutions and their approval for clinical use. Where the devices or software solutions are classified as medical devices, the regulations applying to medical devices will apply. In such circumstances, the sponsor will need to apply to the TGA to have the device included on the ARTG prior to supply.

Given that Australia's digital regulatory landscape is evolving, it is likely that special regulations will be developed in the future which apply specifically to AI/ML-powered digital health devices or software solutions. The TGA has previously contemplated this issue, but no changes have been made to date. The expectation would be that they would be likely to follow, in general terms, the approach adopted by the European Commission, with perhaps some local adjustments.

The Federal Government's Department of Industry, Science and Resources has also released a proposal paper on introducing mandatory guardrails for AI in high-risk settings and contemplates the use of AI in healthcare. The paper does not draw any established definitions of 'high risk' but suggests following EU precedence that would classify AI in healthcare as high risk.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

The TGA has commenced a consultation in relation to necessary changes to the regulatory framework to account for the use of AI in healthcare. This consultation concluded in October 2024, with a TGA report not yet released.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

At this stage, it is not clear what role, if any, clinical validation data will play. It is expected that digital health solutions will continue to be subject to typical reviews under a conformity assessment procedure, which would seek to ensure the relevant solution produces an expected and repeatable result. In that regard, it would be expected that the clinical validation data would be critical.

The TGA has highlighted a number of relevant dimensions that need to be considered in the context of SaMD using AI. Two worthy of mention are the need to demonstrate that the training data used is relevant to the Australian population or sub-population for which the product is to be used, and around the use of synthetic data to train the AI.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

All regulation of digital health products is expected to be undertaken at a Federal level, consistently with other medical devices.

However, we are seeing guidances emerge from State and Territory health departments around the clinical use of AI-based systems, which are manifesting in clinical practice standards being implemented at hospital level around AI-related uses.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

At this stage, there is no tailoring in respect to enforcement actions in relation to the digital health products. It is noted that the TGA's enforcement priorities often reflect areas of high risk, which has often included digital health products. With the continued explosion of such products, and the inclusion of AI-based devices, this may be expected to continue.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Data privacy and the protection of sensitive health data collected in the course of conducting telemedicine is a core issue. Additionally, websites and software packages can be classified as medical devices, imposing increased compliance requirements. Data sharing in the context of telemedicine is likely to be regulated by the My Health Record Act. There is also the need to ensure that the patient can be properly identified and consents to the provision of care by telemedicine, and that appropriate records are retained. The use of telemedicine in the context of 'virtual' supply of tangible therapeutic goods, e.g. weight-loss products and cannabis, has been an area of regulatory focus.
- **Robotics**
  Depending on their intended use, robotic technologies may be classified as medical devices under section 41DB of the TG Act. If this occurs, the sponsor will need to have the device registered before it can be advertised and sold. Increasingly, these products are 'connected' and associated with software, and are becoming integrated into the patient journey, complicating issues such as consent, and typically involving the transfer of identified health information out of Australia.
- **Wearables**
  The core issue with wearables is whether they are inside or outside the regulatory framework. The issue often pivots on the sponsor's promotional material, as it indicates intended use, which underpins the Australian classification. A consistent issue is who owns the data collected from the device wearers. Similarly, issues arise relating to the privacy and security of the data collected from the device wearers. This is an area where the boundary is being continually pushed as devices gather more data, apply sophisticated algorithms and provide users with various metrics by way of feedback, and increasingly by reference to standards or norms, and with some AI oversight. Consumer expectations are also increasing.
- **Virtual Assistants (e.g. Alexa)**
  Issues arise where the virtual assistants begin providing diagnostic or therapeutic advice. Where this occurs, it is likely that the technology will be classified as a medical device, imposing greater compliance requirements.
  Further, issues arise relating to the rights to data collected by the virtual assistant. The technology sitting behind these assistants requires strict compliance with data protection laws and security requirements.
- **Mobile Apps**
  Separation of the apps from the platform on which they run is important. Like wearables, there is often a question of whether the product is within or outside of the regulatory framework. Given such products are often sourced through foreign 'app stores', the question of who is properly regarded as the sponsor can be problematic.
  Ownership of the data collected by the mobile apps, data protection and security requirements, specifically for health and/or monitoring apps, and the issue of liability, are key. Depending on the intended use of the apps, they may be classified as a medical device. The TGA does not regulate health and lifestyle apps that do not meet the TG Act definition of a medical device.
- **Software as a Medical Device**
  The TGA regulates SaMDs. Where the software is classified as a SaMD, regulatory issues arise. These include classifying the device according to the level of harm it may pose to users or patients, obtaining a conformity assessment certification for the device and submitting a declaration of conformity. Note that the question of who is properly regarded as the sponsor can be problematic in the context of SaMDs, again as a result of their provenance and accessibility.
  It is also noted that the software is typically treated as separate from the platform on which it exists. There are, however, questions about the extent to which updates to an operating system render the approvals of the software invalid, or in need of an updated review, or in some cases, recall.
- **Clinical Decision Support Software**
  CDSS that meets the definition of a medical device must be included in the ARTG unless otherwise exempt. Where the CDSS is responsible for storing data, issues of data privacy and security arise. There may also be issues of tort liability where the CDSS is responsible for adverse health outcomes. The regulatory treatment of CDSS remains quite a contentious area, critically depending on the functionality of such software. Clearly, a continuum exists from software that merely provides information for consideration by a healthcare professional, to software that provides a warning or recommendation, to software involved in clinical decisions. This is a key area where the regulatory framework has ambiguities. This

has led to the category of CDSS which is exempt, conditional on notification to the TGA. Essentially, it provides a mechanism for the TGA to monitor how this sector evolves.

- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  Software that is powered by AI/ML is governed by the same legislation applying to other software. If the specific AI/ML-powered digital health solution satisfies the TG Act definition of medical device, it must comply with the TGA requirements, including obtaining a conformity assessment certification for the device and submitting a declaration of conformity.
  Additionally, the Australian Privacy Principles ('APPs') (see question 3.2) are designed to be technology neutral, flexible and principles-based, which can adapt to changing and emerging technologies, including AI. Despite this, it is critically important that personal information used to train AI systems is accurate, and collected and handled in accordance with legal requirements.
  The issue of copyright arises when AI is trained with or generates substantial amounts of work from third parties, potentially infringing upon their rights. Another core legal concern when utilising AI is the ownership of health-related information, as it may qualify as personal information protected by privacy laws, which raises the issue of consent (see https://link.springer.com/article/10.1186/s12911-023-02103-9#Sec1 and https://www.mdpi.com/1999-5903/15/9/286). Furthermore, ownership of data becomes problematic when multiple parties have contributed to AI-powered digital health solutions, not only due to ownership rights but also regarding liability in cases of misuse or exploitation of health-related data (see https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7762914).
- **IoT (Internet of Things) and Connected Devices**
  The issue with IoT is primarily an issue of categorisation. Very similar to CDSS, a continuum exists as to what the connected device is capable of doing. There are simple sensors that merely pass along information, through to more complex devices e.g. a mattress that detects movement and provides an alert. Aspects of intended use may impact categorisation, as may its role in a hospital ecosystem. What we are starting to see is these devices moving closer to the consumer, e.g. directly, or in a pharmacy rather than with a doctor.
- **3D Printing/Bioprinting**
  The use of 3D printing brings in the regulatory framework concerning custom-made medical devices, which has recently undergone significant reform. Depending on the type of product being printed, and the frequency of its use, different regulatory obligations will apply. This includes differences in the need to register a product, as well as the need for ongoing reporting to the TGA. There is also a question regarding the consumables for such printing, their categorisation and place in the regulatory framework. There are also potential patent and design infringement issues associated with some categories of bioprinting.
- **Digital Therapeutics**
  Categorisation of these devices is important, as is their cyber-security. There are concerns around the ability of such devices to be hacked or interfered with, the appropriate treatment of software updates, and the applicable regulatory oversight of these. As noted above, the TGA has highlighted these as a special category of SaMDs.
- **Digital Diagnostics**
  Categorisation of these devices is important, as is their cyber-security. There are concerns around the ability of such devices to be hacked or interfered with, the appropriate treatment of software updates, and the applicable regulatory oversight of these. Typically, these products are increasingly utilising AI, some as an add-on, and some as the core engine. Even limited use of AI in the context of an existing device may have quite profound implications in relation to the scope of regulatory compliance obligations required to be undertaken.
- **Electronic Medical Record Management Solutions**
  Electronic Medical Record systems are typically exempted from the requirement to register as a medical device (if such a product does otherwise satisfy the TG Act definition). This is considered somewhat anomalous given that the validity of the data they hold is so critical to patient care.
  Given the sensitive data that is stored in these systems, privacy and data security are primary concerns. Any management system must be compliant with the Privacy Act if it is storing sensitive information (i.e. health information), which is highly likely. As noted above, it is likely many of these systems are going to need to evolve to more directly interface with Australia's My Health Record system.
- **Big Data Analytics**
  Given much of the data on which they are based was collected before this sort of use was contemplated, consent to use such information for such purposes is a critical issue. Likewise, with the increasing sophistication of AI models and data sets, the concern of re-identification is increasing.
  Ensuring the security and privacy of such vast amounts of data is the main concern; additionally, the ML models applied to outputs of big data analytics must be carefully scrutinised to ensure they do not contain algorithmic bias and can accommodate more than just the majority.
- **Blockchain-based Healthcare Data Sharing Solutions**
  While blockchain offers a solution for a distributed data sharing solution, the incredible fragmentation of healthcare data sets has to date mitigated against its utility to provide usable incremental benefits. The efforts to expand the My Health Record system to become something closer to a single source of truth may provide opportunities for blockchain-based systems to provide their promised benefits.
- **Natural Language Processing**
  Appropriate categorisation of the product as a medical device will be an issue for these, primarily the question of whether it satisfies the regulatory definition. We might expect that from a regulatory perspective the fallback of the relevance of the device to patient safety might be the determinative factor, with the TGA providing clarity through the use of included and excluded orders.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Digital platform providers sit in a difficult space as to whether they are within the regulatory framework or not. There are also potential exposures under the ACL. Digital platform providers must understand the precise scope of their platform and the extent to which such a platform falls within the definition of a medical device. It is also necessary to consider whether a relevant exemption might assist.

Another key issue for digital platform providers is the privacy and security of the data housed in the platform. Any information a digital platform provider collects, uses, stores or discloses will need to comply with the APPs contained in the Privacy Act. The APPs are legally binding principles that are the cornerstone of the privacy protection framework in Australia. The APPs set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information.

For digital platform providers, the APPs of greatest relevance regarding health information is the disclosure to other entities (APP 6), especially cross-border entities (APP 8).

The TGA has once again started to take an interest in platform providers in their guise as publishers of advertisements related to therapeutic goods, which are asserted to not comply with the relevant advertising code. In particular, the concern about the use of influencers to drive the use of certain products.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The use of personal data is subject to the APPs. The key issue in relation to the collection, use, storage and disclosure of personal information is consent of the underlying individual, particularly where the data is collected from a third person (such as a healthcare professional). In such a case, the ability to demonstrate consent is problematic.

There is a critical tension between the need to have evidence of consent and the desire to have a de-identified dataset. De-identification can be critical to downstream processing, e.g. to use as training data for an AI, as it will mean the privacy laws will not apply. This issue of de-identification is becoming more topical as the tools and data-sets available become more sophisticated and profound.

A critically important consideration is whether the data is being used for the primary purpose for which it was collected. Per APP 6, in the absence of the individual's consent, health data can only be used for the primary purpose for which it was collected, or for secondary uses that are directly related to the primary purpose. Essentially, any information collected in the context of the provision of health services will be sensitive information.

Where data is being used and shared in cross-border settings, it is important to consider whether the recipient is willing and able to comply with the requirements contained in the APPs. Often, transfers of data within a family of companies occurs without sufficient consideration of the privacy issues this might cause.

The timely destruction of health information is also important, noting the primary obligation not to retain data once its need for retention has ceased. A number of high-profile breaches highlighted how much old data was being held for no apparent reason.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Personal health data is regulated under the Privacy Act at a Federal level and the APP Guidelines must be complied with when handling personal health data. All States and Territories have their own privacy legislation for public sector entities, as well as certain State and Territory laws governing the treatment of health information, all of which are substantially similar to the Privacy Act and invoke similar protections. Regulation at both levels create obligations on how health data is used, which are based on the primary purpose the data was collected for. In some circumstances, data can be used for a secondary purpose, this includes by consent, where it can be reasonably expected by the patient and is directly related to the primary purpose of collection.

What we have started to see is the implementation of laws designed to allow the sharing of health information to central bodies, effectively overcoming relevant laws requiring consent or waivers.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

In Australia, Government entities are held to a higher standard than regular entities. Additionally, contracts with Government entities often impose obligations on service providers to comply with the Privacy Act as though the party is a Government entity. Further, State and Territory Governments and their instrumentalities, such as the public hospital system, will often mandate compliance with separate State and Territory privacy laws, which are typically more restrictive in terms of data transfer.

4.4 How do the regulations define the scope of personal health data use?

Generally, data use must be for the primary purpose for which it was collected. This can typically be gleaned from disclosures made to the individual at the time of collection, in either a collection statement or privacy policy. This can create difficulty in the case of collection from a third party, since the scope of the primary purpose may be difficult to construe. In the context of healthcare there are frequently disclosures of personal information to service providers, such as pathology or radiology services, followed by expert review. These persons may have no way of contacting patients or obtaining consent, and therefore rely upon the primary collector making sufficient disclosures to the patient as to this purpose for collection.

Further, the data must be reasonably necessary for the business activities undertaken by the organisation. Whether the data is reasonably necessary is an objective test. It is important that whatever the purpose of use is, it is disclosed to the customer in the first instance. This over-capture and over retention of data is becoming a focus for regulators.

In the absence of specific consent, health information may only be used for secondary purposes directly related to the primary purpose for which it is collected. There is general regulator dislike of the collection of health information for purposes other than those directly related to the health function.

Further, health information may also be used where the secondary use is required or authorised by or under an Australian law or a court/tribunal order.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

Contractual considerations will include an acknowledgment that parties to the contract will abide by Australian privacy law, including the APPs, and where applicable, do whatever is reasonable to assist the privacy regulator. Contracts will often deal with the obligation of a party to receive appropriate consent to transfer personal information, as well as obligations to de-identify data whenever possible. As noted above, de-identification can be problematic in the healthcare context, particularly where multiple different sources of personal information can be combined to identify an individual. Contracts will also typically create restrictions on disclosure of personal information and cross-border transfer of data. Further, the parties will typically deal with how withdrawal of consent may occur, and specify which party is the preferred party to deal with requests for access, correction and deletion.

Key contractual considerations will invariably depend upon what is being contracted and the context surrounding the procurement.

A common contentious issue is who takes the lead in a data breach situation, where there may be a tension between regulatory requirements and reputational exposure. This can create issues with State instrumentalities, which are typically not subject to data breach obligations.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Other than data inaccuracy, these issues are not really dealt with by Australian law. From a privacy perspective, entities are required to ensure that personal information is up to date; however, this is the limit of obligation. Where an entity receives a request from the relevant individual to correct personal information, the entity must take such steps as are reasonable in the circumstances to correct that information.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

Comprehensive rights to personal or sensitive data that is used or collected by digital health organisations will depend entirely on consents by individuals and ongoing compliance with the APPs.

It is a requirement under the Privacy Act that an individual reserves the right to withdraw their personal information from an organisation's database. In that sense, it is not possible to secure permanent, ongoing comprehensive rights to Australian personal information.

It is also necessary to ensure that relevant consents are stored for record-keeping purposes, which may be problematic where privacy policies change or are updated. Identification of information that may be health information is also difficult. There may also be obligations imposed on entities that analyse health information, and the consequent obligation to notify individuals of health issues arising from that. This is particularly the case in the context of genetic testing.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

There are a number of issues to consider when sharing personal data. A fundamental issue is whether the individual to which the personal data belongs has provided their consent to its disclosure. This is also subject to the right to disclose for the primary purpose for which the information was collected, as well as secondary purposes directly related to the primary purpose or to which the individual has consented. There is also an obligation on any party that collects personal information to provide a collection statement either before collection or as soon as practical afterwards. In the context of collection from a third party, providing a collection statement can be difficult, and is often overlooked.

There are additional considerations where the personal data is being shared in a cross-border context. It is rare that the jurisdiction the data originates from is the same jurisdiction the data will be housed in. Australian data security laws require that any entity that discloses personal data outside of Australia comply with certain restrictions. These restrictions seek to ensure that the individual is given the opportunity to provide their informed consent, especially with regard to which countries' rules apply.

Further, consideration must be given to whether the data, in the hands of the recipient, identifies an individual. If it does not, it may not be considered personal information, unless it is reasonably possible to re-identify the subject.

The key regulatory requirement applying to data sharing is APP 6, which outlines when an APP entity may use or disclose personal information. APP 6 states that where an APP entity holds personal information that was collected for a particular purpose, it must not use or share the information for a secondary purpose without the individual's consent, or where an exception applies. Disclosure without consent of health information is permitted where the secondary purpose is directly related to the primary purpose.

The information-handling requirements imposed by APP 6 do not apply to an organisation if a 'permitted health situation' exists. In relation to APP 6, there are three relevant permitted health situations:

- the use or disclosure of health information for certain research and other purposes, consent is impracticable and certain specific guidelines are followed;
- the use or disclosure of a person's genetic information to a genetic relative, in certain strictly limited circumstances; and
- the disclosure of health information to the responsible person for another, where that other cannot provide consent, there is no contrary instruction and certain specified circumstances exist.

Additionally, where the data sharing occurs within a cross-border context, APP 8 applies. Per APP 8, where disclosure of personal information is to a person who is not in Australia, reasonable steps must be taken to ensure that the overseas recipient does not breach the APPs in relation to the information. Generally, where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs.

We note also that, in the context of data collected in the process of clinical research, further restrictions may be imposed by relevant ethical approvals, which may limit or restrict the use of the collected data, even if it is de-identified.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Personal health data is regulated under the Privacy Act at a Federal level and the APP Guidelines must be complied with when handling personal health data. All States and Territories have their own privacy legislation for public sector entities, as well as certain State and Territory laws governing the treatment of health information, all of which are substantially similar to the Privacy Act and create similar protections. Regulations at both levels establish obligations on how health data may be shared or disclosed. These are largely based on the primary purpose the data was collected for, typically by way of explicit consent, or for a secondary purpose that is reasonably expected from the primary purpose. Additional exceptions apply, such as where sharing information is required by law or there is a serious threat to life, safety or health of individual. The APP Guidelines also stipulate different requirements for sharing health data to an overseas recipient, which requires taking reasonable steps to ensure the recipient does not breach APPs. The recent Privacy Act reform bill proposed to create a 'white list' of countries with similar privacy laws to Australia to allow for easier overseas data sharing. State and Territory health privacy legislation also prevents data leaving that jurisdiction without the consent of the patient.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

The nature of the entities involved does not really change the issues relating to the sharing of personal information. Where the relevant entity is an organisation and not a public sector entity, it has the right to use and disclose health information for a 'permitted health situation', including to undertake research relevant to public health or safety, or to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the individual in relation to whom data was collected.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

There are several interoperability standards for health information to be shared between people, organisations and systems, with the National Healthcare Interoperability plan 2023–2028 established by the Government.

Sharing of health information in the context of mental health patients is expanding, through a combination of legal changes (see https://www.health.vic.gov.au/mental-health-and-wellbeing-act-handbook/information-sharing) and data sharing protocols (see https://www.health.nsw.gov.au/legislation/Documents/inf-sharing-csnsw.pdf).

The Victorian Parliament has passed a law establishing a new centralised health system that can be accessed by public hospitals to share patient and health information. It is not clear whether other jurisdictions will follow a similar pattern.

A bill has been tabled by the Commonwealth to effectively require various providers of health services to input relevant individuals' health information into the My Health Record. It is subject to an opt-out mechanism. It is not clear whether it will proceed, but if passed, it will have a number of quite profound implications for the sharing of such data.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

The main issues are privacy issues, particularly in relation to access and use of patient data. There are also malpractice concerns if data shared comes under scrutiny for potential wrongful decisions made in the course of a treatment.

Misuse of patient data is also particularly problematic if the data is misused or creates a risk of discrimination.

The forced or facilitated sharing of personal information, particularly sensitive health information, is rather against the basic principles of privacy, and the individual's rights around their information.

The issue of de-identified data sets being re-identifiable is becoming increasingly problematic and is becoming more acute with the advent of AI.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

The scope of patent protection is determined by the *Patents Act 1990* (Cth) ('Patents Act'). There is no special application process for digital health technologies; the process for applying and obtaining a patent is the same across all technologies. In order to obtain a patent, the invention must be new, useful and inventive. Software and algorithm patents are available, though demonstrating inventiveness for software in particular is problematic. It is noted that recent jurisprudence has confirmed that an AI cannot be an inventor for the purposes of the Patents Act.

Patents give the right to stop others manufacturing, using or selling the invention in Australia without the permission of the patent holder. Patents can be owned by the inventor, a person who has legally obtained rights to the invention from the inventor, or a company or employer of someone who made the invention in the course of their normal duties. A person that holds a patent may also grant a third party a licence to exploit the invention on agreed terms.

The duration of the patent will depend on the type of patent; a standard patent lasts up to 20 years (with extension available for certain pharmaceutical patents) and an innovation patent for up to eight years.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

In Australia, the scope of copyright protection is determined by the *Copyright Act 1968* (Cth) ('Copyright Act'), which generally reflects the global copyright treaties. Pursuant to the Copyright Act, drawings, art, literature, music, film, broadcasts or computer programs can be protected by copyright. The owner's original expression of ideas is protected, but ideas

themselves are not. In Australia, copyright is not required to be registered. Copyright is the most usual form of protection for software and other digital health devices. However, copyright cannot prevent the underlying idea being reproduced.

Copyright protection may be limited by contract, especially in the case of open-source-based software. Similarly, the protection available to data and the outputs of devices is at best limited, and the requirement for a human author persists.

Digital health solutions very commonly use or incorporate open-source components. The scope of various open-source licences can impact the ownership and usage rights of created code, and effectively impact the ability to license new code on other than open-source terms.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secrets are any confidential information, including secret formulas or processes and methods used in production. The protection of a trade secret gives the creator certain rights and privileges depending on the type of protection. Unlike other IP rights, trade secrets are not registered; they are protected by keeping them a secret. The most common way to ensure trade secret protection is by ensuring all involved in the process sign confidentiality and non-disclosure agreements. Additionally, trade secrets are commonly protected by limiting access.

There are some limitations. The scope of protection does not extend to protection from other individuals creating the same product independently and exploiting it commercially. However, it can be very difficult in some contexts to prove independent development, especially where there has been some exposure to the relevant information. There are no exclusive rights and trade secrecy is difficult to maintain over a long period of time or where a number of people know the trade secret.

Australia has a quite advanced confidentiality regime, protected by an extensive body of court-based legal principles. However, Courts are typically unwilling to protect general business information without clear rationale, as it becomes an anti-competitive tool, and hence conflicts with public policy.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

There are no specific laws or rules applying to academic technology transfers in Australia, but the typical contractual laws apply. Academic institutions will typically have a standard contract that they use for these scenarios, which will include licensing arrangements for the IP and material produced as a result of the agreement.

There have been moves by the Commonwealth Government to produce a harmonised series of documents for use in academic settings. Most academic institutions will aim to retain ownership of IP they develop, and grant exclusive licences, while retaining an ongoing academic licence to use the IP they develop. They particularly like to retain ownership of patents. This can hamper fund-raising and create complexities when it comes to enforcing the patents.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

SaMDs can be protected via various forms of general IP rights. Novel inventions can obtain patent protection. The underlying software code will typically qualify for copyright protection, though the use of open-source software in the development may infect new code and undermine its commercial worth. Computer-generated works and databases may not be eligible for copyright protection in Australia.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

An AI device cannot be named as an inventor of a patent in Australia. An inventor that is 'human' is necessary to apply for patent protection. This position was confirmed recently by a unanimous decision of the Full Federal Court in *Commissioner of Patents v Thaler*, which determined that an inventor must be a natural person. It is unlikely that the laws in this regard will be changed in the near term.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

There is no broad statutory framework. However, it is becoming increasingly common for rights to be asserted or reserved through contract, particularly to guarantee rights of access on commercial terms. There are no particular rules or laws related to Government-funded inventions in Australia. There is limited funding granted to commercial entities, with most funding being made to universities and research institutes. Some of these agreements may encourage Australian development or exploitation, but have typically not actually intruded into that process. However, we are seeing a trend whereby the Government is being more intrusive in respect of IP developed through activities it funds, in some cases demanding an option over resultant deliverables.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

There is no decision affecting the protection of digital health innovation that is different to the traditional IP process. The Full Federal Court decision of *Commissioner of Patents v Thaler* [2022] FCAFC 62 did clarify that AI cannot be named as an inventor on a patent application, which may hinder some applications to protect digital health innovations. However, typically the innovation itself utilises AI rather than being created by it. It is also noted that the *Thaler* decision was established by the relevant individual almost specifically to be a test case, and may therefore be subject to future jurisprudence. It is also important to distinguish between protecting an abstract idea, which is not allowable in Australia, and patenting specific inventions.

Other forms of IP remain unchanged in their ability to protect digital health innovations, such as copyright subsisting in code used in many digital health inventions. Likewise, design

rights can protect the look of new devices such as wearables through an application to IP Australia.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

A critically important consideration applying to collaborative improvements is the ownership structure of IP rights developed through collaboration (e.g. patents, copyrights, technical know-how, research results/data, etc.), and who has the commercialisation lead. Ownership rights are typically governed by the terms of the agreement between the parties. The rights of use of background IP (and improvements to background IP) for commercialisation purposes are also necessary to consider. Such rights may be on a royalty-free or royalty-bearing basis, and exclusive or non-exclusive. Given the limited protection available to data, it is important to consider the protection of data, particularly where publication is a key consideration.

Another important consideration relates to the licensing of existing IP. In collaborative arrangements, licensing is used to manage protected IP that will be shared through the collaborative arrangement.

Additionally, careful consideration should be given to confidentiality obligations applying to the arrangement. Given the nature of collaborative improvements and the risks posed to existing IP, detailed confidentiality regimes are often implemented to protect existing IP rights.

Consideration also needs to be given to the possible application of the competition laws, in particular where the collaboration participants may be actual or potential competitors.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

An important consideration applying to agreements between healthcare and non-healthcare companies is data privacy and compliance. Noting the likelihood of health data being shared, both parties must ensure they comply with their potentially heightened privacy and data sharing obligations. This is particularly important where the companies are collecting both personal and sensitive health information. Again, de-identification of personal information, and ensuring that appropriate consent has been obtained to transfer, can be critical.

In such agreements, it is particularly important that the healthcare company has properly secured the rights to the healthcare data. If this data has been improperly obtained or secured, the non-healthcare company would be unable to obtain the rights necessary to use such data for its intended purpose. Another important consideration is clarity around ownership of the data shared or produced as a result of such arrangements.

Finally, it is relevant to note that the compliance obligations imposed on healthcare companies are often unknown to companies in other industries. As such, ensuring that clear guidance is provided about the industry-specific obligations, particularly in areas such as marketing and promotion, are important.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

The obvious benefit of federated learning is the avoidance of transfer of data between the participants in the training process. This reduces the risk of misuse or improper access to training data, and protects against entities' breach of privacy and other obligations. In the heavily regulated healthcare industry, the use of federated learning can aid in ensuring access to critical medical and other proprietary records, enabling significant progress in the industry.

The key considerations are similar to other data sharing agreements, particularly ensuring that there is not any reverse engineering or other mechanisms to determine the algorithms underpinning the learning model. It is also necessary to ensure that providers of data do not introduce harmful code into the ML database.

Little attention appears to be paid to the prospect of liability arising from the non-implementation of the learnings that might emerge from such exercises, which typically identify best practice or bad practice.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Parties must ensure that the information generated by AI and being relied on is safe and accurate to use. Guardrails must be implemented to detect hallucinations. The risks can be reduced when the relevant users are specifically trained in the efficient use of AI and in understanding the need for independent verification of information.

Another consideration should be given to the privacy of the patient and the consent obtained to use or share health-related information. Protocols should be developed around the input provided, both for consistency and accuracy.

As a medical provider, consideration should be given to how the information generated is to be interpreted and relayed to patients during a medical appointment. This is essential for quality assessment and accessibility for the patient when they are seeking professional opinions. It is also important to ensure that clinicians understand that digital health solutions are not typically intended to replace their clinical judgment, but rather as an aid.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

There is currently no specific authority or Ministry governing AI. Rather, existing regulatory frameworks, being the Privacy Act and TG Act, which are technology neutral, govern AI. There are existing voluntary frameworks advising on best practice on how to safely develop and deploy AI.

In September 2024, a proposal paper was released suggesting the introduction of mandatory guardrails for AI in high-risk

settings. The guardrails underwent consultation and may be introduced in a variety of ways including domain-specific, new framework legislation to amend existing laws or by introducing a new cross-economy Act. This was issued by the Department of Industry, Science and Research, which is therefore likely to lead more general AI regulations.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

Given there are no AI-specific regulatory schemes, AI is only regulated in healthcare where it is encompassed by existing definitions. AI tools used in healthcare can be regulated by the TGA if it can be classed as a medical device, including AI-enabled software, if it meets the definition and has a therapeutic use.

We are also seeing AI getting some attention at the State levels, typically in the form of guidance documents or policy frameworks. In some cases, these may be picked up and imposed in a contractual setting.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Following the judgment in *Commissioner of Patents v Thaler* [2022] FCAFC 62, the human inventor of the AI is the *prima facie* owner of IP rights in algorithms. As the Court discussed, there are significant complexities involved in considering to whom a patent should be granted in respect of the AI system's output. The Court considered some potential grantees, which included 'the owner of the machine upon which the AI software runs, the developer of the AI software, the owner of the copyright in its source code, the person who puts the data used by the AI to develop its output, and no doubt others'. It should be noted that the ownership may be different as between patents and copyright.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

In the context of licensing data for use in ML, the quality of the data is a critical consideration. This has significant consequences for the efficacy of the ML training and validation. It is important to understand the financial model of licensing data, in particular whether it is a 'one-off' payment or continues to reach through to secondary uses of the data, for example from the ML outputs (such as an AI model or an algorithm). The treatment of combination data sets from different sources raises complexities when allocating value, similar to the problems with royalty stacking arrangements.

Another important consideration is the applicability of any restrictions to the particular data set, which necessarily fall out of the data set's permitted purpose. Commercially, it is also important to consider who owns the rights to the data produced as a result of the ML.

It is also necessary to ensure sufficient rights to the data to allow combination with other data sets (if necessary) and the requirements, if any, to retain data in perpetuity.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

There is no distinction between standard and generative AI at present in regulation. The OAIC has released guidance documents specifically addressing concerns arising in the development and use of generative AI. The 'key takeaways' from the OAIC's document addressing concerns regarding commercially available generative AI focuses on appropriate privacy policies to ensure they are reflective of AI used by a business, as well as ensuring that personal information is not entered into public generative AI. The guidance published by the OAIC is not mandatory, but in conjunction with the Voluntary AI Safety Standard produced by the National AI Centre forms best practice in using generative AI as well as standard AI.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Australia is contemplating a legislative approach to regulating AI, but has not done so as yet. It has recently proposed mandatory guardrails that would apply to AI in high-risk settings as well as recommended guardrails to be implemented.

The OAIC has also released guidance for the use of commercially available AI products, as well as developing and training AI models, both of which are voluntary. The purpose of these guidelines is to set minimum standards on how personal information should be handled by AI.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

The OAIC guidelines for developers address key concerns of what information is appropriate to use to train AI/ML models. The key message of the guidelines is that publicly available information does not mean it is not personal information and should not be used to train generative AI models without the appropriate privacy notices. This is an important message given the difficulty of 'erasing' learnt information from certain AI products.

Using information that developers lack appropriate data rights to may also intersect with the APPs, particularly APP 6, dependent on how the information was acquired and whether training AI/ML can be considered a relevant secondary purpose.

At this stage, there are no disgorgement laws or initiatives in Australia.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

There are no specific theories of liability applying to adverse outcomes in digital health solutions. Australian tort law will

apply where the negligence of a manufacturer or seller causes an adverse outcome.

Australia's consumer law framework also establishes a number of consumer guarantees which provide an additional level of protection. Relevantly, there are consumer guarantees applying to both the sale of goods and provision of services. In relation to goods, suppliers and manufacturers guarantee that goods are of acceptable quality and are reasonably fit for any purpose the consumer or supplier specified. In relation to services, suppliers guarantee that their services are provided with due care and skill and that services will be reasonably fit for any purpose specified by the consumer.

The consumer law framework also incorporates a very broad assurance of the safety of products, which cannot be excluded or limited by contract.

9.2 What cross-border considerations are there?

In circumstances where a product is being sold to Australian consumers, the product, regardless of what it is, must conform to Australian product liability regulatory regimes. In this sense, cross-border considerations do not have an effect on liability. The party that imports the product into Australia is typically deemed as a 'manufacturer' for the purposes of the ACL, which requires the importer to comply with the consumer guarantees.

In the context of the TG Act, in order to legally import and supply a medical device in Australia, the device is required to meet the Essential Principles set out in the TG Regulations. The Essential Principles are concerned with ensuring the safe and reliable performance of medical devices. If devices are imported and supplied that do not meet the Essential Principles, civil or criminal penalties may result under the TG Act. As noted above, this may create issues with apps and other SaMDs that are downloaded, creating questions of who has imported the product.

Additionally, overseas manufacturers may be liable under the ACL, which provides a system for manufacturers' liability. Under the ACL, 'manufacturer' is defined broadly to include, amongst others, a person who produces the goods and a person who imports the goods into Australia if at the time of importation, the manufacturer of the goods does not have a place of business in Australia. That system is designed to compensate for loss or damage suffered as a consequence of goods with safety defects.

From a regulatory perspective, overseas manufacturers are unlikely to face regulatory action by the TGA. The regulatory framework is directed towards local sponsors/distributors and not overseas manufacturers. Realistically, the main scope for liability is where there is a class effect, impacting multiple patients.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

A critical factor is to ensure that the outputs of generative AI are validated and tested before being used for patient care. Protocols should be implemented around the data which is input and its accuracy. It is also important to ensure the users of the outputs are trained in the use of AI, and particularly for healthcare professionals that they understand the output is an aid and not a replacement for their clinical judgment.

Additionally, medical practitioners should warn patients about the issues of using AI to find health-related information, which could be inaccurate or simply not applicable to them. This is similar to issues faced by practitioners with patients having a source of information from internet searches.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Depending on how the healthcare data has been acquired, using it to train AI/ML models could be a breach of the APPs. It is unlikely that healthcare data will be collected for the primary purpose of AI/ML training, meaning its use for a secondary purpose is closely regulated. Considering how healthcare data is collected, it is not reasonable for an individual to expect that sensitive healthcare information would be disclosed for AI/ML training purposes and this is not related to the primary purpose of collection of the data. It is also possible that using third-party data could amount to a breach of copyright.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based services typically involve issues such as cyber-security and data protection. Given the sensitive nature of health information, particular care needs to be taken to ensure the data protocols and security mechanisms are effective and appropriate. Where cyber-security issues arise, the providers of Cloud-based services need to have appropriate disaster recovery protocols in place to limit the adverse consequences arising from a breach.

IT service providers who engage with Government health agencies will typically be required to meet certain minimum IT security standards (for example, see the Digital Transformation Agency's Secure Cloud Strategy). Where IT service providers are using Cloud-based services to share health data across borders, compliance with APP 8 is important.

There are also data location rules, for example in the My Health Record Act, as well as State and Territory health records legislation. It is also noted that recent Foreign Investment Review Board guidance suggests that acquisition of an interest in data that may be considered National Security information will be restricted.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Given the highly regulated healthcare market, non-healthcare companies must consider their ability to achieve regulatory compliance within this environment. As part of this, companies must consider the costs involved in obtaining approvals and licences, as well as the costs required to ensure ongoing compliance with the regulatory framework. Companies must also be mindful of the highly regulated marketing environment to ensure their advertising is compliant.

Importantly, non-healthcare companies must consider the heightened data privacy requirements which will apply. These are likely to be more onerous than the requirements such companies are accustomed to.

Non-healthcare companies should also ensure that the pathways to market are clear. This includes determining whether to be considered a consumer-wellness device, or make medical claims and require registration. It is also relevant for the company to contemplate market entry. Given that the Australian regulatory framework is heavily reliant on the EU, Australia often represents a useful follow-up market after European entry. Companies must ensure a relevant reimbursement pathway, since the Australian market is heavily dependent on Government subsidy if selling directly to consumers. If targeting providers of healthcare services, it is important to appreciate the different appetites and preferences as between the public and private sector.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Venture capital and private equity firms must ensure that they are aware of the regulatory environment applying to the digital healthcare venture. Firstly, this allows investors to understand the upfront and ongoing costs associated with compliance. This also allows investors to better evaluate the risks of investment, particularly given the move towards increased penalties applying to privacy and data breaches.

In terms of timing, firms should consider the approvals and licensing timeframes as these may delay investment and ultimately any return on investment that materialises. Firms should conduct general investor due diligence, including a thorough review of material IT and IP agreements. It is important that firms understand exactly what it is they are investing in, and the rights or restrictions applying to the venture's ability to commercialise this ownership.

Firms should also consider the company's ownership of, or rights to use, IP and other technology that is fundamental to the business's operations, including the rights to license its products commercially. This includes the title to such assets, issues regarding open-source software, and whether licence terms are sufficiently tailored to allow the proposed commercialisation plan. The steps taken to date in order to commercialise a product should be reviewed to ensure that the steps taken will not need to be repeated in order to comply with the regulatory framework. We tend to see companies either pursuing a US- or EC-centric pathway, and these are not necessarily very compatible. It is also important to consider the success rate of, and timelines for, registration for the therapeutic goods developed by the digital healthcare venture.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Currently, there are several barriers impeding the widespread clinical adoption of digital health solutions. Firstly, data privacy, security and the associated consequences of a breach are a significant barrier. Further, as highlighted above, there is an insufficient legislative framework in place to regulate and support the implementation of digital health solutions adequately. The development of bespoke laws relating to digital health technologies may encourage and support more widespread clinical adoption. Further, digital health trends are focusing more on patients rather than clinicians, which can limit take-up.

The difficulty of sharing health information, and the fact that some collectors see it as their valuable asset, inhibits the flow on health information in a patient-centric fashion.

It is also necessary to note that uptake of emerging technologies can be slow, depending on the capital expenditure necessary, particularly in the public health system. Indeed, given the financial constraints on the overall health system, the offering of additional functionality is hard to sell, unless there is a real, relatively short-term cost-saving dividend to be realised.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In Australia, the key clinician certification bodies that influence the clinical adoption of digital health solutions are:

- the Australia Health Practitioner Regulatory Agency; and
- the Royal Australia College of General Practitioners.

Additionally, while not being a clinician certification body, the Australian Government has established the ADHA, which is a Commonwealth entity that seeks to create a collaborative environment to accelerate adoption and use of innovative digital services and technologies. The ADHA is trying to significantly influence the clinical adoption of digital health solutions by advancing the digital capability of Australia's health workforce. The ADHA typically takes a guidance role, which results in a need for customers to make their own judgment regarding products.

It is also necessary to consider the role of the Medicare Services Advisory Committee ('MSAC'), which appraises new technology and products for public funding. The MSAC is responsible for undertaking a health technology assessment ('HTA') to demonstrate quality, safety, efficacy and cost effectiveness of proposed health services. This area is presently under review, and there is considerable uncertainty as to what new model may emerge.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

Whether patients who utilise digital health solutions are reimbursed depends upon the particular digital health solution in question. Generally, the Australian Government aims to assist Australians in accessing digital health products and services. This is achieved by subsidising the cost of health-related goods and services, including through the Pharmaceutical Benefits Scheme (subsidies for certain medicines) and the MBS (subsidies for certain health services). The MBS applies to cover the cost of certain medical devices.

In the wake of the COVID-19 pandemic, telehealth services were permanently made available under the MBS. Further, where a patient has appropriate cover, private health insurers are required to pay benefits for products listed on the Prescribed List of Medical Devices and Human Tissue Products, which is published by the Australian Government Department of Health and Aged Care. This list includes various quasi digital health products such as insulin infusion pumps.

However, there is little direct reimbursement for patients for digital health solutions. There are some efforts by private

health insurers to encourage wellness activities, and therefore the use of relevant devices. However, this is limited by private health insurance regulations.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

The key gaps in Australia's existing framework stem from the non-specific regulatory regime that is currently in place. AI/ML-based solutions in digital healthcare face regulatory issues in terms of standards of privacy, algorithmic discrimination and automation bias, as well as misinformation and disinformation.

The provenance of data is also a real issue. A key concern is consent, potentially de-identification and confidentiality obligations. As noted above, cogent evidence of consent in respect of de-identified data is quite problematic.

New legislation has been proposed to address gaps pervading the healthcare ecosystem. The proposed mandatory guardrails for AI in high-risk settings is likely to apply to many healthcare settings; likewise, the recent bill to combat disinformation and misinformation also aims to address due diligence gaps that leave the capabilities of AI and like technology in the healthcare space unverified.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

The following are highlighted as trends or developments that will affect the adoption and development of various types of digital health solutions:

- Because so much of the health system is funded by Government or private health insurers, the mechanism by which reimbursement levels for these technologies is established is critical. A critical HTA review has recently been completed, and we are awaiting the implementation phase. It is expected that digital health products seeking reimbursement may have clearer pathways, but will be required to not only provide evidence of utility, but also actual savings and likely uptake. The collection of this sort of data needs to be an area of focus.
- Significant reforms to the Privacy Act are underway, with some already passed and scheduled for implementation. These are continuing the ratcheting up of standards, and penalties for breach of the same. At the same time, cyber-security has become an area of particular focus, especially where an incident may impact the operational effectiveness of hospital systems. We are seeing much more intrusive investigation of the cyber-security aspects of digital health products, both at the time of tender and in resulting contracts.
- Companies using digital health tools to get closer to, and more tightly bind themselves to, patients – This trend started with some tools used in the context of clinical trials, to Patient Support Programs with adjunctive digital health support tools, which are becoming increasingly sophisticated and very much part of the patient treatment journey. The sophistication of these tools is increasing to the point where some may fall within the scope of regulated SaMDs.
- By-passing – Whereby consumers are using digital health solutions, typically apps, which the TGA considers are medical devices, and how it addresses this issue.

Bernard O'Shea has been working in the life sciences sector for over 30 years. He has an extensive practice based around the development and commercialisation of products in this sector. His experience encompasses the whole spectrum of regulatory and reimbursement issues the sector confronts. His background in computer science, and many mandates involving privacy and data issues, mean he is adept at assisting clients in the digital health sector. He is recognised by *Chambers Life Sciences Guide* as a Tier one practitioner, and is much sought after for his incisive and strategic advice around emerging issues. Bernard has had the rare privilege of assisting multiple clients to bring novel products to market, and is actively involved in assisting multiple digital health companies to develop their products, protect their data and satisfy their regulatory obligations.

Norton Rose Fulbright
Level 38, Olderfleet, 477 Collins Street
Melbourne
Australia

Tel: +61 3 8686 6573
Email: bernard.oshea@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/bernard-oshea

Rohan Sridhar is a commercial, regulatory and IP Partner based in Melbourne. He practises extensively in the life sciences sector. His experience in the sector covers the full life cycle of pharmaceutical, biotech and med tech products, from discovery to commercialisation. This includes foundational IP licences, research and development collaborations, clinical trials, product registration, pricing and reimbursement, manufacturing, marketing, warehousing, distribution, import/export and recalls. Rohan is also experienced in assisting start-up and spin-out entities with corporate management and fundraising. Rohan has assisted a number of digital health companies to access, develop and commercialise their technologies.

Rohan also advises clients in relation to privacy-related issues, including issues around transfer of data sets and the export of personal information.

Rohan's background in pharmacology enables him to understand the complexity of products existing in this sector and deliver pragmatic and commercial advice to clients.

Norton Rose Fulbright
Level 38, Olderfleet, 477 Collins Street
Melbourne
Australia

Tel: +61 3 8686 6670
Email: rohan.sridhar@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/rohan-sridhar-21477252

Belarus


Marina Golovnitskaya


Yauheni Budchanka

Alba LLP

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

Under Belarus law, digital health is a set of information systems and resources, and information and communication technologies, functioning in the healthcare sector on the basis of common principles and rules, providing information interaction between organisations and citizens, as well as serving their information needs. This definition is included in the Concept for the Development of Digital Health in the Republic of Belarus for the period up to 2022 (**Concept**), approved by the order of the Ministry of Healthcare. The Concept sets key goals, objectives and principles of digital health development as well as expected results. The definition has not been changed since 2022.

Another definition of "digital health" was elaborated in the Model Law on Digital Health approved by the Regulation of the Interparliamentary Assembly of Member States of the Commonwealth of Independent States (**CIS**) No. 55-22 dated 14 April 2023. Digital health is defined as a method of planning and managing healthcare, organising and providing medical care, ensuring prevention and developing a healthy lifestyle, providing information support to citizens and healthcare professionals based on digitalisation using the results of continuous data processing in digital form, which significantly increases their effectiveness through the use of modern methods of processing and analysing such data (including artificial intelligence (**AI**) methods), and also forms a systemic information basis for making management and medical decisions, significantly affecting the effectiveness, quality and safety of services and activities in the healthcare sector. This definition is not in legal force in Belarus, as the Model Law has not been implemented in Belarus at the national level.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

One of the main directions of digital health in Belarus is the creation and use of the Centralised Healthcare Information System (**CHIS**), which is an integrated information system that provides centralised storage and processing of medical information, as well as users' access to it in accordance with the established procedure.

In 2024, the Order of the President "On the Centralised Healthcare Information System" (**Order**) was adopted, establishing principal directions of the CHIS development. Importantly, the Order specified subsectors/subsystems of the CHIS, which should be developed and introduced in 2024–2025. The work on the CHIS project is organised in two stages respectively per year.

The first stage (planned for 2024) included the creation of:

- integrated electronic medical records (**EMRs**) (e.g. patient registry, repository of structured and unstructured medical information about patients);
- regulatory and reference information (e.g. repository of centralised information about healthcare organisations and specialists);
- patients' personal accounts (e.g. quick access to personal medical information, self-registration for appointments with healthcare professionals);
- management of infrastructure modules (e.g. ensuring uninterrupted and trouble-free operation of the CHIS); and
- an information security subsystem (e.g. control of access to medical information, the CHIS users' registration).

The second stage (planned for 2025) includes the creation of:

- a cloud-based medical information system (e.g. unification of healthcare services provision, maintenance of EMRs);
- a unified laboratory trials system;
- a unified medical images archive;
- patients queue management (e.g. patient flows between healthcare organisations, hospitalisation scheduling, maintenance of waiting lists); and
- an informational and analytical subsystem (e.g. a decision-making tool based on big data, forecasting demand for healthcare services and planning medical processes and procurement).

Moreover, telemedicine technologies are currently the most developed part of the digital health sector in Belarus, enabling the provision of medical assistance to patients remotely, conducting medical monitoring and medical examinations, as well as consultations between medical specialists. Please see question 3.1 for details.

1.3 What is the digital health market size for your jurisdiction?

There is no publicly available information on the digital health market size in Belarus.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

The CHIS is a state information system, the general coordination of which is carried out by the Ministry of Healthcare.

The Republican Scientific and Practical Centre for Medical Technologies, Informatisation, Management and Economics of Healthcare is the CHIS operator. Consequently, currently the main players in digital health in Belarus are the state, state authorities and organisations, so it is not possible to highlight the five largest (by revenue) companies in the digital health sector.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Please see question 1.4 for details. It is not possible to highlight the five fastest growing companies in the digital health sector.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The principal regulatory authority for digital health is the Ministry of Healthcare of the Republic of Belarus. The Ministry of Healthcare has the role of organising the provision of healthcare to the population, providing pharmaceuticals and medical devices, conducting scientific research and training scientists, and providing information support in the field of healthcare. There are state organisations under the supervision of the Ministry of Healthcare which assist it in carrying out its functions and duties.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

Regulation of healthcare in Belarus, including digital health, is covered by the Law of the Republic of Belarus "On Healthcare" (**Law on Healthcare**). It establishes the specifics of the regulation of health information support.

There are also core legal acts of the government and sectoral authorities that regulate some issues of digital health, such as: the Order; Regulation of the Council of Ministers "On Functioning and Using the Centralised Healthcare Information System"; Regulation of the Ministry of Healthcare "On Approval of the Provision on the Specifics of Providing Medical Care Using Telemedicine Technologies"; and the Order of the Ministry of Healthcare "On Certain Issues of Telemedicine Consulting in the Republic of Belarus".

The general regulation of medical devices is contained in the Law on Healthcare. The Regulation of the Council of Ministers "On State Registration (Re-registration) of Medical Devices and Medical Equipment" describes the medical devices registration procedure for legal entities and individual entrepreneurs engaged in their production, import, sale and use. Registration is conducted by the Centre for Examinations and Tests in Healthcare.

AI, generative AI, SaaS, software as a medical device (**SaMD**), and combination product regulatory approvals are not specifically regulated by Belarus law.

The general rules for the regulation of information protection, including personal data, creation and use of information resources, information systems and information networks are contained in the Law of the Republic of Belarus "On Personal Data Protection" (**Law on PDP**) and the Law of the Republic of Belarus "On Information, Informatisation and Data Protection".

The particularities of the legal regulation of information relationships concerning state secrets and medical secrets, as well as specifics in terms of personal data protection, are regulated by the Law of the Republic of Belarus "On State Secrets" and the Law on Healthcare.

Regulation of the anti-kickback issues is stipulated in the Law of the Republic of Belarus "On Measures to Prevent Legitimisation of Money Obtained by Criminal Actions, Financing of Terrorist Activities and Financing Weapons of Mass Destruction Proliferation".

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The key areas of enforcement relating to digital health are confidentiality, data security, data protection obligations, legal qualification as a medical device, medical secrecy regime, liability in case of damage, safety and intellectual property specifics.

In addition, the new Code "On Healthcare" is to be adopted in 2025 (**Project Code**). The Project Code affects some digital health regulations, including SaMD, AI, VR and 3D printing matters. This Code is under public discussion until 1 February 2025, and its wording may be amended until its adoption.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

Belarus legislation does not contain legal regulation of SaMD as of January 2025.

In Belarus, medical devices mean any instruments, apparatus, devices, equipment, materials and other items that are used for medical purposes separately or in combination with each other, as well as with accessories necessary for the intended use of medical devices (including special software), intended by the manufacturer to provide medical care, including monitoring of the human body, conducting medical research, recovery and other uses. This definition, as well as general questions of regulation of the circulation of medical products, is contained in the Law on Healthcare.

Therefore, software should not be identified as a medical device, but may be an accessory necessary for the use of a medical device, unless they have suitable features (e.g. accompanying hardware).

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

In Belarus, there are currently (as of January 2025) no regulations that apply to AI/ML-powered digital health devices or software solutions. The Project Code contains provisions regarding implementation of these technologies in the healthcare system, but regulations upon the matter have not been developed yet.

Being essentially software, they should not be subject to medical device regulations, unless they have suitable features. For example, if relevant software is accompanied with certain

hardware, it may be subject to medical device regulations. As a general rule, medical devices are allowed for production, sale and medical use in Belarus after their state registration or registration within the Eurasian Economic Union.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

To the best of our knowledge, state authorities agree with the fact that AI/ML-based digital health solutions are extensively developing, including in healthcare sector; however, comprehensive regulatory solutions are not proposed as of January 2025. The Project Code might assign certain duties to the Committee on Bioethics, which is subordinate to the Ministry of Healthcare, to develop expertise in the field of AI in medicine.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

In Belarus, there are currently (as of January 2025) no regulations that apply to clinical validation data in the course of regulatory considerations for AI/ML-based digital health solutions.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

There are no differences related to digital health products and solutions regulations in Belarus. All the regulatory authorities of every Belarus region should stick to the unified policy in this regard, as described in this chapter.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

There are no specific regulations that apply to enforcement actions digital health products and solutions in Belarus.

Instead, general enforcement actions should apply. Namely, state supervision over the circulation of medical devices is carried out by the state institution "*Gospharmnadzor*" in accordance with the legislation on control (supervisory) activities. This supervision is carried out in the forms of scheduled and unscheduled inspections, technical and preventive activities.

Other state authorities within their competence may conduct such supervision as well. For instance, the National Personal Data Protection Centre, the Belarusian data protection authority (**DPA**), monitors compliance with data protection legislation.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Telemedicine technologies are one of the most innovative IT manifestations in healthcare in Belarus as of January 2025.
  Personal data protection in the framework of medical secrecy regime seems to be the core issue in telemedicine regulation. The introduction of an intelligent system for remote monitoring of health (telemedicine, robotics in high-tech operations) is provided for in the programme of social and economic development of the Republic of Belarus for 2021–2025.
  Telemedicine technologies are defined as information technologies integrated in the CHIS that provide for remote interaction of healthcare professionals between each other and with patients for the purposes of:
  - conducting medical consultations;
  - providing an additional medical opinion on the assessment of a patient's health status, clarifying the diagnosis, determining the prognosis and methods of medical care;
  - healthcare professionals remotely carrying out medical monitoring of a patient's health after an in-person appointment (examination, consultation); and
  - conducting medical examinations.

  Telemedicine consultations are divided into the following types:
  - online consultations – they are based on video-conferencing in the "point-to-point" mode or multi-point video-conferencing during consultations, lectures, conferences or discussions for the analysis of complex pathology; and
  - offline consultations – telemedicine EMRs placed on the republican telemedicine server using specially organised software are analysed by healthcare professionals who form advisory opinions and recommendations for the treatment of the patients being consulted.
- **Robotics**
  There are no specific robotics regulations in Belarus healthcare as of January 2025.
  The introduction of an intelligent system for remote monitoring of health (telemedicine, robotics in high-tech operations) is provided for in the programme of social and economic development of the Republic of Belarus for 2021–2025.
  Legal qualification as a medical device, personal data protection in the framework of medical secrecy regime and liability in case of damage seem to be the core issues in case special regulation is introduced with regard to robotics in healthcare.
- **Wearables**
  There are no specific wearables regulations in Belarus healthcare as of January 2025.
  Legal qualification as a medical device, considering wearables may have functions different to a medical nature, processing personal data considering the medical secrecy regime and safety seem to be the core issues in case special regulation is introduced with regard to wearables in healthcare.
  According to the Project Code, as part of digitalisation of healthcare, solutions based on AI and other innovative approaches shall be developed and implemented (wearables are given as an example). Thus, the issue is reasonably relevant.
- **Virtual Assistants (e.g. Alexa)**
  There are no specific virtual assistant regulations in Belarus healthcare as of January 2025.

To the best of our knowledge, virtual assistants (such as Alexa or Siri) do not have special medical functions. They potentially can be used for collecting medical information from patients. In this case, legal qualification as a medical device and processing personal data considering the medical secrecy regime seem to be the core issues in case special regulation is introduced with regard to virtual assistants in healthcare.

- **Mobile Apps**
  There are no specific mobile app regulations in Belarus healthcare as of January 2025.
  To the best of our knowledge, the Eurasian Development Bank, an international financial institution whose members are Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia and Tajikistan, launched the mobile app "Travelling without COVID-19" during the relevant pandemic. This app serves the purposes of collecting results of COVID-19 tests and demonstrating them when crossing borders.
  The implementation of mobile applications in healthcare is included in the priorities of the CIS, of which Belarus is a member.
  Legal qualification as a medical device and processing personal data considering the medical secrecy regime seem to be the core issues in case special regulation is introduced with regard to mobile apps in healthcare.
- **Software as a Medical Device**
  There are no specific healthcare regulations in Belarus with regard to software considered as a medical device as of January 2025.
  Legal qualification as a medical device considering such software has other components and may have functions different to a medical nature and processing personal data considering the medical secrecy regime seem to be the core issues in case special regulation is introduced with regard to software considered as a medical device.
  Please also see the comments regarding legal protection of such software from an intellectual property perspective in question 6.5.
- **Clinical Decision Support Software**
  There are no specific healthcare regulations in Belarus with regard to clinical decision support software as of January 2025.
  Legal qualification as a medical device, processing personal data considering the medical secrecy regime and medical ethics seem to be the core issues in case special regulation is introduced with regard to clinical decision support software.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  There are no specific AI/machine learning (**ML**) regulations in Belarus healthcare as of January 2025.
  Processing personal data considering the medical secrecy regime, liability in case of damage and interaction with healthcare professionals seem to be the core issues in case special regulation is introduced with regard to AI/ML in healthcare.
  Please also see the more detailed comments in questions 8.1–8.7.
- **IoT (Internet of Things) and Connected Devices**
  There are no specific IoT regulations in Belarus healthcare as of January 2025. IoT-connected devices can be used to provide remote health monitoring and emergency alert systems.
  Legal qualification as a medical device and processing personal data considering the medical secrecy regime seem to be the core issues in case special regulation is introduced with regard to IoT and connected devices in healthcare.
- **3D Printing/Bioprinting**
  There are no specific bioprinting regulations in Belarus healthcare as of January 2025.
  The development of new methods of treatment based on bioprinting is provided for in the programme of social and economic development of the Republic of Belarus for 2021–2025. According to the Project Code, 3D printing is considered as an innovative solution for digitalisation of healthcare.
  Licensing such type of activity, legal qualification from civil law and intellectual property perspective, medical ethics and liability seem to be the core issues in case special regulation is introduced with regard to bioprinting.
- **Digital Therapeutics**
  There are no specific healthcare regulations in Belarus with regard to digital therapeutics as of January 2025.
  Licensing such type of activity, legal qualification as a medical device, processing personal data considering the medical secrecy regime, liability in case of damage and interaction with healthcare professionals seem to be the core issues in case special regulation is introduced with regard to digital therapeutics.
- **Digital Diagnostics**
  There are no specific healthcare regulations in Belarus with regard to digital diagnostics as of January 2025.
  The Project Code (which might enter into force in the future), however, refers to digital diagnostics within implementation of clinical decision support systems as a tool for healthcare professionals.
  Processing personal data considering the medical secrecy regime, liability in case of damage and interaction with healthcare professionals seem to be the core issues in case special regulation is introduced with regard to digital diagnostics.
- **Electronic Medical Record Management Solutions**
  EMR management solutions are actively developing in Belarus and are represented by EMRs of patients and personal electronic accounts of patients.
  Personal data protection in the framework of medical secrecy regime seems to be the core issue in the EMR management solutions.
  EMR is defined as a structured collection of electronic medical documents, including information about the patient's state of health, visits to healthcare professionals, and other details, maintained within the CHIS.
  A personal electronic account is a web-interface providing the patient with access to the nationwide automated information system, designed to facilitate electronic interaction with the CHIS. In other words, this account enables patients to schedule appointments with healthcare professionals, access their EMRs, and interact with other healthcare services.
- **Big Data Analytics**
  There are no specific healthcare regulations in Belarus with regard to big data analytics as of January 2025.
  One of the key objectives in the digital development of healthcare, according to the Project Code, is the accumulation of big medical data to train AI.
  Processing personal data considering the medical secrecy regime seems to be the core issue in case special regulation is introduced with regard to big data analytics.

- **Blockchain-based Healthcare Data Sharing Solutions**
  There are no specific healthcare regulations in Belarus with regard to medical data sharing based on blockchain as of January 2025. Blockchain in healthcare may be used to facilitate data sharing between patients, medical institutions and EMR systems.
  Processing personal data considering the medical secrecy regime seems to be the core issue in case special regulation is introduced with regard to blockchain-based healthcare data sharing solutions.
- **Natural Language Processing**
  There are no specific healthcare regulations in Belarus with regard to natural language processing as of January 2025.
  Legal qualification as a medical device and processing personal data considering the medical secrecy regime seem to be the core issues in case special regulation is introduced with regard to natural language processing in healthcare.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Digital platform/solution providers face issues derived either from lack of specific regulation in relevant regulation or continuous development of the legal framework in the sphere.

Providers of those digital platforms that are being developed and operated as a part of state digital healthcare mostly focus their efforts on the creation and implementation of platforms in line with scope, time and budgets agreed for their development.

All the issues referred to in answer to question 3.1 above are relevant for digital platform providers, as well as specific obligations related to platform operation that may be prescribed in the legal acts regulating particular digital solutions/platforms (e.g. those developed for the use of telemedicine in Belarus).

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The key issue to consider for use of personal data is the correlation between general requirements for personal data protection and specific rules established in the healthcare sphere. Personal data operated in healthcare may also be subject to the medical secrecy regime, which triggers protection of the same information both from personal data and medical secrecy perspectives. Under medical secrecy, the following information should be protected:

- information about a patient's request for medical assistance and his/her health status;
- data about diseases;
- diagnosis;
- possible methods of medical assistance;
- risks related to medical intervention as well as alternatives to it; and
- other data, including personal data, obtained when providing medical assistance, and results of postmortem examinations.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Regulation of personal data is implemented at the state level and exists mainly in the form of the Law on PDP and the Law on Healthcare, which apply equally to all individuals, private or public entities, authorities and other defined subjects in Belarus.

The DPA is the authorised body responsible for protecting the rights of personal data subjects and controlling of personal data processing by operators, regardless of their nature or level of operation.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

A service provider should take into account the territorial scope of the Law on PDP, which does not specify whether it has an extraterritorial effect.

The definition of the operator (analogue to the controller under the GDPR) comprises "other organisations" without clarification on whether foreign organisations processing personal data of Belarusians are concerned. However, the DPA currently maintains the position that the scope of the Law on PDP is limited to the territory of Belarus and does not apply to foreign organisations having no local presence. Therefore, providing services and performing processing of personal data from abroad by a non-Belarusian legal entity without local presence should not fall in the direct scope of the Law on PDP application.

Application of the Law on PDP does not differ depending on the state/private type of company ownership. Laws may establish specific requirements/obligations for personal data processing. Should processing of personal data apply to biometric and genetic data or other special categories stipulated by the Law on PDP, a special regime of protection is required. As a general rule, processing of such special personal data without the consent of the data subject is prohibited. However, as one of the exemptions, this consent is not required for purposes of organising medical care, provided that such personal data is processed by a healthcare professional who is obligated to ensure the protection of personal data and is subject to the medical secrecy regime.

4.4 How do the regulations define the scope of personal health data use?

The Law on PDP covers the protection of personal data while processing of such data is accomplished with the use of:

- automated means (tools); or
- non-automated means (tools), if such means (tools) provide the possibility to search for personal data and/or access personal data with the help of certain criteria (card indexes, lists, databases, logs, etc.).

Processing means any type of actions taken in relation to personal data, including the collection, systematisation, storage, modification, use, depersonalisation, blocking, distribution, provision and erasure of personal data.

The Law on PDP will not apply to the processing of personal data that is:

- accomplished for personal use, not relating to professional and entrepreneurial activity; or
- related to state secrets.

As for the scope of data use, it may be established either by the operator itself (e.g. describing the purpose and scope of processing in a privacy policy, when the processing performed is based on consent) or established in the legislation (e.g. a particular number of data that should be reflected in the patient file).

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

An operator may authorise another person or entity for the processing of personal data based on the agreement. The agreement between the operator and the authorised person should contain the following provisions:

- a list of actions with regard to personal data that could be performed by the authorised person;
- the purposes of the above actions;
- confidentiality obligations with respect to personal data; and
- measures to ensure the protection of personal data in accordance with the Law on PDP.

Mandatory measures to ensure the protection of personal data are:

- legal measures, such as publication of documents defining the policy of the operator (authorised person) regarding the processing of personal data;
- organisational measures, such as: appointment of a structural unit or a person responsible for the control over the processing of personal data (Data Protection Officer); familiarisation of employees and other persons directly engaged in the processing of personal data with the provisions of the legislation on personal data, including the requirements for the personal data documents of the operator (authorised person), as well as training of these employees and other persons; establishing the procedure for accessing personal data; and
- technical measures, such as implementation of technical and cryptographic protection of personal data.

Notwithstanding the terms of the agreement, the operator remains the party responsible for the proper processing of personal data (but not the authorised person).

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The Law on PDP introduces a number of principles, including the following:

- processing of personal data should be proportionate to the stated purposes of their processing and ensure at all stages of such processing a fair balance of the interests of all interested parties;
- content and volume of personal data processed should correspond to the stated purposes of their processing – the personal data processed should not be excessive in relation to the stated purposes of their processing; and
- the operator is obliged to take measures to ensure the accuracy of the personal data processed by it and, if necessary, update them.

Current legislation does not establish the right not to be subject to automated decision-making in terms of personal data processing.

There is no specific regulation of data bias and/or discrimination in the healthcare sphere in Belarus as of January 2025.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The Law on PDP provides for a specific list of legal bases for the processing of personal data. Generally, the processing of personal data is carried out on the basis of the data subject's consent. Exceptions to that rule are stipulated by the Law on PDP and other legislative acts. The list of legal bases vary depending on the type of personal data: special (sensitive); or other types.

The laws in the sphere of healthcare also provide for certain deviations for the general requirements in certain aspects. For instance, healthcare regulations establish specific procedure for giving consent to process personal data and information that constitutes medical secrecy in the CHIS. Moreover, information constituting medical secrecy could be disclosed without the patient's (his/her legal representative's, guardian's, spouse's or close relative's) consent in certain cases as defined in legislation (e.g. upon written request of bodies of criminal prosecution and courts in relation to conducting an investigation or court proceedings).

With regard to clinical trials, participation of patients in clinical trials is voluntary and subject to written, informed consent. The investigator must fully inform a potential patient or their legal representative about all significant aspects of a trial, *inter alia*, providing information about the trial in writing.

Operators should also note other key requirements, such as rules for cross-border transfer, requirements for the contracts with authorised persons (analogue to the processor under the GDPR), respect for the rights of data subjects, developing data processing policies, etc.

To the best of our knowledge, no initiatives are currently being undertaken by the authorities in this regard. In our opinion, the existing regulations should apply to personal data used and collected within the CHIS.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

When sharing personal data, one should generally consider (i) the availability of proper legal basis for sharing data, e.g. consent of the data subject, and (ii) whether the sharing party complies with cross-border data transfer requirements (if applicable).

Personal data may also be subject to the medical secrecy regime, which triggers protection of the same information as medical secrets. This, among others, affects the scope of the parties who may claim for sharing information that constitutes a patient's medical secrets.

In particular, the patient has the right to decide to whom information about his/her health condition can be disclosed, or to forbid disclosure to certain persons. Medical secrecy concerning a patient who is a minor is provided to the patient's legal representatives: parents; adoptive parents; guardians; custodians; etc. If the patient is not able to make a conscious decision due to health reasons, information constituting medical secrecy may be shared with the patient's spouse or one of their close relatives (parents, adult children, siblings, grandchildren, grandparents). The persons mentioned above have the right to receive extracts from medical documents, medical certificates on the state of health and other documents containing information on the patient's health, in accordance with the procedure established by Belarus legislation. Legislation also stipulates cases in which medical secrecy may be provided to certain public authorities and organisations without the consent of the patient or persons mentioned above.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Personal data sharing, including data subject to the medical secrecy regime, is regulated uniformly at the state level without any specifics or waivers in regions.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Regarding the personal data requirements, please see the answer to question 4.3.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Regarding laws and initiatives for sharing healthcare data, please see the answer to question 4.7.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

There is no specific regulatory framework in relation to federated models of healthcare data sharing. Regarding this issue, please see sections 4 and 5.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

The main Belarus legal act describing patent protection is the Law of the Republic of Belarus "On Patents for Inventions, Utility Models, Industrial Designs". Medical devices and equipment containing digital health technologies can be patentable under the provisions of this law.

The exclusive right to an invention is protected and is certified by a patent which is issued upon application. The scope of patent protection related to an invention is determined by the invention claims.

Legal protection is granted to an invention in any field of technology (e.g. medical devices and equipment containing digital health technologies), if it relates to a product or a method, appears as novel, involves an inventive step and is industrially applicable. Product implies an object of human labour. Method denotes a process, technique or method of performing interrelated actions on a material object with the help of material means.

According to Belarus law, only an individual can be the invention creator; the status of AI activities is debatable.

Computer programs and mathematical methods are not patentable *per se*. However, if the invention (1) meets the above criteria, and (2) is created with the help of computer programs or AI, it may be patentable.

The exclusive right to use an invention includes the right to use the invention at one's own discretion, assuming this does not violate the rights of others, and the right to prohibit others from using the invention.

The patent term related to an invention is 20 years from the application filing date (in some cases this term may be extended, but by no more than five years).

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

The main Belarus legal act describing copyright protection is the Law of the Republic of Belarus "On Copyright and Related Rights". General copyright rules apply to digital health technologies that are eligible to obtain copyright protection.

Computer programs (including software, source code, designs) are eligible for copyright protection. For instance, software used for the functioning of a medical device, provided that the threshold of copyrightability is achieved, is protected by copyright in general order.

Copyright protection arises by virtue of the fact of its creation. Acquisition and exercise of copyright do not require any formalities (e.g. receiving protection documents).

Copyright protection extends to works of science, literature and art that are the result of creative activity, regardless of the purpose and dignity of the works, as well as the way they are expressed.

Copyright is protected with regard to both published and unpublished works which exist in some objective form, for example: in sound or video recordings (mechanical, magnetic, digital, optical, etc.); or in electronic form, including in digital form.

Copyright does not extend to ideas, methods, processes, systems, concepts, principles, discoveries or facts, even if they are expressed, displayed, explained or embodied in a work.

According to Belarus law, only an individual can be the author of a particular work and the status of AI activities is debatable.

There are two types of rights under copyright: economic rights, which allow the owner of the rights to derive financial reward from the use of the works by others; and moral rights, which allow the author to take certain actions to preserve the personal link between himself/herself and the work. Economic rights are valid, as a general rule, during the life of the author and 70 years after his/her death, according to the recent amendments to the Civil Code. Moral rights are protected indefinitely.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

The main Belarus legal acts describing trade secret protection are the Civil Code of the Republic of Belarus and the Law of the Republic of Belarus "On Commercial Secrecy". Trade secret protection for digital healthcare technologies in Belarus is governed by the same legal acts that regulate trade secrets in general, with no specific provisions for this sector. However, it is important to note that data, which falls under the medical secrecy regime, is not eligible for protection as a trade secret.

Information constituting a trade secret is protected under the regime of commercial secrecy, if all of the following criteria are met:

- it is not generally known or available to third parties that usually deal with this kind of information;
- it has commercial value for its owner due to being unknown to third parties;
- it is not an object of exclusive rights to the results of intellectual activity; and
- it is not a state secret.

The commercial secrecy regime is considered to be established after (1) determining the list of information subject to protection, and (2) taking a set of measures necessary to ensure confidentiality by the information owner.

The legislation also defines the list of information that cannot fall under the commercial secrecy regime, for example: medical; attorney; banking; tax; or other secrets protected by law or information about the state of the environment.

The trade secret owner has the right to use and protect the trade secret from being used by others without permission under the condition that this trade secret is under the commercial secrecy regime. Trade secrets are protected without any procedural formalities (registration, acquisition of a certificate, etc.). They are not formally limited by any term and are valid while the above-mentioned criteria are met.

Unpatented digital technologies or medical devices, etc. can be protected as a trade secret, i.e.:

- trade secret protection can appear as an alternative to patenting; and
- if the rightsholder can obtain patent protection with regard to a significant solution, the information needed for its realisation may be protected as a trade secret.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Academic technology transfers are not regulated in detail in Belarus as of January 2025. Overall, in such cases general rules related to works and inventions for hire should apply.

A work for hire is a work created in the course of performing an official assignment or official duties by an employee. The moral rights belong to its author; the economic rights belong to the author's employer.

An invention for hire is the invention that relates to the field of the employer's activity, and the activity that led to its creation relates to the official duties of the employee. Alternatively, the invention for hire may be created in the course of completing a specific task received from the employer, or the employee used the employer's experience or funds. The moral rights belong to the creator of the invention for hire; the right to obtain a patent and the economic rights belong to the creator's employer, unless otherwise provided by the agreement between them. By acquiring the economic rights, the employer also acquires the obligation to pay appropriate remuneration to the employee, of which the minimum amount is established by law.

Furthermore, Belarus law establishes obligatory commercialisation of the results of scientific activities at the expense of public funds. Intellectual property and documented scientific and technical information created in the course of scientific activity at the expense of public funds, in accordance with agreements for performing research, development and technological work, are considered as the results of scientific activity. Please see question 6.7 for more details.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Belarus law does not specifically describe protection for SaMD.

Software being interpreted as a computer program is not patentable in Belarus. As mentioned in question 6.2, software is eligible for copyright protection. If software is a component of a medical device consisting of some other components (e.g. hardware), such medical device may still be patentable.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

No, an AI device cannot be named as an inventor of a patent in Belarus. According to Belarus law, only an individual can be the invention creator. Therefore, we believe that the results of AI activities (e.g. devices) cannot be granted legal protection as inventions.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

The main Belarus legal act describing the rules applicable to government-funded inventions is the Edict of the President of the Republic of Belarus "On Commercialisation of the Results of Scientific and Scientific-Technical Activities Created at the Expense of Public Funds".

According to this Edict, Belarus law establishes obligatory commercialisation of the results of scientific activities at the expense of public funds. Intellectual property and documented scientific and technical information created in the course of scientific activity at the expense of public funds, in accordance with agreements for performing research, development and technological work, are considered as the results of scientific activity. Commercialisation implies the following options (the list is not exhaustive):

- sale of goods created with the use of the results of scientific activity, or use of these results for other needs;
- fee-based or gratuitous license of the right to use the results of scientific activity;
- fee-based or gratuitous assignment of property rights to the results of scientific activity;
- fee-based or gratuitous transfer of information constituting trade secrets; and
- fee-based or gratuitous transfer of documented scientific and technical information.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

We are not aware of precedents affecting intellectual property rights protection of digital health innovations in Belarus. Importantly, court decisions in Belarus are not regarded as a source of law, but may tacitly affect law-enforcement practice.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

In addition to determining: collaboration purposes; participants' rights and obligations; applicable regulations and liability allocation; and collaboration termination, it is also important to determine a specific intellectual property regime that should be applicable to the specific collaboration improvements. Allocation of IP rights that have resulted from collaborative improvements, is core for parties to technology-driven collaboration agreements.

In data-driven collaborations it is important to deal with privacy considerations. Both the company, which receives and processes data to achieve some digital health solutions, and the company providing such data, should meticulously comply with data privacy legislation to avoid any regulatory risks.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

Firstly, such agreements must comply with the general principles and rules of Belarus civil law on agreements, as well as competition legislation. Secondly, data privacy compliance with a particular focus on medical secrecy. In addition, prices and tariffs in the healthcare sector are regulated by the state, therefore pricing requirements must also be complied with. Finally, with regard to agreements between Belarus residents and non-residents, it is important to comply with local foreign trade rules.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Being data-driven agreements, federated learning healthcare data sharing agreements should meticulously comply with data privacy legislation to avoid any regulatory risks. Parties should consider data privacy issues at the stages of primary data collection and processing. They also should ensure that no personal data inadvertently leaks into federated models. Provisions highlighting responsibility for privacy concerns should be included in the data sharing agreement, along with mechanisms for addressing potential breaches or non-compliance.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Generative AI models rely on a huge amount of data while training and processing medical data. Therefore, the principal concern that should be addressed is data privacy.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

AI/ML regulation in Belarus has not developed sufficiently yet, and as a result no specific authorities have been designated to regulate this matter.

According to the Edict of the President of the Republic of Belarus "On Legal Policy Concept" dated 2023, one of the key directions for the development of law in Belarus will be the establishment of regulations governing the application of AI. The Project Code also mentions the importance of AI usage in healthcare, but not its regulation.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

Authorities responsible for introducing regulatory schemes related to AI/ML are not designated in Belarus as of January 2025. As to healthcare, in our opinion, the Ministry of Healthcare may be a key regulator and should control the respective activities based on general rules.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

This matter is not regulated in Belarus as of January 2025. According to Belarus law, only an individual can be the author of a particular work (e.g. a computer program) – please see question 6.2. Moreover, algorithms should not be protected as copyright because copyright does not extend to methods, processes or systems, even if they are expressed, displayed, explained or embodied in a work (e.g. a computer program).

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Confidentiality of personal data, permissions to use relevant data, the scope of rights to be licensed and regulatory restrictions may be key commercial considerations that apply to licensing data for use in ML.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

This matter is not regulated in Belarus as of January 2025.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

This matter is not regulated in Belarus as of January 2025, and we are not aware of initiatives aimed at development of respective regulations.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

Belarusian law does not directly regulate this matter, but the Law on PDP contains general provisions regarding the lawful use of personal data and establishes liability for breaching operator's obligations of the lawful use.

Processing of personal data without the data subject's consent may be conducted only in the course of particular cases, for instance, "for scientific or other research purposes, provided that the personal data is anonymised".

There are no disgorgement laws and/or initiatives in Belarus as of January 2025. However, in the absence of legal grounds for processing personal data, an operator is obliged to cease the processing of personal data and ensure its deletion or blocking. Additionally, if an operator is found to have violated personal data legislation, it may face administrative or criminal liability.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Belarus legislation does not contain specific rules and theories on liability for violations in the field of digital health; therefore, general principles on civil, administrative and criminal liability apply.

In particular, liability for breach of medical secrecy may include:

- disciplinary liability (reprimand, admonition and dismissal, in accordance with labour legislation);
- administrative fine, if disclosure does not contain elements of crime;
- civil liability (e.g. compensation of damages and/or moral harm); or
- criminal liability.

In relation to the illegal processing of personal data, non-compliance with requirements on data protection measures may lead to administrative fines. Some violations in the sphere of the protection of personal data may cause criminal liability; in particular:

- the unlawful collection or distribution of information relating to the private life, personal or family secrecy of another person without his/her consent; or
- the failure to comply with measures to ensure the protection of personal data by a person who processes personal data, which has inadvertently resulted in their dissemination and caused serious consequences.

9.2 What cross-border considerations are there?

There are some legal provisions that are subject to extraterritoriality in certain cases (e.g. personal data or antitrust regulation). In practice, however, the question of enforcement in such cases is open.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

The best practice to minimise liability risks in this regard is to ensure high-quality depersonalisation of data and comply with the purpose of data use, as well as with other personal data protection regulations. It should be taken into account that in the healthcare sector there can be a huge volume of sensitive data, so not only data privacy regulations, but also the medical secrecy regime may apply.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Please see our response to question 9.1 for details.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Information security and data protection are the key issues in Cloud-based services for digital health. Please see our responses to sections 4 and 5.

Local parties involved in data processing may be affected by certain localisation requirements. According to the Edict of the President of the Republic of Belarus No. 60 dated 1 February 2010, an activity involving selling goods, performing works or rendering services in the territory of Belarus through information networks, systems and resources, having connection to the Internet, is carried out by legal entities, their branches and representative offices, incorporated under the Belarus law with the seat in Belarus, as well as individual entrepreneurs, registered in Belarus, by using information networks, systems and resources located in Belarus and duly registered. In our opinion, this provision should be interpreted narrowly, and consequently applies only to Belarusian residents (e.g. when using Cloud-based solutions, located outside Belarus, to render services in Belarus) and shall not affect foreign Cloud-based providers directly.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Comprehensive regulatory due diligence, including data protection and investment issues, should be considered.

Moreover, due to significant state-involvement in healthcare, it is important to consider local licensing and regulatory peculiarities. For example, clinical trials are conducted in state healthcare organisations defined and authorised by the Ministry of Healthcare. An agreement on conducting clinical trials is concluded between the sponsor and healthcare organisation; direct agreement with the investigator is not allowed.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

From a legal perspective, regulatory due diligence is recommended. As well as analysing the state of the field of venture capital and/or direct financing, investors should identify negative trends on the Belarus market that affect its development.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Based on the Concept, one of the main problems is the lack of necessary standards for the exchange of medical information in the healthcare system in accordance with the requirements of the legislation. Additionally, there is a lack of formed databases and data banks, as well as a lack of technical equipment. The state authorities intend to develop these areas nowadays.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

There are no clinician certification bodies in Belarus; and we are not aware of any other bodies that have a power to influence the clinical adoption of digital health solutions. The relevant decisions are made in cooperation, mainly, between the Belarus government and the Ministry of Healthcare.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

There are no special regulations related to utilising digital health solutions and corresponding reimbursement. Instead, general reimbursement principles related to causing harm to patients' health should apply.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

The regulatory frameworks for AI/ML-based healthcare solutions are still evolving, and the lack of clarity can create gaps in understanding compliance requirements. For now, general principles and provisions from general civil, intellectual property and data privacy law shall apply.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

Currently, Belarus is developing the central software platform of the CHIS with the intent to introduce the platform. The plan for this platform is to provide access for each patient to their personal account and access to their medical data. The patient will be able to make an appointment through a personal account, receive test results and conclusions issued after consultations by specialists. Another stream worthy to note is development and adoption of the Project Code, which is intended to unify and update multiple regulations applicable to the healthcare sector.

Marina Golovnitskaya is a Partner heading the firm's CR practice and Life Sciences Sector group. She participated in and led most complex commercial and regulatory projects, also having experience in corporate and M&A. She has been recognised by international directories such as *The Legal 500* and holds a certificate of patent attorney.
With nearly 15 years of experience collaborating with legal counsels and decision-makers of transnational pharmaceutical companies with regard to Belarus, Marina possesses a deep understanding of the Big Pharma companies' local business processes, enabling her to provide tailored, business-oriented legal advice.

Alba LLP
Internatsionalnaya Str. 36-1
220030, Minsk
Belarus

Tel: +375 29 188 4328
Email: marina.golovnitskaya@alba-llp.by
LinkedIn: www.linkedin.com/in/marina-golovnitskaya

Yauheni Budchanka possesses a profound depth of knowledge in commercial and regulatory affairs, especially in the domains of intellectual property and the pharmaceutical industry. His professional background encompasses many significant cases concerning interactions with healthcare professionals and regulation of clinical trials, pharmacovigilance and marketing authorisation processes. Yauheni holds Legal Service Provider Certification No. 347.
Yauheni has been engaged in numerous IP projects including those related to trademarks (both national and international registrations), copyright (characters, software, photos, cinema, etc.), licensing, assignment, franchise agreements and customs registration.

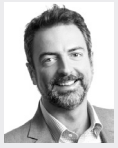
Alba LLP
Internatsionalnaya Str. 36-1
220030, Minsk
Belarus

Tel: +375 29 702 0757
Email: yauheni.budchanka@alba-llp.by
LinkedIn: www.linkedin.com/in/yauheni-budchanka

Alba LLP is a full-service Belarusian law firm with an international background. Our mission is to help clients succeed by providing legal services. Not only are we trained to the highest standards of counselling, but we are passionate about what we do.
Alba provides full legal and tax support for the needs of the Life Sciences & Healthcare sector, starting from regulatory, corporate, employment, litigation and IP legal issues to M&A transactions and projects. We provide an international level of services that global-level players expect and apply a risk management system to match rigorous standards. Our team is formed by lawyers with ample work experience at leading Belarusian and international law firms, and advises clients and investors from life sciences and healthcare fields, including pharmaceuticals, medicinal products, diagnostics and medical services, chemicals, cosmetics and biotechnology (R&D laboratories, start-ups, scientific communities, etc.).

www.alba-llp.by

Belgium


Olivier Van Obberghen


Pieter Wyckmans


Amber Cockx


Chaline Sempels

Quinz

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

While more than one definition exists, digital health or e-health is generally described as "the use of information and communication technologies within healthcare to optimise patient care".

1.2 What are the key emerging digital health subsectors in your jurisdiction?

In recent years, Belgium has seen a rise in the development and implementation of a number of digital health technologies such as apps, wearables, platform technology and AI-based software across the life sciences value chain and into the patient journey with a focus on remote, personalised, precision and preventative care. While patient-facing health and wellness apps have been around for a while now, we observe a growing number of provider-focused digital health tools, including digital diagnostics and remote patient monitoring tools.

1.3 What is the digital health market size for your jurisdiction?

There are currently no official statistics available that provide a clear overview of the size of the Belgian digital health market due to the broadness of the concept of digital health and the difficulty of delineating its boundaries. Some unofficial sources estimate that the digital health market in Belgium generated a turnover of 850 million euros, excluding exports, in 2024.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

In line with question 1.3, no definite statistics on Belgium's largest digital health companies exist. Belgium's digital health landscape is populated by multinational (tech) corporations headquartered abroad, biotech and pharmaceutical companies venturing into digital branches and a large number of MedTech companies and fast-growing start-ups, scale-ups and spin-offs. BeMedTech is the Belgian federation representing the medical technology industry, encompassing nearly 200 companies that account for 80% of the market in Belgium. Their website features a list of prominent digital health companies.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

See our response to question 1.4.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

First, the Belgian National Institute for Health and Disability Insurance (NIHDI) is responsible for establishing reimbursement schemes for healthcare services, health products and medicines. Further, the Federal Agency for Medicines and Health Products (FAMHP), in cooperation with the European Medicines Agency, supervises the quality, safety and efficacy of medicines and health products and enforces the legislation applicable thereto. The Institute for Public Health (Sciensano) monitors public health and diseases and evaluates the effectiveness and safety of vaccines, medicines and health products and was therefore of paramount importance during the COVID-19 pandemic. Additionally, professional associations such as the Order of Physicians and the Order of Pharmacists regulate the deontological aspects of healthcare professions, while the self-regulatory organisations Pharma.be and BeMedTech provide industry guidance. The Belgian Data Protection Authority (DPA) enforces compliance with data protection legislation and the recently established Health Data Authority oversees the sharing and use of healthcare data. For the federal government, the FPS BOSA has been appointed as the "single information point" for the purpose of the implementation of the EU Data Governance Act.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

- Act on the Performance of the Healthcare Professions of 10 May 2015.
- Act on Hospitals and Other Care Facilities of 10 July 2008.
- Health Care Quality of Practice Act of 22 April 2019.
- Patients' Rights Act of 22 August 2002.
- Law on Medicines of 25 March 1964.

- EU Regulation 2017/745 on Medical Devices (MDR); Medical Devices Act of 22 December 2020; EU Regulation 2017/746 on *In Vitro* Diagnostic Medical Devices (IVDMDR) of 5 April 2017; and *In Vitro* Diagnostic Medical Devices Act of 15 June 2022.
- Law on Experiments with Humans of 7 May 2004; EU Regulation 536/2014 on clinical trials on medicinal products for human use of 16 April 2014.

Additionally, there are a number of legislative initiatives and already adopted instruments in light of the EU's digital and data strategy, such as the Digital Services Act (EU Regulation 2022/2065) and the Artificial Intelligence Act (EU Regulation 2024/1689) (AIA), and the EU's general data strategy, such as the Data Governance Act (EU Regulation 2022/868), the Data Act (EU Regulation 2023/2854) and the Regulation establishing the European Health Data Space, will significantly impact the offering of digital health goods and services on the EU market in the future.

Furthermore, the legislation on product safety, personal data protection and e-commerce apply to digital health and healthcare IT. In addition, general regulations on competition, consumer law and unfair commercial practices must be kept in mind. Certain specific rules might also be relevant (e.g. the Act of 21 August 2008 establishing and organising the eHealth platform or the EU framework on cross-border healthcare).

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The DPA and the Market Court in Brussels are responsible for investigating and enforcing penalties for data protection infringements. In addition, the FAMHP can take administrative sanctions and restrict the placing of medicines and health products on the market. The EU Commission and the Belgian Competition Authority implement the competition policy on the Belgian market, while the public prosecutor's office investigates, prosecutes and brings to judgment offences that are criminally curbed. The AIA is expected to become an emerging area of enforcement, with potential fines reaching up to 35 million euros or 7% of the consolidated annual turnover.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

If software is considered a medical device (for more information on this classification, see question 3.1) or an accessory to a medical device, the Medical Devices Act of 22 December 2020, the MDR and/or the IVDMDR will apply, depending on the type of medical device. The Belgian national regulatory framework was brought in line with the MDR and IVDMDR by the Acts of 22 December 2020 and 15 June 2022 and a Royal Decree of 13 September 2022. Prior to being placed on the market, medical devices must undergo a clinical evaluation and conformity assessment to review the safety and performance of the device. Demonstrating conformity is in the first instance the responsibility of the device manufacturer. For most medical devices (except for class I medical devices), the conformity then needs to be confirmed by a "notified body" designated by the Belgian (or another EU Member State's) government. In addition, medical devices need to be traceable throughout the supply chain up until the end-user. Finally, the FAHMP is responsible for post-market surveillance of (software as a) medical device(s).

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Software that is powered by AI/Machine Learning (ML) is first of all governed by the same regime as other software (see question 2.4).

If AI/ML-powered digital health devices or software solutions fall within the scope of the MDR or the IVMDR, they must thus be CE-marked (after having completed a successful conformity assessment) before being placed on the market. In addition, they will soon need to comply with the AIA, which entered into force on 1 August 2024.

The AIA recognises that if AI/ML-powered digital health devices or software solutions constitute medical devices, they may be identified as high-risk, and both the requirements of the MDR/IVMDR and the AIA will have to be complied with.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Please see question 10.7 regarding the dynamic nature of AI/ML-based digital health solutions. Every authority is striving to evolve alongside rapidly developing technologies, which does not always proceed smoothly. On 3 September 2024, the Belgian House of Representatives published a draft resolution directing critical requests at the federal government, such as making high-quality digital health a priority (with particular attention to vulnerable groups), and calling on the Belgian Healthcare Knowledge Centre (KCE) to conduct research on the implementation of digital health solutions. This resolution suggests the implementation of a system, inspired by Germany's "Fast-Track-*Verfahren*", to speed up the approval and reimbursement of digital health applications that have yet to demonstrate their socio-economic value. This system should include a comprehensive guide detailing the procedure, application process and evidence requirements, and should promote collaboration with mHealthBelgium, FAMHP, NIHDI and the eHealth platform. It also advocates for the establishment of a legal framework for the use of health applications, ensuring that the processing of personal data required for the purpose thereof complies with General Data Protection Regulation (GDPR) standards. However, the resolution does not clarify how Belgium plans to tackle the impact of AI and the extensive new AI regulatory framework. It also overlooks the challenges faced by (med)tech and pharmaceutical businesses when launching digital therapeutics (DTx) or other health software technologies, such as bottlenecks with notified bodies and stricter CE-marking requirements.

The shortcomings of the current system are particularly evident in the lack of actual reimbursement for digital health solutions, preventing their adoption in clinical practice. Some small steps in the right direction can be noted. The mHealthBelgium validation pyramid, as mentioned in question 3.1, received a slight revamp and will provide more information and transparency about the reimbursement decisions of the NIHDI with regard to digital health applications included in the pyramid, as well as about the use and funding of similar applications in surrounding countries. Although no specific public funds were allocated for mHealthBelgium in 2024, it was recently announced that the Belgian industry association for medical devices, "beMedTech", will continue

updating the platform. The NIHDI also launched a new procedure for evaluating mobile medical applications last year, which should allow mobile medical applications to move more quickly into real-world care pathways. Digital health is one of the priorities in the Flemish Government's coalition agreement 2024–2029 (see question 2.8).

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

As noted above, the MDR and IVDMDR require clinical evidence (i.e. demonstrating safety, efficacy and clinical benefit) for medical devices before such devices can be placed on the market. If classified as a medical device (see question 3.1), an AI/ML-based digital health solution will generally fall into a higher risk class, requiring a more stringent clinical assessment.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Belgium has a complex healthcare landscape with fragmented political competences and sometimes divergent approaches. The Belgian federal government is responsible for laying out Belgium's general healthcare policy, supervises the (placing on the market of) medicines and healthcare products, and oversees the regulation and financing of compulsory health insurance, as well as the funding of hospital services. On the other hand, the Communities (the Flemish Community, the French Community and the German-speaking Community) are responsible for health promotion and prevention, and for the recognition and quality assurance of healthcare providers (HCPs) and healthcare institutions. In other words, the approval and post-market surveillance of digital health products and solutions are primarily a federal responsibility, whereas the use of such solutions in clinical practice is overseen by the Communities. The creation of a Belgian Integrated Health Record (BIHR) should improve cooperation between the various government bodies involved (see below).

A dedicated chapter of the Flemish Government's coalition agreement 2024–2029 focuses on the digitisation of healthcare, highlighting the importance of empowering patients to manage their health without needing to visit doctors or hospitals. The Flemish Government intends to promote the use of digital health applications and technologies to alleviate the burden on HCPs and enhance the quality of care. This promotion of digital health applications seems to be supported by the federal parliament as well, as shown by its recent resolution regarding the accessibility of digital health applications (see question 2.6).

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

As stated above (see question 2.3), the main areas of enforcement in digital health concern data protection infringements, violations of rules governing the marketing and sale of medical devices, and competition considerations. While enforcement actions are not being specifically tailored to digital health products and solutions, there are indications that enforcement authorities will focus their efforts on the digital health market in the coming years.

A notable example of an enforcement action in the digital health space is a 200,000 euros fine imposed on 17 December 2024 by the Belgian DPA on a hospital for GDPR violations following a 2021 cyberattack. The DPA's investigation revealed several failings in the hospital's data protection practices, including the absence of a Data Protection Impact Assessment, inadequate staff training, weak password policies and overall insufficient security measures at the time of the breach. While not specific to digital health products, this case demonstrates that Belgian authorities are willing to take action against healthcare entities for data protection failures.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Belgium does not have an all-encompassing framework on telemedicine yet and there has been long-term opposition against consultations at a distance where a diagnosis of the patient is made, especially by the National Council of the Order of Physicians (NCOP). Concerns mainly related to the quality and credibility of online HCPs, and the privacy and security of patient data. There has, however, been a switch in mindset. As from 2022, teleconsultations – complementary to face-to-face patient care – are acceptable under certain conditions. In particular, amongst other requirements: (i) the duration and circumstances of the teleconsultation must be sufficient to guarantee the quality of care; (ii) the physician needs to be able to verify whether there is consent of the patient and there is an adequate therapeutic relationship between the patient and the physician established; (iii) the continuity of care must be warranted (e.g. by completing the patient's electronic patient record); and (iv) any prescriptions must be made through the official system for electronic prescriptions, Recip-e. In addition to that, certain remote consultations by doctors are being reimbursed by the NIHDI. It should be noted that, in the last quarter of 2024, the federal (caretaker) government proposed to suspend the reimbursement of teleconsultations in order to relieve the federal budget for 2025. However, such a saving required a political agreement that could not be reached in time. The suspension of the reimbursement of teleconsultations is therefore expected to be delayed until 2026. In the meantime, as of January 2025, the NIHDI reimburses hospitals that have entered into a new agreement for the telemonitoring of patients recently hospitalised due to heart failure.
- **Robotics**
  Although the traditional rules regarding (contractual, extracontractual, medical and product) liability apply (see question 9.1 below), it may be difficult for a patient suffering damage due to robot-assisted surgery to assess the most suitable remedy for their claim and the current EU and national liability framework may prove to be inadequate.
- **Wearables**
  Wearables are subject to considerably different regulatory frameworks based on their classification as a medical device or not. The decisive criteria to determine whether a wearable constitutes a medical device, is to establish whether the instrument, appliance or software

is intended to be used for one of the medical purposes in art. 2(1) of the MDR (e.g. for the diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of a disease or disability). The medical devices framework is relatively burdensome, giving manufacturers an incentive to indicate that their health product is not intended to be used for one of these medical purposes in order to avoid having to comply with the MDR. On the other hand, reimbursement for wearables is currently limited to CE-certified medical devices (see further under "Mobile Apps").

- **Virtual Assistants (e.g. Alexa)**
  Virtual (voice) assistants (VVAs) have ample applications in healthcare settings. They can aid in clinical notetaking, in assisting an aging population or patients suffering from mobility issues, in medication management and in health information-seeking activities. However, data protection and privacy concerns have been raised by (amongst others) the European Data Protection Board (EDPB) in its Guidelines 02/2021 on VVAs. Careful consideration must be given to the legal basis of the processing of personal data by virtual assistants under art. 6 of the GDPR and the requirements of art. 5(3) of the Directive 2002/58/EC on privacy and electronic communications (as transposed into Belgian law by the Electronic Communications Act of 13 June 2005 and as currently being revised on the EU level). Since VVAs require processing of biometric data for user identification, an exemption under art. 9 of the GDPR must also be sought. Other data protection challenges have also been raised, for example regarding the data minimisation principle and the accidental collection of personal data or the collection of background noise or other individuals' voices besides the user. The European Commission has also voiced antitrust concerns about virtual assistants in light of its consumer Internet of Things (IoT) inquiry. These concerns included the high entry and expansion barriers of the technology, certain exclusivity and tying issues, the lack of interoperability, the large amounts of data feeding into the technology and VVAs functioning as intermediaries between the user and smart devices or IoT services. The Digital Markets Act might also have a significant impact on the marketing and use of VVAs as companies offering core platform services, which includes, amongst others, virtual assistant services, could be considered a "gatekeeper" if they meet other requirements indicating that such companies have a position of power in the market.
- **Mobile Apps**
  Since January 2021, mobile apps that meet all the criteria of the mHealth Belgium validation pyramid can be reimbursed. In the first instance, they need to be CE-certified as a medical device and meet the requirements of the GDPR. Secondly, they need to pass certain interoperability and connectivity criteria. Lastly, a socio-economic benefit must be demonstrated in order to receive reimbursement by the NIHDI. Up until now, the success of the validation pyramid has been limited, as proving the socio-economic importance of apps remains difficult. For this reason, the NIHDI has established a new procedure for submitting reimbursement dossiers for health apps, which should allow more stakeholders to submit a reimbursement application and improve the process of assessing such apps. Dossiers are expected to be evaluated by a multidisciplinary working group within the NIHDI, with a maximum evaluation period of 270 days. (Note that mobile apps can also be financed by other payers such as hospitals, healthcare professionals or health insurance companies). Nonetheless, some other issues concerning mobile apps remain. For example, if mobile health apps are used in healthcare and prescribed by a healthcare professional, patients that do not have access to the Internet may be discriminated and the patients' rights under the Patients' Rights Act need to be respected, such as the right to quality healthcare. With regard to the GDPR, the Belgian DPA has issued guidelines specifically tailored for mobile health apps. Again, mobile apps may be classified as a medical device if intended to be used for medical purposes and may consequently have to comply with the medical devices' framework, while other apps may be considered a wellness or lifestyle device. The latter category of devices is not (yet) subject to specific legislation, but the collection and processing of any personal data through such apps must of course be in compliance with the GDPR.
- **Software as a Medical Device**
  The classification of Software as a Medical Device (SaMD) suffers from the same shortcomings as the ones for wearables and mobile apps. Software will be considered a medical device if: (i) it is intended by its manufacturer to have a medical purpose or if the software meets the definition of an "accessory" for a medical device; (ii) it performs an action on data that goes beyond storage, archival, communication or simple search; and (iii) it is for the benefit of individual patients. As said, classification as a medical device has consequences for the regulatory framework that applies to software.
- **Clinical Decision Support Software**
  Besides the undeniable ethical challenges, clinical decision support software (CDSS) raises a number of legal issues. It is, for example, uncertain which party will be responsible in the event of a medical accident as a result of a decision made on the basis of CDSS. In addition, there are data protection and medical confidentiality concerns, for instance if the patient data that is submitted to the CDSS is used, not only to render a medical decision concerning the relevant patient, but also to improve the CDSS or for other business purposes of the CDSS manufacturer. As further set out below, due to the requirements of the GDPR in relation to automatic decision-making, human intervention by a healthcare professional before making a final medical decision is in any case advised.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  A key barrier in the widespread implementation of AI/ML-powered solutions in healthcare concerns the massive amounts of special-category personal data that are often needed for the optimal functioning of these devices and the accompanying data protection aspects, for example in relation to automated decision-making by AI/ML-powered solutions. The exercise by the data subject of certain rights, such as the right to access and erase personal data might (technically) also be notably difficult. Besides data protection, the interplay of the AIA and the MDR results in stringent requirements for AI-powered medical devices. Any AI-powered medical device that must undergo a conformity assessment procedure by a notified body is considered as a high-risk AI system within the meaning of the AIA (art. 6 and

Annex II of the AIA), subject to strict monitoring obligations. Since most SaMD will be classified as Class IIA or higher and must therefore undergo a conformity assessment, the majority of AI/ML-powered medical devices will be deemed to be high risk under the AIA.

- **IoT (Internet of Things) and Connected Devices**
  Again, while IoT and connected devices offer great advantages for patients (e.g. assisted living), for physicians (e.g. telemonitoring) and for hospitals (e.g. stock management and patient identification), privacy, data protection and security issues have been raised.
- **3D Printing/Bioprinting**
  Legal considerations on bioprinting include IP questions (copyright, patentability and design rights of techniques and materials), the classification of the bioprinted product (as medical device or (advanced therapy) medicinal product) and the liability of the variety of actors involved.
- **Digital Therapeutics**
  DTx have great potential in shifting healthcare to be more personalised, preventative and patient-centred. The downside, however, includes major concerns relating to cybersecurity, data protection and privacy. By using digital implements such as mobile devices, sensors and IoT, DTx transfers enormous amounts of personal information over the Internet and hence, risks of unauthorised access and manipulation of these products and underlying data (e.g. further use of real-world evidence) could compromise both trust in the product and patient care. Since some of the key therapeutic areas of DTx include cognitive behavioural therapy and lifestyle management (e.g. for patients with chronic conditions), it may be especially difficult to distinguish whether a DTx solution is a medical device or not. Unless it concerns a mobile app or a medical device, the financing for DTx is also uncertain.
- **Digital Diagnostics**
  Digital diagnostics are tools used in the diagnosis of medical conditions or for measurement of health parameters (e.g. digital biomarkers). Such tools will often qualify as a medical device or an *in vitro* diagnostic medical device, depending on the intended use and functionalities of the product. The classification of a medical device and *in vitro* diagnostic medical device determines the regulatory requirements associated with the product and the conformity assessment that the product must undergo prior to being placed on the market.
- **Electronic Medical Record Management Solutions**
  Storing patient information in an electronic medical record is mandatory under art. 34 of the Belgian Healthcare Quality of Practice Act. The patient's right to privacy and to a carefully kept patient record (arts 9 and 10 of the Act of 22 August 2002 on Patients' Rights and arts 33–40 of the Health Care Quality of Practice Act of 22 September 2019) needs to be taken into account when processing, storing and accessing patient health information via electronic medical records. The Belgian National Commission of Representatives of Physicians and Health insurance funds has also issued a list of acceptable electronic medical record software providers to avoid interconnectivity or security issues (see also question 4.3 below). Furthermore, the Regulation establishing the European Health Data Space includes technical requirements for electronic health record systems to ensure the security of such systems and their interoperability across the EU, facilitating the exchange of health data between systems from different manufacturers.
- **Big Data Analytics**
  ML and AI systems are trained on large amounts of data, which are examined to identify trends, patterns and correlations. The insights resulting from such advanced analytical process allow the system (or its user) to make data-informed decisions in the future. As already explained above (see Artificial Intelligence/Machine Learning-Powered Digital Health Solutions), ensuring compliance with data protection legislation can be challenging. When data collected in a specific (medical) context are being used to develop and/or improve a system or for other business objectives, the legal basis providing the justification for the initial data collection and processing might not cover such secondary use. The interplay between GDPR and the AIA brings about additional complexities, especially as the latter seems to allow certain processing activities with respect to personal data without adequately addressing GDPR considerations.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Blockchain technology enables secure decentralised data sharing, while providing the possibility to monitor, trace and revoke data exchanges. This enhances security, data privacy and efficiency in the storage and management of the large amounts of data involved in IoT devices. In February of 2023, the European Commission introduced the "European Blockchain Regulatory Sandbox for innovative use cases involving Distributed Ledger Technologies", establishing a pan-European framework for cross-border dialogue between regulators and supervisors on the one hand, and (private or public) developers of blockchain use cases on the other hand. Such regulatory dialogue has proved necessary to increase legal certainty for innovative blockchain technology solutions.
- **Natural Language Processing**
  This technology is similarly impacted by data protection concerns as virtual assistants are (see above). Healthcare professionals wishing to use this technology in the management of electronic health records may also encounter interoperability issues. Additionally, natural language processing technology raises issues concerning discrimination on language grounds and a range of other ethical and legal issues such as transparency, fairness, accountability, etc. As natural language processing technology is AI driven, the AIA will also need to be considered.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

The EU Digital Services Act imposes extensive transparency obligations on intermediary service providers (including providers of digital platform services) and requires them to designate a single point of contact for communications with authorities and users. In addition, to avoid liability, if the provider gains knowledge of an infringement committed through its services, it needs to act expeditiously to remove or to disable access to the illegal activity or illegal content concerned and it needs to inform the public prosecutor of such infringement. Even more obligations are imposed on online platforms (a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public) and very large online platforms (platforms with over 45 million active users monthly), which have to put in place measures to actively counter the spreading of illegal goods, services or

content online, such as mechanisms to identify sellers of goods and buttons for users to flag illegal content.

Digital platforms offering remote consultations with doctors need to take into account the quality standards set by the Health Care Quality of Practice Act, as well as the conditions listed in question 3.1 under "Telemedicine". For example, consultations organised through a digital platform will rarely be eligible for reimbursement, as one of the conditions for reimbursement holds that the doctor and patient have an existing treatment relationship (i.e. the doctor is the patient's primary care physician, the patient physically visited the doctor at least once in the past calendar year or the patient was referred to the doctor-specialist by another doctor).

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

As in most jurisdictions, the use and processing of personal data in healthcare in Belgium has drastically changed over the last decades. In the past, a patient's medical records were usually stored by their treating physician in a paper version and were solely used for the purposes of treatment. With the introduction of e-health, other actors have entered the process, resulting in greater risks of privacy and/or data protection breaches. Under the GDPR and the Belgian Law on the Protection of Natural Persons with regard to the Processing of Personal Data, data related to health are considered as "sensitive personal data" or a "special category of personal data". In principle, such data cannot be processed unless a valid legal basis can be found and an exception applies, e.g. informed consent, medical diagnosis by someone under the obligation of professional secrecy, reasons of public interest in the area of public health, etc. (arts 6 and 9 of the GDPR). The right to privacy (art. 8 of the European Convention of Human Rights, art. 7 of the Charter of the EU and art. 22 of the Constitution) and the right to data protection (art. 8 of the Charter of the EU, art. 16 of the Treaty on the Functioning of the EU and art. 10 of the Act on Patients' Rights) of a patient need to be reconciled with the advantages of the processing and sharing of certain medical data. On an individual basis, electronic health records and the automatic processing of personal data may facilitate long-term follow-up by several different HCPs. On a larger scale, (big) data analyses of personal data may increase the quality and efficiency of healthcare, offer predictive therapeutic models and allow for the personalised care of patients. In January 2024, the Data Act came into effect, aiming to set clearer rules for individuals and businesses on the use of both personal and non-personal data generated by connected objects, also known as the "Internet of Things" and applying, amongst others, to medical and health devices. However, to give stakeholders time to make the necessary technical arrangements, the Act will only be applicable starting from September 2025.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

The implementation and enforcement of the GDPR is governed on a national level in Belgium with a national DPA and the Belgian Law on the Protection of Natural Persons with regard to the Processing of Personal Data.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

As a consequence of the introduction of e-health, the personal data of patients are no longer solely processed by physicians and other HCPs, who are bound by professional secrecy under the penalty of criminal sanctions in accordance with art. 458 of the Criminal Code (art. 25 of the Code of Medical Ethics of the NCOP). Employees of the medical devices industry or health app providers may be in direct contact with patients and process their personal data. Under the GDPR, one may only process personal health-related data when one of the grounds of art. 9.2 applies. Personal data may be processed for purposes of preventive or occupational medicine, medical diagnosis or the provision of health or social care treatment, but this may only be done under the responsibility of a professional subject to the obligation of professional secrecy (arts 9.2(h) and 9.3 of the GDPR). Accordingly, health app providers cannot benefit from this provision and will have to rely on any of the other exceptions in art. 9 (e.g. freely given, specific and informed consent (art. 9.2(a)), where processing is necessary for reasons of public interest in the area of public health (art. 9.2(i)) or where processing is necessary for scientific research purposes (art. 9.2(j)).

4.4 How do the regulations define the scope of personal health data use?

The GDPR and the Belgian Law on the Protection of Natural Persons with regard to the Processing of Personal Data adopt a definition of "processing", which includes nearly any action or operation related to personal data: "'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." (Art. 4.2 of the GDPR and arts 5 and 26.2 of the Law on the Protection of Natural Persons with regard to the Processing of Personal Data.) Personal information related to health, as well as genetic and biometric data used for identification purposes, is classified as sensitive personal data or special category data under arts 9 of the GDPR and 10 of the Law on the Protection of Natural Persons with regard to the Processing of Personal Data. The processing of such data is generally prohibited unless a valid justification is provided. Consequently, health-related personal data can only be processed in exceptional circumstances.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

When more than one party is involved in the processing of (health-related) personal information, both territorial aspects and the relationship between the parties need to be

considered. On the one hand, compliance with the GDPR and national implementing laws is required when the controller or processor of personal data is established in the EU, as well as when the processing of personal data concerns data subjects who are located in the EU (if related to the offering of goods and services or the monitoring of behaviour of data subjects within the EU). If personal data that is subject to the GDPR is transferred to a controller or processor outside the EEA (not normally subject to the GDPR), a transfer mechanism (such as the (updated) standard contractual clauses) needs to be implemented and a transfer impact assessment may be necessary. On the other hand, it is essential to allocate the rights and responsibilities of each actor involved in the processing. Whenever a processor processes data on behalf of a controller, a data processing agreement must be concluded (art. 28.3 of the GDPR). This is the case if a physician makes use of a medical device for the diagnosis of their patients and personal data will be processed by the medical device provider for such healthcare purposes. If such provider also processes personal data for its own purposes and means (e.g. to improve its products and services), such provider may – in addition – be considered a controller, for which the GDPR does not require a specific agreement. Further, if the physician and medical device provider jointly determine the purposes and means of the processing and thus relate to each other as joint controllers, the parties must conclude a transparency agreement (art. 26 of the GDPR). Furthermore, in B2B relations, the Data Act bans unfair contractual terms related to data access or usage. It also provides a list of clauses that are always deemed unfair and another list of clauses that are presumed to be unfair.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The principle of data accuracy and the right to rectification (art. 5(1)(d) of the GDPR) of incorrect personal data (art. 16 of the GDPR) about oneself are closely connected. The Knowledge Centre for Data and Society considers that the more important the data is for training an AI system, the greater the effort must be to verify that it is correct or needs to be adjusted. The datasets used to train or "feed" AI systems must be sufficiently reviewed to ensure they do not incorporate bias or prejudice that may reinforce discrimination and socio-economic injustice. As discussed under question 7.4, issues arise also in relation to the data subject's right not to be subject to a decision made solely by automated means, especially if the decision has a considerable impact on the data subject. As a consequence, decision-making by AI must be transparent and verifiable (there must be an "explainability" of decisions made by AI systems, AI systems must be auditable or at least suitable for *post-hoc* interpretability). If this review does not happen on a regular basis, the use of an AI system could lead, for example, to discrimination based on historical data patterns contrary to the Gender Act, the Anti-Racism Act and the Anti-Discrimination Act.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The GDPR maintains high data protection standards, including a purpose limitation principle, meaning that personal data that is collected for a certain purpose cannot be used for a new and incompatible purpose (art. 5.1(b) of the GDPR). It is thus important to establish all purposes for which the personal data will be used at the time of collection. This is particularly relevant in the context of clinical trials. All too often, personal data collected in the course of a clinical trial (first use) may become of interest for the use in other research, independent of this clinical trial (further use). The purpose limitation principle prohibits further processing of personal data incompatible with the initial purpose; however, further processing in accordance with art. 89(1) of the GDPR for scientific research purposes shall not be considered incompatible with the initial purpose. Nonetheless, if the legal basis for the further processing of personal data (secondary use) is consent under art. 6.1(a) of the GDPR, this may pose certain problems. Consent must be freely given, specific, informed and unambiguous. However, often at the beginning of the clinical trial (first use) when consent of the data subject is sought, it is not yet entirely clear for which further research purposes the personal data may also be used (further use). Fortunately, recital 33 of the GDPR allows for some flexibility in this regard and notes that data subjects should be permitted to give their consent for the further use of their personal data for scientific research on a more general level. Ensuring that data subjects give their consent at the time of collection for all purposes for which one intends to use the personal data is good practice and avoids the situation where one would have to go back to the data subject to ask for consent for additional purposes.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

In order to assure confidence of a patient in the healthcare industry and protect an individual's data and privacy, adequate safeguards must be provided to ensure personal data is not shared with third parties without a patient's knowledge and/or without their consent (if the legal basis for the processing of personal data is consent). In an information society, the obligation to professional secrecy no longer suffices to protect a patient's medical data. In this context, it is highly recommended to enter into a data sharing agreement addressing what data can be shared, who has the authority to access the data and which security measures are required, especially when there is a large number of parties involved in the processing of personal data. These considerations are also at the forefront in the recently adopted regulation creating a European Health Data Space, intended to facilitate the use and sharing of European health records to boost the availability of qualitative health data in the EU, both for the purpose of providing healthcare services and for "secondary purposes" such as research and policy-making.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

As mentioned above, the GDPR is implemented and enforced on a national level. The Belgian Health Data Agency is specifically tasked with the governance of health data sharing.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Data protection laws must ensure that the personal data collected by a physician, a medical device or a health app is, on the one hand, not shared with, for example, insurance companies but, on the other hand, can be consulted by a physician administering emergency care. The Data Act outlines the conditions under which public sector bodies and specific EU institutions, like the European Commission, can request data holders to provide access to data necessary for fulfilling their statutory duties in the public interest.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Since 2008, a national e-Health platform has been established, where HCPs upload electronic health records of a patient to allow all other HCPs having a therapeutic relationship with that same patient to access and review such records in a secure way. More recently, an amendment to art. 5.4(b) of the Law Establishing and Organising the eHealth Platform has been adopted by the legislator, removing the need for prior patient consent to upload such records to the platform and instead provide an opt-out option for patients. One of the common themes in the Belgian eHealth Action Plan 2022–2024 is the development of a BIHR, a more advanced model of data exchange via a central digital platform that should allow for closer collaboration between all actors in health to ensure a seamless continuum of care for the patient. One of the objectives is to make the "real-world data" from the BIHR available as "routinely collected data" and increase the documentation, findability, accessibility, quality and reusability of the data. In relation thereto, a Belgian Health Data Agency has been established to supervise secondary use of health data and, more generally, play a facilitating role in the exchange of health data for research purposes.

The EU Data Governance Act aims to facilitate the sharing of data which are in the possession of government agencies and are not to be made publicly available, for commercial and non-commercial reuse. Under the Data Governance Act, each government should establish an easily accessible central location where all relevant information is available and through which requests for data access or reuse can be submitted. For the Belgian federal government, the FPS Policy and Support (BOSA) is designated as the central information point. A new Royal Decree of December 2024 imposes restrictions on HCPs' access to patients' health records. It stipulates that HCPs conducting examinations without the intent to preserve, restore or improve a patient's health cannot access health data maintained by HCPs responsible for these objectives, unless a specific legal framework permits such data sharing.

Additionally, the Royal Decree introduces stricter requirements for obtaining informed consent when a patient's data is managed by another HCP. These provisions ensure that patients are fully informed and explicitly consent to the handling of their health data by different HCPs.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Federated learning avoids the exchange of raw data between the parties – instead, the models trained on each local dataset are shared and aggregated. While this form of collaborative model training offers clear benefits in terms of data minimisation and quality of training, data leakage and security concerns are still present. Other issues relate to data processing roles and responsibilities and secondary data use, as further discussed below (see question 7.3).

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Since there are no specific intellectual property (IP) regimes for digital health technologies, the scope of protection is defined by applicable traditional regimes. Inventions, in all fields of technology, are patentable if they are new (in other words, they are not part of the state of the art), if they are the result of the inventiveness or resourcefulness of the inventor, if they are capable of industrial application, and lawful (Title 1 of Book XI of the Code of Economic Law (CEL) and Part II of the European Patent Convention). Software and mathematical methods are specifically exempt from patent protection; however, only to the extent that a patent application relates solely to software or mathematical method as such. One can apply for patent protection for "mixed inventions", for instance, for a new product of a technical nature that incorporates a software program. Similarly, methods for diagnosis are not patentable under European law, but medical devices used to carry out the diagnostic method are.

The European Patent Office (EPO) classifies AI- and ML-related applications as mathematical methods in its guidance. From 2023, inventions in the EU can be protected by a European patent with unitary effect (the "unitary patent"). This patent offers protection in the EU Member States that have ratified the Agreement on a Unified Patent Court and is administered centrally by the EPO. It is supplemented by the Unified Patent Court.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Copyright protects literary or artistic works in a broad sense (Title 5 of Book XI of the CEL). A work is eligible for copyright protection provided that it represents the author's own intellectual creation (the "originality" requirement). The author of a work that fulfils these conditions is granted copyright protection without any formality, up until 70 years after their death. Copyright includes both transferable property rights and inalienable moral rights. However, the originality requirement seems to be problematic in relation to digital health technologies. While the expression of software (i.e. the code and preparatory design work) and the structure of a database (i.e. the selection and arrangement of the data) can be protected by copyright, the ideas and principles underlying the technology (such as algorithms and functionalities) are not copyrightable, nor is the content of a database. The latter could be protected by the *sui generis* database right, provided that the acquisition, verification and presentation thereof constitute a substantial investment by the author (art. XI.306 of the CEL). Interestingly, there seems to be a legislative trend to limit the scope of copyright protection in order to facilitate the development of digital technologies and the sharing of data. The

EU Directive 2019/790 on Copyright and Related Rights in the Digital Single Market (the Copyright Directive), which has been transposed into Belgian law by the Act of 19 June 2022, has introduced exceptions to copyright for text and data mining (i.e. the automated analysis of large bodies of data in order to generate knowledge on patterns, trends and correlations). This will allow developers of AI systems to extract data from a database without having to obtain the prior authorisation of its owner. Art. 43 of the Data Act provides that the *sui generis* database right does not apply to databases containing data obtained from or generated by a connected (IoT) product or related service.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Information is considered a trade secret if the information is secret, not publicly known or easily accessible, if the information has commercial value due to its confidentiality, and if the information was made subject to reasonable measures to protect its confidentiality (Title 8/1 of Book XI of the CEL). As such, trade secrets can protect raw or processed data and databases, methods, algorithms, codes, processes, parameters, etc. Trade secrets are not protected by an IP right and do not require registration, but the wrongful acquisition of such information is prohibited and may be enforced in court by means of a claim for injunctive relief and damages. It should be noted that independent discovery or creation of the same information remains lawful.

Digital health technology companies may rely on trade secrets for the protection of the data used to train their AI models, provided they can prove the commercial value thereof. This will be easier when it comes to a combined dataset rather than with respect to any part of the data in isolation. However, as part of the data sharing obligations introduced by the new Data Act, the trade secret holder may be required to disclose its trade secrets to the user of a connected device or even a third party (subject to the user of a connected device or third party taking adequate technical and organisational measures to preserve the confidentiality of the trade secret).

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Higher education is a competition of the Communities in Belgium. For the Flemish Community, the Codex Higher Education stipulates that any property rights to inventions made by salaried staff as part of their research duties shall belong exclusively to the university or the university college. The Codex further lays down rules for the participation of universities or university colleges in spin-off companies and for scientific services performed by universities and university colleges. Most academic technology or knowledge transfers are handled by the tech transfer offices of the universities or university colleges and take the form of license or other types of collaboration agreements or participation in spin offs.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

As said above, software may be protected by a patent if incorporated in technology, such as a medical device. In addition, the expression of software enjoys copyright protection if it is original in the sense that it is the author's own intellectual creation (Title 6 of Book XI of the CEL). In this respect, copyright can also protect the appearance (i.e. graphics and multimedia elements) of a digital health application.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

The EPO has confirmed on multiple occasions that AI (devices) cannot be named as inventors on patent applications, as the European Patent Convention stipulates that the inventor must be a person with legal capacity.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

The core rules and laws applicable to government-funded inventions in Belgium are noted down in the CEL, Book XI, Title 1, Chapter 2. Irrespective of any governmental funding, the inventor is considered the person who developed the invention.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

In the Eva-Maria Painer case, the CJEU ruled that copyright applies only to works that reflect the author's personality and result from their free and creative choices. Based on this reasoning, AI-generated outputs may not qualify for copyright protection, meaning individuals using AI to create content would not hold any copyright over those works.

On 12 September 2024, the Advocate General De La Tour issued his opinion on a request for a preliminary ruling from the Administrative Court of Vienna to the CJEU, stating that a data subject's right to receive meaningful information about the logic involved in automated decision-making (art. 15(1)(h) of the GDPR) should be balanced against the (IP) interests of the controller, such as the protection of its trade secrets. It is up to the supervisory authority or court involved to, based on the actual information and the facts of the case, determine the extent of the right of access that must be granted to the data subject. In any case, the controller should not be required to disclose to the data subject information which, by reason of its technical nature, is so complex that it cannot be understood by persons who do not have particular technical expertise, which precludes disclosure of the algorithms used in automated decision-making. It remains to be seen whether the CJEU judgment will follow the opinion of the Advocate General.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

The allocation of IP rights must be carefully assessed before concluding collaborative agreements. Both the ownership

of results and the IP that arises from such results as potential licence rights and the limits to such licence rights must be considered before R&D commences.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

In any collaboration in the healthcare industry, one must be wary of anti-competitive agreements. The (health) tech and pharmaceutical landscape is often characterised by major players, so caution needs to be exerted when contracting. In addition, the healthcare industry is one of the highest regulated sectors. The healthcare company must take the lead in assuring that the non-healthcare company understands and abides by healthcare regulations whenever it applies to the latter.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

As discussed above (see question 5.5), federated learning can help to overcome data protection-related obstacles to collaborative big data projects, amongst others, by reducing the amount of personal data processed by third parties (data minimisation) and by avoiding the need to transfer data to other jurisdictions (with potentially inadequate data protection and privacy laws). However, it does not solve the typical uncertainties relating to data processing roles and responsibilities. Indeed, a party can be considered a data controller in relation to certain data without actually receiving such data in raw form. Consortium partners need to take into account that having their respective roles and responsibilities clearly defined is imperative to avoid ambiguity for data subjects. This can cause considerable delays in the negotiation of partnership agreements. Another important consideration is whether the partners have the right to process existing research data for secondary use in a federated learning project, especially when the data subject's consent is used as the legal basis for the original collection and processing. The GDPR and the European Commission's guidelines offer some flexibility when it comes to obtaining consent for a broader area of research rather than for one research project (see Recital 33 of the GDPR).

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

As already discussed above (see questions 3.1 and 4.7), several data protection-related challenges need to be overcome when using generative AI in the field of healthcare. The most fundamental barrier may be the right of a data subject not to be subject to a decision based solely on automatic means that significantly affects them (art. 22 of the GDPR). While there are exceptions to this principle (e.g. explicit consent and suitable safeguards), a data subject has the right to receive meaningful information about the logic involved in the automatic decision-making and to obtain human intervention and contest a decision made by automated means. This is particularly difficult when the processing has been done by artificial neural networks, as it may be impossible to determine how the AI decided on a particular outcome.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

Under the AIA, each Member State should designate at least one notifying authority and at least one market surveillance authority as national competent authorities for the purpose of supervising the application and implementation of the Act. These authorities are still to be appointed.

The notifying authority will be responsible for setting up and carrying out the necessary procedures for the assessment, designation, notification and monitoring of conformity assessment bodies (i.e. third-party bodies which, once notified, are responsible for verifying conformity of high-risk AI systems before their placement on the market). For Belgium, it is anticipated that the existing notifying authorities under current EU legislation will be designated as the notifying authorities for the AIA within their respective areas of competence. In the case of digital health products, this role is expected to be assigned to the FAMHP.

It is further expected that the Belgian DPA will be appointed as the market surveillance authority responsible for enforcing compliance with the AIA. This is also the recommendation of the KCE in its recent policy brief on the implementation of the AIA in Belgium. A key argument in favour of having data protection authorities at the forefront of AI regulation is that this would allow for a centralised (cross-product) approach to market surveillance. The DPA's decisions would apply to all types of products incorporating AI/ML systems, which reduces the risk of having conflicting interpretations of the AIA by different authorities regulating different types of products. The Belgian DPA has already offered guidance on how the GDPR interacts with the AIA.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

As stated above (see question 2.2), the AIA has recently entered into force. The AIA's obligations will be implemented in phases. The provisions related to prohibited AI systems and AI literacy will take effect on 2 February 2025. Specific obligations for general-purpose AI models will become applicable on 2 August 2025. Most other obligations under the AIA, including those for high-risk AI systems and systems with specific transparency requirements, will take effect on 2 August 2026. The remaining provisions will become applicable on 2 August 2027. Consequently, several procedures are still ongoing regarding the designation of the competent authorities and the further implementation of the regulation.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

According to the case law of the Court of Justice, copyright protection is merely possible if the author has been able to express his creative abilities by creating free and creative choices that give a personal touch to the work. A work, made

or improved by AI or ML, cannot be protected by copyright if it is created without creative human involvement and does not meet the requirement of originality. With regard to patents, according to the EPO and art. XI1. 4 of the CEL, algorithms are *per se* of an abstract mathematical nature and normally exempt from patent protection. If not exempt from patentability, for example, when incorporated in technology, other problems occur. When AI is merely used as a tool to aid a researcher in the development of an invention, the researcher shall still be the inventor. It becomes more complicated if human involvement is limited or non-existent. Problems may arise with the condition of inventiveness if the human intervention in the creation of an invention did not require any originality, creativity or intellectual contribution from the researcher. Under current patent law, an inventor can only be a person, and AI cannot be seen as the inventor. The question arises in such cases whether it is more adequate to allocate the patent to the developers of the AI technology or to the owners of the AI technology, rather than to the person who "notices" the invention developed by the AI (the researcher).

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

The quality of the data used in ML is essential for the quality of the results it presents. Therefore, companies developing AI technology will become increasingly interested in (exclusive) licences on quality datasets with the least restrictions possible. However, the GDPR principle of data minimisation and the restrictions on processing data for a purpose other than for which it was initially collected, may directly clash with the commercial interests of tech companies. Moreover, data protection legislation principally prohibits the processing of health-related data, unless an exception, such as consent of the data subject, applies. Transparency and patient empowerment could have beneficial effects on a patient's willingness to consent to the use of its data for certain purposes. As stated above, the European Health Data Space will also improve the access to and encourage the sharing of healthcare data in the EU market.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Generative AI differs from standard AI as it is not limited to rule-based predictive tasks but instead uses ML to analyse data, recognise patterns and generate new content that mimics human creativity. Both generative and standard AI fall within the AIA framework. The AIA recitals classify generative AI models as "general-purpose AI models", given their ability to generate diverse content such as text, audio, images and video for various tasks. These models are subject to a distinct regulatory framework under the AIA. While most AIA provisions apply to both generative and standard AI systems, additional transparency obligations apply to generative AI providers and deployers, including the requirement to clearly indicate when content has been artificially generated or manipulated.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Most of the risks associated with AI in general are enhanced when dealing with generative AI technologies. First of all, generative AI can contribute tremendously to the spreading of misinformation and the distribution of harmful content online. The additional transparency obligations imposed by the AIA on generative AI systems should (somewhat) alleviate concerns in that respect (see question 8.5). Further, generative AI poses additional challenges with respect to copyright infringements. The development and training of generative AI models require access to vast amounts of text, images, videos and other data. Text and data mining techniques may be used extensively in this context for the retrieval and analysis of such content, which may be protected by copyright and related rights. When generative AI tools are trained on copyrighted material, the copies of the input data created by these tools may be considered "reproductions" of the original content. If these copies are made without the prior authorisation of the rights holder, such use could constitute copyright infringement. The AIA addresses the interaction between AI technologies and copyright protection. Providers of general-purpose AI models must implement a policy to comply with EU laws on copyright and related rights, in particular to identify and respect the rights of copyright holders. They must also provide a detailed summary of the content used for training the general-purpose AI model so that rights holders can enforce their rights. Finally, ensuring compliance with GDPR and determining liability for damage caused by the output system are also complicated by the specific nature of generative AI.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

Data protection authorities are stressing the importance of compliance with the GDPR in the development of AI systems. The Belgian DPA has recently released guidelines on AI and the GDPR, highlighting the critical need to follow data protection principles to ensure AI systems operate ethically. The guidelines discuss the main data protection principles that are relevant to AI systems, such as lawfulness, purpose limitation and data minimisation, storage limitation, etc. However, the guidelines do not address the deletion of (unlawfully processed) personal data embedded within AI models. Even if personal data was processed lawfully in the development of the AI model, the GDPR requires the erasure of personal data without undue delay upon request of the data subject. For AI model developers, this may technically not be feasible.

On 18 December 2024, the EDPB adopted an opinion on the use of personal data for the development and deployment of AI models. In this opinion, the EDPB states that when an AI model was developed with unlawfully processed personal data, this could render the subsequent operation of the AI model unlawful, unless the AI model has been duly anonymised (meaning that it is very unlikely to directly or indirectly identify individuals whose data was used to create the model, or to extract such personal data from the model through queries). However, the extent to which the lack of legal basis for the initial processing activity impacts the

lawfulness of the subsequent processing should be assessed on a case-by-case basis, depending on the context of the case. If the AI model is developed and deployed by different controllers, the controller deploying the AI model should in any case conduct an appropriate assessment to demonstrate compliance with GDPR as part of its accountability obligations.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Besides the general regimes of contractual and extra-contractual liability, the regimes of product liability and medical liability must be considered. A two-track system exists for medical liability in Belgium. On the one hand, the patient can invoke the medical liability of its physician or the hospital. On the other hand, a fund has been established to compensate severe damage caused by "medical accidents without liability". Furthermore, product liability is based on strict liability. A party claiming damages must only demonstrate a defect in the product, the damage and the causal relationship between the defect and the damage. The fault of the manufacturer need not be established. A product is defective if it does not provide the safety one is entitled to expect from that product. Any person in the production chain, the EU importer and the supplier may be held liable. As such, a physician or hospital may take the role of manufacturer or supplier of a defective product. The EU has recently made efforts to modernise the product liability regime to be more resilient for the current digital age, by means of the (slightly) updated liability framework of the Digital Services Act, the new Product Liability Directive (which entered into force on 8 December 2024 and should be transposed into national law by 9 December 2026) and the Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). These instruments aim for a more equal sharing of the burden of proof for complex digital solutions between the claimant and manufacturer, ensuring better protection for victims.

9.2 What cross-border considerations are there?

Within the EU, product liability is more or less harmonised and a patient suffering damages from a defective product such as a medical device will be granted similar protection in all Member States. The EU importer can also be held liable in the same manner as a foreign manufacturer can be. This ensures there is always an EU-based liable party from whom a victim can claim compensation, even when the manufacturer itself is not based in the EU. However, as for medical liability, the Law on Medical Accidents of 31 March 2010, providing compensation for medical accidents without liability, only applies to healthcare provided on Belgian territory (regardless of the patient's nationality). Several other countries do not have a regime for faultless medical liability; accordingly, a Belgian patient may not enjoy equal protection when receiving healthcare services abroad. Lastly, the EU Directive on the Application of Patients' Rights in Cross-Border Healthcare is taking its first steps in ensuring proper professional liability insurance in cross-border healthcare within the EU.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

In addition to the aforementioned considerations relating to cybersecurity and data protection, companies developing and marketing AI-driven digital health solutions should be aware of the stringent regulatory and compliance framework under which the healthcare sector operates, which entails corresponding rigorous duties and liabilities. It is therefore important to seek (local) expert advice and guidance on the requirements associated with entering the healthcare market in general.

To minimise the risk of medical errors caused by the use of AI-driven devices, it should be kept in mind that AI may work well in efficiently processing large amounts of data to suggest and verify conclusions (perhaps correcting human mistakes), but should not be deployed without human intervention and oversight. From a data protection perspective, data subjects (e.g. patients) have the right not to be subject to a decision based solely on automated processing (art. 22 of the GDPR). It is therefore important that every diagnosis or treatment decision made by or on the basis of AI-driven technology is carefully reviewed by a natural person (i.e. the HCP). This can be challenging as it may not always be clear how the software has reached a certain conclusion. The new EU Product Liability Directive and the proposal for an AI Liability Directive provide for the combined application of a strict (product) liability and a fault-based liability regime for AI technologies. The latter introduces a (rebuttable) presumption of a causal link between the provider's or user's fault and the output produced by the AI system, as well as disclosure requirements to aid victims in providing the evidence to support their claim. The proposal also aims to complement the Product Liability Directive by extending liability beyond AI providers to include users, holding them accountable for both the output and failure to produce output generated by the AI system. Parties involved (providers, manufacturers, importers, distributors and users of AI systems) thus have a great interest in allocating roles and responsibilities in an appropriate manner and addressing potential risks when negotiating (service) agreements. Attention should hereby also be given to consistency with the roles of data controller and data processor in such agreements. Finally, the express recognition of software as a product within the scope of the strict product liability regime urges manufacturers of AI systems to regularly supply the updates or upgrades necessary to address evolving cybersecurity vulnerabilities and maintain the product's safety.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

GDPR enforcement consists of a combination of public enforcement (by supervisory authorities imposing administrative sanctions as well as through the criminal justice system) and private enforcement (civil liability).

There are several legal grounds on which a data subject can file a complaint with the Belgian DPA to initiate public enforcement. The dispute chamber can impose various sanctions, including fines, but it does not have the authority to award

compensation to the data subject. Consequently, the proceeds from financial sanctions will not benefit the complainant.

To receive compensation for the damage suffered due to misuse of healthcare data in the training of AI models, the injured party can rely on art. 82 of the GDPR. Similar to the general regimes of contractual and extra-contractual liability in Belgian law, which are also available to the injured party in this instance, the claimant must provide proof of a violation of the GDPR, material or immaterial damage and a causal link between the violation and the damage. It should be noted, however, that a claim for compensation based on art. 82 of the GDPR can only be brought against data controllers and data processors.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Caution should be exercised when making use of Cloud-based services, as this is an area particularly sensitive to data breaches, cybersecurity issues and other data protection hazards. If a (digital) health company/healthcare organisation makes use of the services of a Cloud service provider, such service provider will generally be considered the processor, which processes personal data on behalf of the company or organisation (controller) and which may be working with multiple sub-processors. Consequently, a sound data-processing agreement must be concluded, including extensive audit rights for the controller and a liability clause that sufficiently protects the controller in the event of claims by data subjects or a data protection authority as a result of infringements by the processor. Furthermore, the healthcare industry is notably vulnerable to cyber-attacks; therefore, it is of utmost importance to ensure that Cloud service providers offering services to the (digital) health industry have taken adequate organisational and technical measures to safeguard any personal data and confidential documents stored. In this regard, the Directive (EU) 2022/2555 (NIS 2 Directive), which aims to ensure a higher level of security for essential service providers, entered into force on 16 January 2023 and has been transposed into Belgian law by the Act of 26 April 2024, which will apply as of 18 October 2024. NIS2 extends the scope of entities to which the NIS requirements apply to also cover hospitals and other HCPs. Finally, Cloud service providers are also included as intermediary service providers in the Digital Services Act. Cloud service providers are under an obligation to implement appropriate "notice and take action" mechanisms and need to be transparent if content is taken down.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Entering the healthcare industry means entering a highly regulated context, in which innovating might be challenging. Market strategies shall have to be adapted to the specific regulatory framework governing health products and services. For instance, the promotion of medical devices has been severely restricted. Further, the company shall have to be prepared to invest heavily in compliance, e.g. data protection laws, medical device regulation, product safety, etc. Lastly, the company will have to bear in mind that it will have to represent the interests, not only of the end-user, but also of doctors, hospitals, health insurance providers and the NIHDI.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

To assess the growth potential and the relative strength of a digital healthcare venture amongst its competitors, one needs to take account of certain elements. It is important to evaluate the IP protection the venture has obtained (or can likely obtain in the near future) for its product, whether the product shall classify as a medical device or not and whether reimbursement has been obtained or is foreseeable to be obtained in the near future. The safety of the product and potential risks for liability claims need to be determined and one needs to ensure that there is a market for the health product, consisting not only of end-users, but also physicians and hospitals willing to prescribe or use the product in their provision of healthcare services.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The lack of reimbursement for a great number of digital health solutions is one of the major deficiencies in the Belgian (regulatory) landscape. In addition, uncertainty regarding the interpretation of existing legal frameworks on new health technology hinders swift adoption. Although the primary responsibility for healthcare remains with the Member States, a more harmonised approach at EU level may benefit the cross-border offering of digital healthcare services and products, a situation that might improve once the EU's Digital Strategy is fully implemented. Finally, it needs to be noted that, although the government has already initiated certain financial incentives for health practitioners to implement electronic health records, such incentives may need to be extended to other digital health applications.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The NIHDI is responsible for the accreditation of physicians and pharmacists, while organisations such as the Joint Commission International accredits hospitals in Belgium. As the NIHDI is also the institution responsible for reimbursement decisions (see question 10.6), naturally, its endorsement of digital health solutions is essential to steer clinical adoption. In addition to the NIHDI, the guidance and advice of the deontological body of physicians, the NCOP, are crucial in the long road ahead to better patient care through digital health.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

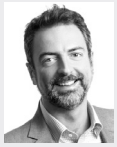
Digital health solutions that are medical devices can be reimbursed by the NIHDI if they fulfil the reimbursement criteria (see question 3.1 above). However, other digital health solutions and telehealth services are currently not part of the nomenclature of the NIHDI and therefore are not currently reimbursed.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

There are several gaps in the regulatory framework for the assessment of digital health solutions, particularly those incorporating AI and ML. One key challenge involves the evaluation of the safety and efficacy characteristics of SaMD and AI/ML-powered solutions. For instance, under the MDR, a medical device needs to undergo a new conformity assessment if it undergoes modifications before being placed on the market. While this approach is well-suited for traditional, static medical devices, it poses challenges for dynamic technologies that frequently require updates, security patches and algorithm refinements on the basis of new data. The AIA does not fully resolve this issue of continuous learning AI models, with algorithms evolving based on real-world data.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

The current economic turbulence, inflation and supply chain disruptions will undoubtedly continue to have an impact on the digital health landscape. Payers will have to find new and inventive ways of funding health solutions to accommodate constrained healthcare budgets and fragmented reimbursement schemes, for example by exploring value-based payment schemes. On the other hand, consumers and patients may find difficulty in affording innovative, health-targeted consumer devices or medical devices due to the relatively higher cost of living. Shortages in, for example, the chip industry have important consequences for the costs and availability of medical devices. Finally, (venture capital) investment in healthcare companies leveraging (generative) AI has exponentially increased and will likely continue to do so in 2025.



Olivier Van Obberghen works exclusively for clients in the life sciences and innovative technologies sectors. He co-heads the Life Sciences department of Quinz together with Pieter Wyckmans.

Quinz
Medialaan 28B, B1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: olivier.vanobberghen@quinz.be
LinkedIn: www.linkedin.com/in/olivier-van-obberghen-5906a4

Pieter Wyckmans provides expert advice to companies and organisations active in the (bio-) pharmaceutical, biotech and smart devices sectors. Pieter co-heads the Life Sciences department of Quinz together with Olivier Van Obberghen.

Quinz
Medialaan 28B, B1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: pieter.wyckmans@quinz.be
LinkedIn: www.linkedin.com/in/pieter-wyckmans-39499b8

Amber Cockx is a Life Sciences lawyer with a main focus on technology and data protection matters. Amber provides transactional and regulatory support to clients active in the pharmaceutical and medical devices sector. Her main areas of expertise comprise transactional and regulatory assistance throughout the entire product life cycle, from negotiating and drafting contracts, coordination of international R&D collaborations, through clinical phases, marketing authorisations, advertising and promotion, pricing and reimbursement, and interactions with healthcare professionals and healthcare organisations.

Quinz
Medialaan 28B, B1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: amber.cockx@quinz.be
LinkedIn: www.linkedin.com/in/amber-cockx-520914170

Chaline Sempels is a lawyer focusing on the life sciences industry, including digital health. She supports clients ranging from innovative start-up ventures to multinational corporations in (strategic) transactions and European regulatory affairs, throughout the entire product life cycle. In this context, her main areas of expertise include negotiating and drafting (supply chain and distribution) agreements, co-ordination of international R&D collaborations (the Horizon 2020 funding programme, the Innovative Medicines Initiative (IMI2) programme), medical devices, software applications and emerging technologies, and interactions with healthcare professionals and organisations.

Quinz
Medialaan 28B, B1800 Vilvoorde
Belgium

Tel: +32 2 255 73 80
Email: chaline.sempels@quinz.be
LinkedIn: www.linkedin.com/in/chaline-sempels-387605179

Quinz is a Brussels-based law firm with a strong focus on Life Sciences. Quinz assists the global, regional (EMEA, LATAM, APAC) and local (Belgium, Luxembourg and the Netherlands) legal departments of pharmaceutical companies on a broad array of (strategic, operational, licensing and M&A) transactions throughout the life cycle of a life sciences product. Quinz has also developed a sound expertise in regional and local regulatory work (including pricing and reimbursement, clinical trials, data transparency, marketing authorisation procedures, cGMP) and compliance matters (including transfers of value, promotion of life sciences products, antitrust compliance questions, patient-directed programmes, GDPR). Its Life Sciences department is headed by Pieter Wyckmans and Olivier Van Obberghen.

www.quinz.be

Canada


Vanessa Grant


Véronique Barry


Manpreet Singh


Sarah Pennington

Norton Rose Fulbright

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

"Digital health" is defined as health technologies that improve access to healthcare information, facilitate diagnosis and treatment, and improve patient access to care. More specifically, "digital health" may be defined as data-driven healthcare solutions and individualised delivery of therapeutics and treatments to patients using information technologies that enable seamless integration and communication between patients, healthcare providers, and others supporting healthcare systems.

Digital health technologies include stand-alone software applications, integrated hardware and software platforms, and medical devices (MDs) that include software and artificial intelligence (AI).

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Canada's health regulatory authority, Health Canada (HC), notes that its key areas of focus for digital health include:

- wireless MDs;
- mobile medical apps;
- telemedicine;
- software as a medical device (SaMD);
- AI;
- cybersecurity; and
- MD interoperability.

1.3 What is the digital health market size for your jurisdiction?

According to Statista, a global data and business intelligence platform:[1]

- revenue in the digital health market is projected to reach US$3.933b in 2025;
- revenue is expected to show an annual growth rate (CAGR 2025–2029) of 7%, resulting in a projected market volume of US$5.156b by 2029;
- the average revenue per user is expected to amount to US$176.90;
- in global comparison, most revenue will be generated in the United States (US$54b in 2025); and
- the market's largest area will be digital treatment and care with a total revenue value of US$2.507b in 2025.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

It is difficult to indicate the five largest by revenue, as many companies in the digital health space are privately held. Revenue information is not available for privately held companies in Canada. Based on a report from Capital IQ, the five largest (by revenue) publicly traded companies that indicate that digital health is a business line include Telus Corporation, WELL Health Technologies Corp., Medical Facilities Corporation, Vitalhub Corp., and Mednow Inc.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Please see our answer to question 1.4 above.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The responsibility for Canada's healthcare system is divided between the federal government and provincial and territorial governments.

The federal government determines and administers national health guidelines (including regulatory approvals), provides financial support to the provinces and territories and administers the provision of healthcare to certain federal groups (for example, the military). HC is the primary regulatory authority responsible for the administration of federal legislation as it applies to digital health, particularly through its Medical Devices Directorate (MDD).

The provincial and territorial governments are responsible for funding and delivering healthcare services in accordance with both federal and provincial legislation.

As a result of this division of power, both federal and provincial laws apply to the regulation of digital health, including:

- the *Food and Drugs Act* (Canada) (FDA);
- the Medical Devices Regulations (Canada) (MDR); and
- provincial laws, including professional and ethical standards.

HC can take enforcement action to address non-compliance, including:

- refusal, suspension, cancellation, or revocation of an authorisation, licence, or registration;

- recommending the refusal or seizure of imports at the border;
- adding new terms and conditions to an authorisation;
- issuing a recall order; and
- seizure and detention, forfeiture, and destruction.

HC also works closely with other federal, provincial, and territorial agencies to enforce federal requirements, including the Public Health Agency of Canada (PHAC), the Competition Bureau, and Justice Canada. HC can also apply for a court injunction to prevent certain conduct or refer the results of any investigation to the Public Prosecution Service of Canada, recommending prosecution of offences under the FDA and the *Criminal Code of Canada*, where applicable.

From a regulatory perspective, the FDA, MDR and HC guidelines govern the import, sale and advertisement of devices and SaMD in Canada.

Other federal statutes apply with respect to the sale and advertisement of digital health services, including:

- federal privacy legislation (discussed below) administered by the Office of the Privacy Commissioner of Canada (OPC);
- the *Competition Act* (Canada), administered by the Competition Bureau, which applies to all commercial activities in Canada, and deals with, among other things: misleading advertising; anti-bribery and corruption legislation; and
- sanctions and related measures imposed by Canada against a number of countries, individuals and entities.

Provincial and territorial laws are typically administered and enforced by:

- the ministries of health of each of the provinces and territories that are responsible for the provision of healthcare in their jurisdiction;
- public insurance agencies; and
- professional colleges, orders, and associations, with respect to healthcare professionals (HCPs).

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

From a regulatory perspective, the federal government regulates the approval, import, sale, and advertisement of devices and SaMD under certain laws, including the FDA and the MDR.

Provincial and territorial legislation also governs the provision of digital health services, including, for example:

- professional and ethical standards for healthcare providers;
- legislation specifically applicable to digital health services, e.g., medical billing processes and medical/privacy standards;
- legislation applicable to the provision of products and services (including digital health), e.g., consumer laws, privacy, cybersecurity, and procurement rules; and
- legislation and professional standards, codes and guidelines for HCPs and pharmaceutical companies, established by the legislature, industry associations, professional colleges, and other self-regulatory groups.

Anti-kickback and competition laws are also in force in Canada, including the following:

- The *Competition Act* (Canada) governs how businesses deal with their competitors. Under the Act, any action viewed as promoting an anti-competitive business strategy can lead to severe penalties, ranging from injunctive actions and financial penalties to prison sentences for serious offences. Advertising for digital health services and advertising by HCPs also fall under the general advertising rules of the Act, in addition to any provincial legislation.
- Transparency and anti-kickback regulatory schemes include the *Canada Business Corporations Act*, where private entities governed by that Act must create and maintain a register that identifies individuals with significant control over a corporation. Similar requirements also exist in some provinces.
- Codes of conduct promulgated by professional organisations, such as the Medtech Code of Conduct, require members to comply with transparency requirements.
- Provincial and territorial transparency and anti-kickback requirements apply to HCPs, and, in some provinces, may also extend to entities interacting with HCPs.
- Canada has also enacted anti-bribery legislation, including the *Corruption of Public Officials Act* (Canada), which implemented Canada's obligations under the Organisation for Economic Co-operation and Development (OECD Convention on Combating Bribery in International Business Transactions). There are criminal sanctions under the Criminal Code of Canada for domestic bribery and corruption. In Québec, anti-corruption compliance is enforced by a multi-sector agency under the *Anti-Corruption Act* (Québec).

Privacy is dealt with both federally and provincially, and the following are some of the federal and provincial laws that may apply to digital health:

- The federal *Personal Information and Protection of Electronic Documents Act* (PIPEDA) is the general statute governing private-sector privacy considerations. Alberta, British Columbia, and Québec have their own private-sector privacy laws, which replace the PIPEDA with provincial personal information (PI) considerations. The same applies to the personal health information (PHI) protection laws of New Brunswick, Nova Scotia, Ontario, and Newfoundland and Labrador. Québec's PHI protection law also came into force in 2024.
- Many laws impose various restrictions and requirements on access and processing of PI. Informed consent must be obtained from individuals before processing their PI. Requirements for consent to be valid vary by province and involve providing clear information about what PI is being collected and the purposes of collection, use or disclosure. In most cases, express consent is required. If third parties are involved, individuals must also be informed of this beforehand.
- Most laws impose disclosure obligations in case of a privacy breach. In addition, most jurisdictions consider PHI to be "sensitive PI", subject to stricter requirements and expectations.
- Major privacy reforms have taken place at both the provincial and territorial and federal levels. After Québec, which has reformed its PI/PHI protection regime in the past years, notably to emulate the European General Data Protection Regulations, other provinces, including Ontario and Alberta, are discussing implementing statutory changes to their provincial data protection laws.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

Key areas of enforcement

At a federal level, the MDD's key areas of focus include:

- wireless MDs;
- mobile medical apps;
- telemedicine;
- SaMD;
- AI;
- cybersecurity; and
- MD interoperability.

At a provincial and territorial level:

- professional associations, orders and colleges ensure that only licensed or duly qualified HCPs perform reserved/exclusive activities and that the services provided comply with applicable professional and ethical standards; and
- ministries of health and other relevant ministries ensure that digital health products and services comply with provincial and territorial laws and standards.

Both federal and provincial and territorial authorities will ensure that digital health products and services are advertised in accordance with federal, provincial, or territorial law.

Emerging areas of enforcement

The areas of focus described above are supplemented by emerging standards and rules, such as:

- non-binding standards adopted by non-profit organisations such as Canada's Drug Agency;
- codes of conduct, such as the MedTech Code of Conduct, promoting ethical business practices and socially responsible interactions with HCPs, healthcare institutions and government officials;
- emerging rules and standards, such as the federal Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems, identifying measures that organisations are encouraged to apply to their operations when developing and managing AI systems; and
- proposed laws, for example, Ontario's Bill 231 (the *More Convenient Care Act*), which aims to regulate digital health identifier activities and describe how PHI may be collected, used, and disclosed in relation to these activities.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

The FDA and MDR apply to devices, including SaMD. HC has published the guidance "Software as a Medical Device (SaMD): Definition and Classification", setting out when software is considered to be a MD and therefore subject to the MDR and how such a MD may be classified depending on the potential risks of its use (e.g., Class I, II, or III).

Specifically, software intended to inform patient management, drive clinical decision-making, or treat or diagnose disease is regulated as a MD. If the types of disease involved are non-serious, the software may be classified as a Class I or II device. If the types of disease are more serious or critical in nature, the software is more likely to be classified as a Class III device.

If the software is intended to image or monitor a physiological process or condition, it is more likely to be classified as a Class II device rather than a Class I device. If an erroneous result could lead to immediate danger, it is more likely to be classified as a Class III device rather than a Class II device.

Manufacturers of Class II, III, and IV MDs must have each MD approved and licensed by HC. HC will review data supporting design, instructions for use and efficacy and safety data when determining whether to license a product for import and sale into Canada. In some cases, MDs must comply with quality standards established by recognised self-regulatory organisations, such as the American Society for Testing and Materials or the International Standards Organization. Additional steps and requirements will need to be met for investigational MDs to be imported and used in clinical trials.

Manufacturers of MDs are also typically required to apply for and obtain a medical device establishment licence (MDEL) from HC to manufacture, import or distribute MDs in Canada. Among other requirements, the manufacturer must show the MDs are designed and manufactured in compliance with ISO 13485 and other MD-related good manufacturing practices.

In addition to federal requirements, provincial or territorial requirements may apply to devices and software, imposing constraints (notably on the supply of devices to end users) or additional obligations on companies or their intermediaries.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

HC's Draft Guidance Document[2] provides that a MD that uses machine learning (ML) to achieve "medical purposes" within the meaning of the FDA qualifies as a MD and is therefore subject to the FDA and MDR. In order for such a MD to be approved for clinical use, it will have to comply with the steps described above, including considerations of safety and effectiveness.

Digital health devices that are classified as MDs also must comply with federal, provincial, and territorial privacy laws, and with the health and other core regulatory schemes detailed elsewhere in this chapter.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

HC has begun rolling out guidance regarding considerations for AI/ML-based digital health solutions. In conjunction with US and UK health authorities, HC identified guiding principles to be considered when developing AI/ML-based digital health solutions, to ensure they are safe, effective, and high quality. These principles are meant to promote the adoption of good practices proven in other industries and create new specific practices for the medical technology and healthcare sector.

Furthermore, the Director of the Digital Health Division for the MDD has indicated that updated guidance on ML-enabled MDs is expected in response to feedback received on its draft guidance document. The Director has also suggested that predetermined change control plans will be permissible under the new guidance. As such, manufacturers will likely be able to submit plans for what modifications will be made to a MD at a later date and how the modifications will be assessed. Federally, Canada is also exploring legislative changes to regulate AI systems, which may impact AI/ML-enabled digital health devices.

More recently, HC has also established transparency guiding principles to be considered by the healthcare industry when developing AI/ML-based health solutions. These transparency principles were developed to:

- promote proper communication of information that could impact risks and patient outcomes;
- consider what information should be made available to the intended user/audience of a given AI/ML-based technology; and
- ensure the use of the best media, timing and strategies for proper communication.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

See question 2.4.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

See question 2.2.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

This is regulated at a federal and provincial level depending on the cause of action or type of request.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

In addition to the specific items noted below, manufacturers should consider compliance with data privacy and protection, the protection of PHI and cybersecurity, as well as healthcare regulatory matters. In addition to relevant legislation, there may be common or civil law remedies if a digital health technology causes harm to a patient.

- **Telemedicine/Virtual Care**
  The Federation of Medical Regulatory Authorities of Canada recently published the FMRAC Framework on Virtual Care,[3] which proposed minimum standards for members regarding the provision of "virtual care". "Virtual care" is defined to include interviewing, examining, advising, diagnosing, and/or providing treatment services by means of electronic communication.
  HCPs performing virtual care must comply with the licensing requirements imposed by the regulatory college where they are licensed to practise, as well as the requirements of the college of the jurisdiction where the patient receiving virtual care is based.
- **Robotics**
  Robotics in a healthcare setting may be subject to the MDR, as well as regulations governing assistive devices for consumers. If robotics are classified as MDs, then, as noted elsewhere in this chapter, the manufacturer of such MDs must ensure the MD receives market authorisation and where applicable, an MDEL is obtained before the MDs can be imported, advertised, or sold.
- **Wearables**
  Depending on the intended use, wearables may be subject to regulation under the MDR. Wearables may also be subject to consumer product legislation.
- **Virtual Assistants (e.g. Alexa)**
  Issues arise where the virtual assistant provides diagnostic or therapeutic advice, in which case it may be classified as a MD and will be subject to the requirements described elsewhere in this chapter.
- **Mobile Apps**
  Mobile apps may, in some circumstances, be classified as a MD.
- **Software as a Medical Device**
  Software is considered a "medical device" when it is intended to be used for one or more medical purposes, and it performs these purposes without being part of a hardware MD.
- **Clinical Decision Support Software**
  Software intended to drive clinical decision-making and treatment may be regulated as a MD.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  There is currently no regulatory framework in Canada specific to AI. Some health regulations apply to certain uses of AI, but there is no overarching approach to ensure that AI systems address systemic risks during their design and development. Canada is in the process of developing and implementing common standards to ensure that AI systems are developed safely and ethically.
- **IoT (Internet of Things) and Connected Devices**
  Canada does not currently have Internet of Things (IoT)-specific legislation. The current approach to the regulation of web-enabled objects is a combination of federal, provincial, and territorial legislation.
  The primary issue with IoT is categorisation. The intended use of the connected devices impacts their categorisation – for instance, if a device plays a role in a hospital ecosystem, then it may be categorised as a MD.
- **3D Printing/Bioprinting**
  3D printing may engage the regulatory framework for custom-made MDs.
  Potential patent and industrial design infringement issues can also arise with some categories of bio-printing.
- **Digital Therapeutics**
  Digital therapeutic products are held to the same standards of evidence and regulatory oversight as other therapeutic products and must demonstrate their safety, efficacy, quality, patient centricity, privacy, and ongoing clinical impact.
- **Digital Diagnostics**
  Digital diagnostics, in performing diagnostic functions, may be classified as MDs and subject to regulation under the MDR.
- **Electronic Medical Record Management Solutions**
  Software intended to serve as electronic patient records, or tools to allow a patient to access their PHI, are excluded from regulation under HC's SaMD Guidance Document.
  Components, accessories, or modules within an electronic medical record system intended for use to diagnose, treat, mitigate, or prevent a disease, disorder, or abnormal physical state (or their symptoms) are considered a MD, and are subject to regulatory oversight under the MDR.

- **Big Data Analytics**
  Issues include ownership and use rights, privacy, informed consent, and data security. Federal, provincial, and territorial governments have introduced laws and/or guidance that are designed to govern the ethical use and generation of such data. Discrimination laws also exist to prohibit against discrimination against consumers in many jurisdictions.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Informed consent must be obtained from individuals before processing their PI. Some federal and provincial laws restrict the cross-border transfer of PI. Provincial cross-border transfer requirements can also apply as soon as PI is communicated outside the province, even within Canada. Some laws even limit the ability to transfer PI or impose additional preconditions.
- **Natural Language Processing**
  The appropriate categorisation of a Natural Language Processing (NLP) SaMD will be an issue, namely, whether the software or product satisfies the regulatory definition. If the NLP software is used as a part of a MD or SaMD used for diagnostic or therapeutic purposes, then it will likely be subject to the MDR.
  In addition, NLP models in public health settings should be trained with unbiased data and/or data where biases are appropriately accounted for (using data annotation).

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Key issues for digital platform providers include the following:
- whether the digital platform is required to be approved by HC or other regulatory bodies;
- data privacy and cybersecurity, including appropriate data management systems;
- informed consent from patients and other participants in the platform;
- cross-border transmission of PHI;
- liability for use of the digital platform; and
- intellectual property ownership and data governance.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

In Canada, there are both federal and provincial and territorial laws that cover the use of personal data and PHI. Each province and territory in Canada has a commissioner or ombudsman responsible for overseeing provincial and territorial privacy legislation.[4] Similarly, the federal government also has the OPC, which serves the same function on a federal level.

The key legal and regulatory issues to consider include:
- data privacy and cybersecurity, including appropriate data management systems;
- informed consent from patients and other participants in the platform;
- cross-border transmission of PHI;
- liability for use of the digital platform; and
- intellectual property ownership and data governance.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Federally, the PIPEDA governs private sector organisations' handling of PI in commercial activities. The PIPEDA applies across Canada (except, other than for cross-border transfers, in provinces that have enacted their own privacy laws deemed substantially similar to the PIPEDA). Additionally, the provinces may have their own laws specific to health data, such as Ontario's *Personal Health Information Protection Act* (PHIPA). These provincial laws impose various restrictions and requirements on collection, use and disclosure of PHI and often cover public sector entities and health information custodians (e.g., healthcare providers), with specific provisions tailored to the healthcare setting, such as obligations around the use of electronic health records.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

See question 4.2.

4.4 How do the regulations define the scope of personal health data use?

Where organisations collect or process PHI, they are required to obtain an individual's consent when they collect, use, or disclose that individual's PHI. For instance, Ontario's PHIPA governs how health information custodians, such as doctors, hospitals and other healthcare providers, handle PHI, with an emphasis on consent, data security, and limiting the use and disclosure of PHI to what is necessary for providing care. The provinces may also have laws focused on managing PHI in electronic health records and contain breach reporting and notification requirements. Generally, most laws are designed to regulate activities relating to PHI in the healthcare setting, highlighting the need for consent, individual access rights and protection of data. These laws collectively ensure responsible and secure use of PHI, with a strong emphasis on patient consent and privacy.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

The key contractual considerations include the following:
- ensuring appropriate consent for the collection of PI or PHI (and the regime for withdrawal of consent, access to and correction of PI or PHI) and defining specific purposes for data use;
- ensuring compliance with privacy laws including implementing physical, administrative, and technical data security measures;
- restrictions on disclosure of PI or PHI and cross-border transfer of data and establishing data retention periods and disposal methods; and
- establishing a liability regime for failure to comply with privacy laws.

Additionally, contracts should outline third-party processing requirements and include procedures for breach notification as a common issue in these types of agreements includes who takes the lead where there has been a data breach.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Under various privacy laws, PI and PHI must be kept accurate and complete as necessary for the purposes for which it is to be used. Organisations are directed to implement policies to maintain the accuracy of PI and PHI to reduce the risk of errors when making decisions about individuals or sharing information with third parties. Further, individuals typically have the right to access their own PI and PHI held by organisations and to request its correction if they believe the information is inaccurate.

Canadian law on bias and discrimination is also evolving. The federal government has previously issued guidance to federal institutions on their use of generative AI tools. The guidance complements and supports compliance with many existing federal laws and policies, including in areas of privacy, security, intellectual property, and human rights.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

See question 4.6.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Key issues under federal and provincial laws include:

- whether appropriate consent has been obtained;
- the scope of the consent and whether the person or entity obtaining the consent is complying with the scope of the consent;
- whether the data will be shared across borders; and
- whether the data can be used to identify a specific individual.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

See question 4.2.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

The nature of the entities does not change the issues relating to the sharing of PI or PHI.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

There are some initiatives to establish standards in Canada. The PHAC established an Expert Advisory Group (EAG) to advise on a pan-Canadian Health Data Strategy. In its final report, released in 2022, the EAG found that the sharing of healthcare data in Canada suffered from the following issues and recommended the adoption of a pan-Canadian Strategy:

- Duplicative and competitive activities: There is little formal coordination among initiatives to improve health data collection, access, sharing and use. Some of these efforts are duplicative and may move jurisdictions in different directions that fragment data and prevent learning.
- Mis-aligned priorities and specialised agendas: Health data priorities often prioritise solutions that make sense for individual jurisdictions, but do not scale. This may lead to systemic health inequities as data capabilities advance.
- No common vision for health data across jurisdictions: Past strategies have been incoherent without a unifying goal for health data. Governance structures have been incentivised to deliver short-term success without priority for long-term benefits within and across jurisdictions and for all people in Canada.
- Fragmented incentives and measurements: With a common vision, incentives can be aligned and organisations held accountable for following through on the Strategy.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

See question 5.4.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

The scope of patent protection for digital health technologies is similar to other technologies, protecting inventions that are novel, non-obvious (similar to inventive step) and have utility.

Digital health technologies are often implemented using computer or life-sciences technologies, and it is important to note that there is jurisprudence relating to whether such inventions should be considered patentable subject matter (similar to the United States concept of patent-eligible subject matter).

The most recent guidance is the practice notice PN2020-04, providing guidance on the current understanding by the Canadian Intellectual Property Office (CIPO) of the legal principles applicable in determining whether the subject matter defined by a claim is patentable subject matter, particularly in respect of computer-implemented inventions, medical diagnostic methods and medical uses.

Also noteworthy, the scope of industrial design protection for digital health technologies is similar to other technologies, protecting novel designs applied to physical or digital

products. Industrial design protection can apply to graphic user interfaces (GUI) and lasts for at least 15 years.

Digital health technology companies should consider industrial design protection to supplement or as a backup to patent protection, as GUIs face greater hurdles in obtaining patent protection compared to other technologies.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

The scope of copyright protection for digital health technologies is similar to other technologies, protecting literary, artistic, dramatic, or musical works and other subject matter known as performer's performances, sound recordings and communication signals. Copyright can apply to original literary, dramatic, musical and artistic works where the author was at the date of the making of the work a citizen or subject of, or a person ordinarily resident in, Canada or a treaty country (Berne Convention, Universal Copyright Convention or a WTO member), or any work that is first published in a treaty country even if the author was not a citizen or subject of, or a person ordinarily resident in, Canada or some other treaty country.

Copyright lasts for the life of the author, the remainder of the calendar year in which the author dies, and for 70 years following the end of that calendar year. Note that this lengthened term life of author plus 70 years is effective December 30, 2022.

Copyright can be protected both in a non-registered and registered form, with the benefits for registration being a notice mechanism providing evidence that copyright exists and that the person registered is the owner of the copyright. A formal copyright registration is useful in respect of enforcement and is typically sought for in respect of video game code and, consumer software, among others. The Copyright Office does not guarantee the legitimacy of ownership or the originality of a work.

Where an artistic design is applied to a useful article that is produced in quantities of 50 or more, the copyright becomes unenforceable. The only enforceable protection available in this situation is an industrial design registration.

The Canadian approach to "fair dealing" is an important consideration for copyright protection for digital health technologies. In particular, fair dealing provides an exception that allows the reproduction/use of copyrighted materials without permission, provided that use/dealing is "fair". Similar to the concept of "fair use" in the United States, in Canada, "fair dealing" is limited to specific enumerated grounds of protection.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

There is no registration process for trade secrets, but there can be criminal sanctions for fraud. It is important to maintain confidence, and the trade secrets must have economic value to be enforced. A key benefit of trade secret protection is that it can provide a protection without an expiry date.

Digital health technology companies should carefully consider trade secret protection against patent protection, as patent protection would necessarily require a disclosure.

Trade secret protection is a useful mechanism for protecting important intellectual property that requires protection for a period longer than patent protection or may have issues being protected by a patent. Trade secret protection can be useful for protecting process parameters, ML models and/or trained ML models, algorithms, processes, workflows, sensitive business information, customer lists, data, annotations, or labels for data sets, among others.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Academic institutions in Canada typically have published policies in respect of their internal policies for academic technology transfer to corporate entities. Each academic institution has different approaches for negotiating collaboration agreements as well as ownership and responsibilities for intellectual property protection.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

The scope of intellectual property protection for SaMD is treated similarly to the intellectual property protection for software (i.e., potentially protected under a combination of patents, industrial designs, copyrights, and trade secrets).

Similar issues arise in respect of the patentability of computer implemented inventions (e.g., software), and there are additional considerations around a prohibition around patenting methods of medical treatment (e.g., performance of surgery, administration of medicine).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

Whether or not an AI device can be named an inventor is not settled in Canada.

In November 2021, the CIPO issued a non-compliance notice for the Canadian patent application number CA3137161[5] identifying DABUS as the inventor along with a statement that "[t]he invention was autonomously generated by an AI" (the DABUS Application).

The CIPO stated that "[b]ecause for this application the inventor is a machine and it does not appear possible for a machine to have rights under Canadian law or to transfer those rights to a human, it does not appear this application is compliant with the Patent Act and Rules". However, the CIPO's notice noted that the applicant may attempt to comply with the *Patent Act* and *Patent Rules* by submitting a statement on behalf of the AI machine and identify, in this statement, himself as the legal representative of the machine.

It is not clear at the time of writing how a court would resolve the issue of whether an AI device can be named as an inventor of a patent or a patent application in Canada.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

Certain Canadian departments and agencies hold patent rights (e.g., federal science-based departments and agencies). There is a requirement of disclosure and ministerial approval

for any patent applications under the *Public Servants Inventions Act* involving an inventor who is a Canadian public servant (including reserve members of the Canadian Armed Forces and auxiliary members of the Royal Canadian Mounted Police).

There is no legislation in Canada that governs intellectual property rights resulting from research subsidised by public funds, but each organisation may have their own rules. Certain organisations will retain ownership and grant licences, while others transfer ownership to a university or a research institution.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

See above.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

The following are some key considerations:

- intellectual property ownership: who owns improvements, joint inventions, and who is responsible for any filings and maintenance;
- intellectual property liability: how will liability for intellectual property be divided;
- restrictions on use of intellectual property;
- third-party intellectual property considerations: infringement and licensing of third-party intellectual property;
- data collection, use and protection;
- cybersecurity;
- how the parties will apportion liability;
- limitations of liability between the parties;
- confidentiality obligations; and
- financial considerations: how will any resulting intellectual property be commercialised?

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

In addition to those set out above, common considerations include:

- data privacy and compliance;
- obtaining appropriate rights to use data;
- marketing and promotional activities; and
- regulatory restrictions.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Key considerations are similar to those in any data sharing agreement and include:

- reverse engineering;
- harmful code;
- whether the data will be shared across borders; and
- conditions and levels of access (ranging from fully open to limited access with permission).

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Key contractual and strategic considerations include:

- understanding the limits of the training data used to generate the information;
- guardrails to detect hallucinations;
- validation and testing of the outputs of the system;
- training of personnel to understand the limits of both the training data and the outputs, as well as understanding how to review outputs critically; and
- to the extent that the results of the generative AI are used to support clinical decision-making, HCPs in particular should note that the use of generative AI is intended merely as an aid to, and not as a substitute for, clinical judgment.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

Canada is making progress in establishing a regulatory framework for AI; however, there is no AI-specific regulation at the time of writing.

The most recent federal legislative effort was the *Artificial Intelligence and Data Act* (AIDA), part of Bill C-27, the *Digital Charter Implementation Act, 2022*. The AIDA aimed to regulate international and interprovincial trade and commerce in AI systems within a harms-based framework (e.g., high-risk applications compared to lower risk applications). However, this proposed law has not been enacted.

In 2023, the federal government introduced the Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems.[6] This code provides guidelines for organisations to follow, covering principles like accountability, safety, fairness, transparency, human oversight, and robustness. For public sector workplaces, the federal government also released a "Guide on the use of generative artificial intelligence", which provides similar best practices. Both guides are advisory in nature and do not carry the force of law.

Recent provincial initiatives to regulate AI systems include Ontario's proposed Bill 194, called the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*, which, if passed, would enact the *Enhancing Digital Security and Trust Act, 2024*, and allow the government to regulate how certain public sector entities use AI systems, including requirements to provide information, to develop and implement accountability frameworks and to take steps respecting risk management.

Canada's privacy regulators also oversee the use of PI and PHI in relation to AI systems. For example, the OPC jointly with its provincial counterparts provided guidelines in 2023 for the responsible use of generative AI.[7] These include principles for transparency, accountability, and fairness, helping organisations develop and deploy AI systems that protect privacy.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

See above.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Intellectual property rights to algorithms are generally owned by the organisations that developed the algorithms (e.g., wrote the original source code), and are protected using a combination of copyright, trade secret, and confidential information as intangible property.

For example, for an algorithm that is improved by ML without active human involvement, the Court of Queen's Bench of Alberta noted that a human authorship element is still required for copyright to subsist.

In 2022, the CIPO allowed a copyright registration of a painting "SURYAST" created by an AI tool, the RAGHAV Painting App (RAGHAV), and the intellectual property lawyer who created RAGHAV, Ankit Sahni, both of whom are listed as authors, and only Ankit Shani is named as the owner.

In this example, Ankit Shani allegedly provided the style and inputs, while RAGHAV chose the brush strokes and colour palette. As the CIPO does not review copyright applications for compliance, it is important to note that there may be limited precedential value in the CIPO registration until it is considered in a future court proceeding. For inventions without active human involvement in the software development, such as the DABUS inventions, it is still not clear whether the AI can take an ownership interest in the intellectual property rights.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Key commercial contractual and strategic considerations include:

- **Licence terms**: identify key licence terms before deciding which data set to be used, and to monitor compliance with these licence terms.
- **Attribution and notice requirements**: Attribution/notice requirements are typically straightforward to comply with, but a number of popular licences have "copyleft"/share-alike type provisions, and these must be assessed carefully for suitability. For example, if there are any additions, transformations, changes, etc., there may be an obligation to share the updated dataset. CDLA-Sharing-1.0, for example, has a data-set specific section stating that the terms do not impose obligations or restrictions on results from users' "computational use" of the data. See CDLA-Sharing-1.0 at Definitions 1.2, 1.11, 1.13, and most importantly, Section 3.5. ODbL is also a copyleft licence that has a share-alike requirement. These obligations could lead to a potential disclosure of proprietary information.
- **Quality of the data set**: Another important consideration is that there may be unaddressed or unidentified liability relating to errors, omissions, or inaccuracies in the underlying data set. Most data sets are provided "as-is" with disclaimers, and these issues could impact the accuracy or appropriateness of ML outputs. For healthcare data, there are additional considerations around identifiable personal data and ensuring compliance with health information protection and privacy laws. Further, a data set may inadvertently include unauthorised third-party data.
- **Uncertainty of enforcement**: In Canada, jurisprudence relating to intellectual property enforcement in respect of data sets is still evolving, and it is still unclear whether certain uses would even constitute infringement. For example, it is not clear whether the mere act of training a ML model using copyrighted works without authorisation of the copyright owner, without making a copy of the copyrighted work, would satisfy all of the elements required for copyright infringement.
- **Uncertainty of liability**: Similarly, if a trained ML model is directed by a user to perform an activity that is a potential infringement of a third party's intellectual property, such as generating an infringing work using a general-purpose trained model, it is not clear whether liability would attach to the provider of the ML model or the user, or both.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

As noted, a governing framework for AI in Canada is still evolving and as such, there is a lack of clarity on the regulation of AI technologies.

In 2023, however, the Canadian government introduced the Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems[8] to provide guidelines for private sector organisations to follow, covering principles like accountability, safety, fairness, transparency, human oversight and robustness. For public sector workplaces, the federal government released a similar Guide on the use of generative AI.

Canada's privacy regulators also oversee the use of PI and PHI in relation to generative AI systems. For example, the OPC, together with its provincial counterparts jointly provided guidelines in 2023 for the responsible use of generative AI.[9] These include principles for transparency, accountability, and fairness, helping organisations develop and deploy AI systems that protect privacy.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

See above. In 2024, the Competition Bureau released a Discussion Paper on AI and competition. The Discussion Paper explores several considerations for how AI may affect competition:

- AI and mergers and monopolistic practices: AI could affect market concentration and market power.
- AI and cartels: AI could be used to implement or sustain harmful or illegal cartel agreements.
- AI and deceptive marketing practices: AI, particularly generative AI, could be leveraged in deceptive or misleading marketing practices.

- AI and competition promotion: pro-competitive policies can be used to foster competition in the Canadian AI market.

An emerging issue in digital health is the use of transcription AI tools by HCPs. These tools can be used to capture and summarise conversations between HCPs and patients in real time. While these tools permit HCPs to spend more time face-to-face with patients rather than performing administrative tasks, they also come with various considerations related to transparency, accuracy, accountability, and data privacy. Professional colleges and other self-regulatory organisations are continuing to update their policies regarding the use of this and other generative AI-based technologies. Rules regarding patient consent or medical record-keeping related to AI transcription are expected to continue to evolve.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

See above.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Unlike some jurisdictions, there is no single source of law in Canada for product liability and adverse outcomes in digital health solutions. The sources of law will vary depending on whether the digital health service or product is subject to regulatory approval (as discussed above), how the product or service is delivered (for example, under a software licence agreement), to whom the product or service is marketed and sold (for example, is the sale to a consumer, a HCP, or a business), and what is incorporated in the product or service (for example, AI algorithms, or if PHI is being used and stored).

Sources of product liability law in Canada include the common law (in each of the provinces and territories, other than Québec) and the civil law in Québec. Common law and civil law, for example, will govern where the negligence of a manufacturer or provider of digital health services results in an adverse outcome. In general, subject to the regulatory status of the digital health product or service and the requirements of relevant provincial or territorial laws, product liability for digital health technologies is most often founded on failure to disclose risks, design concerns, and/or failure to meet specifications.

Consumer protection laws (federal, provincial, and territorial) may also apply to a digital product or service. For instance, the *Canada Consumer Product Safety Act* (CPSA) prohibits the manufacture, import, and sale of products that pose a danger to human health or safety. The CPSA's prohibition also extends to any advertising, packaging, or labelling that may mislead consumers as to the safety of the product. Similar prohibitions against false and misleading/deceptive advertising are set out in the FDA, the MDR, and the *Competition Act*.

The CPSA also restricts the sale of certain products and prohibits the sale of specific, inherently dangerous products. The CPSA does not provide for a private right of action for breach of the statute. However, consumers may initiate legal claims relating to the safety of goods and services based on common law negligence and failure to warn principles. In Québec, consumers have similar protections under the *Civil Code of Québec*.

To the extent that a digital health product's use and/or sale is subject to the terms of a contractual agreement, liability for adverse outcomes may also be governed by the law of contract. Contractual warranties as to the safety or quality of a product may introduce liability for any adverse outcomes that arise in respect of a digital health product.

9.2 What cross-border considerations are there?

Any digital health product or service sold in Canada is required to comply with Canadian federal, provincial, and territorial laws. As noted above, what laws apply will depend on the type of digital health product or service that is being offered.

If a digital health product is classified as a MD, an MDEL is required by importers or distributors of all device classes to permit them to import or distribute a MD in Canada.

International sales in Canada may also be subject to the *United Nations Convention on Contracts for the International Sale of Goods* (CISG), which was ratified by federal statute and provincial international sale of goods legislation. The CISG implies a warranty of fitness generally similar to that of provincial sale of goods legislation.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Best practices include:

- understanding the limits and biases of the training data used to generate the information;
- validation and testing of the system's outputs to assess accuracy and reliability;
- establishing AI/ML use policies for personnel;
- training of personnel to understand the limits and biases of both the training data and the outputs, as well as understanding how to review outputs critically;
- ensuring that any commercial contracts governing the use of AI/ML explicitly address liability for any errors; and
- to the extent that the results of the generative AI are used to support clinical decision-making, HCPs in particular should be aware that the use of generative AI is merely an aid to, and not a substitute for, clinical judgment.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

See question 9.3.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based services raise some of the following issues:

- Privacy issues: Some federal and provincial and territorial laws restrict cross-border transfers of PI. Cross-border transfer requirements can also apply when PI

is communicated between provinces and territories. Preconditions will need to be met prior to transfers taking place (e.g.: Québec legislation requires a privacy impact assessment be carried out prior to a transfer, to ensure that PI will be adequately protected at destination). Even when transfers can take place, companies are required to implement measures to ensure that PI shared across borders receives similar levels of protection.
- Cybersecurity issues and concerns: Implementation of effective security mechanisms, disaster recovery protocols and breach notification requirements are key.
- Records retention: HCPs are required to retain PHI for specific periods of time and need access to patient information on a continuous basis and in a timely manner.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Market access and adoption can be hampered by:
- The fact that the digital healthcare market is a highly regulated sector. In addition to federal requirements, provincial and territorial laws will apply. Legal requirements vary in each province or territory. Complying with all these regulatory requirements and obtaining all required authorisations can be challenging, in addition to representing significant time and cost investments, which companies may not be accustomed to or not be able to make.
- The need to comply with additional regulatory schemes if companies wish for their products or services to be covered by the public health plan or used by public healthcare institutions and HCPs.
- Practice of medicine and related laws, pursuant to which "reserved/exclusive" activities can only be performed by HCPs.

Each company will also need to comply with additional federal, provincial, and territorial requirements when doing business in Canada, including:
- advertising and marketing requirements;
- consumer laws in some cases;
- data privacy laws; and
- tax and trade and customs considerations.

These issues will be in addition to the practical challenges that companies may face, including:
- interoperability of their products and services with current technologies; and
- the patentability of their products and services.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Key considerations include:
- the availability of intellectual property protection;
- what, if any, data sets are being used;
- regulatory requirements;
- Canadian market adoption, since health technology adoption in Canada varies between provinces and territories; and
- Canada's public healthcare system and federal, provincial, and territorial reimbursement.

Despite the considerations noted above, Canadian companies are uniquely positioned to take advantage of opportunities outside of Canada in light of Canada's diverse population and proximity to the United States.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Barriers to adoption include:
- the fragmentation of the healthcare system in Canada;
- compliance, including regulatory and data privacy;
- public procurement rules; and
- medical billing process.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

At a federal level, HC approves MD and SaMD for their import, sale, and advertising in Canada.

Provincial and territorial HCP associations, colleges and orders determine those types of products and services that can be used by HCPs in order to enable them to comply with their legal, professional, and ethical requirements.

The federal, provincial, and territorial governments must approve products and services in order for them to be implemented by public healthcare institutions or paid for by public funding.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

Reimbursement for healthcare services in Canada is primarily funded by the federal, provincial, and territorial governments. Reimbursement for most Canadians is determined by each province and territory, with the federal government determining reimbursement for federal undertakings, such as the military. In addition, many employers offer healthcare insurance to cover services that are not insured (such as prescription glasses, dental care, and wellness services).

If a digital health solution provider wishes to obtain reimbursement through the public system, it will need to apply to each level of government where it wishes to obtain reimbursement. If reimbursement is expected in the private system, the digital health solution provider will need to either confirm that its solution falls within existing reimbursement codes or apply for and obtain appropriate reimbursement codes.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Advancements in digital health solutions outpace the introduction of regulations to govern them. Safety monitoring can be inadequate or ineffective for certain threats, such as cybersecurity. Likewise, some laws fail to address concerns, such as transparency, impacts of self-learning tools and the uses made of such data.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

In 2022, the Canadian Competition Bureau released Part 3 of its Digital Healthcare Market Study. The Competition Bureau made three key recommendations:

1. "Review payment models for health care providers to support the appropriate use of digital health care.
   a. Expand billing codes and digital programs to promote the uptake of valuable innovative technologies.
   b. Use lessons learned from the COVID-19 pandemic to create permanent and appropriate virtual care billing policies in the short term.
   c. Reform compensation models in the longer term to further enable digital health care and support better health outcomes.
2. Implement licensing frameworks that allow providers, where appropriate, to practise beyond provincial and territorial borders to improve digital health care delivery.
3. Review and modernise policies to facilitate the effective uptake of digital health care."

In addition to the foregoing, other issues include privacy and cybersecurity, data protection (including specific concerns around data from Indigenous persons) and the use of generative AI.

As digital health solutions become more widely accepted, there will be increasing pressure on Canada's healthcare systems to determine appropriate reimbursement for these solutions.

Endnotes

1 https://www.statista.com/outlook/hmo/digital-health/canada (accessed January 18, 2025).

2 https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents/pre-market-guidance-machine-learning-enabled-medical-devices.html

3 https://fmrac.ca/wp-content/uploads/2022/07/FMRAC-Framework-on-Virtual-Care.pdf

4 https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight

5 https://www.ic.gc.ca/opic-cipo/cpd/eng/patent/3137161/summary.html

6 https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems

7 https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai

8 https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems

9 https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai

Vanessa Grant is a Senior Partner in our Norton Rose Fulbright Canada Toronto office and advises companies (both large and small) that derive their value from intangible intellectual property and those venture capital and private equity investors that invest in them. She is particularly interested in the convergence of technology and life sciences. She has extensive experience in commercial contracting, investments and mergers and acquisitions in such areas as precision medicine (e.g. AI/ML, computational genomics/bioinformatic, molecular diagnostics and companion diagnostics) and digital health (e.g. mobile apps, clinical decision support, software, imaging diagnostics, etc.).

Norton Rose Fulbright
222 Bay Street, Suite 3000, P.O. Box 53
Toronto, Ontario M5K 1E7
Canada

Tel: +1 416 216 4056
Email: vanessa.grant@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/vanessa-grant-9821449

Véronique Barry's practice covers all aspects of commercial and corporate law, with a particular focus on drafting commercial contracts and on matters relating to life sciences and healthcare. Véronique has gained valuable experience in personalised medicine, clinical trials and other research projects, AI and other innovative technologies, and the use of technology in healthcare. She has also developed a keen interest in access to information and protection of personal information, intellectual property matters, as well as French language and Canada's anti-spam legislation requirements. Over the last few years, Véronique has given several presentations and has published various articles and taken part in drafting law books on these topics.

Norton Rose Fulbright
2828 Boulevard Laurier, Bureau 1500
Québec, Québec G1V 0B9
Canada

Tel: +1 418 640 5170
Email: veronique.barry@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/veronique-barry

Manpreet Singh is a regulatory and privacy lawyer based in Toronto with a focus on the life sciences, food, cosmetics, cannabis, technology and agribusiness sectors. She advises clients on a range of regulatory matters, including supply chain issues, recalls, licensing, advertising, packaging and labelling. She routinely advises on clinical trials, patient support programmes, telemedicine and digital health, including matters relating to healthcare professionals and the delivery of health services across Canada. As part of her privacy and technology practice, Manpreet also advises clients on data governance, AI, cross-border data transfers and the privacy implications of collecting, using and disclosing personal information, particularly in the context of patient services, marketing initiatives, digital health, and data transfers.

Norton Rose Fulbright
222 Bay Street, Suite 3000, P.O. Box 53
Toronto, Ontario M5K 1E7
Canada

Tel: +1 437 352 0948
Email: manpreet.singh@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/manpreet-singh3927

Sarah Pennington is a regulatory and litigation lawyer based in Toronto with a broad and growing intellectual property practice. Sarah advises clients across a range of industries, including those in the pharmaceutical, life sciences, technology, food and beverage, fashion, healthcare, and consumer product sectors. Her practice touches on all facets of intellectual property, including patents, copyright, and trademarks, with a particular focus on disputes and regulatory advice. In her litigation practice, Sarah provides strategic advice and representation to businesses and individuals faced with litigation or potential litigation. Sarah has acted for clients in patent, trademark, and copyright disputes before the Federal Court.

Norton Rose Fulbright
222 Bay Street, Suite 3000, P.O. Box 53
Toronto, Ontario M5K 1E7
Canada

Tel: +1 416 216 4770
Email: sarah.pennington@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/sarahpenningtonip

Norton Rose Fulbright provides a full scope of legal services to the world's preeminent corporations and financial institutions. The global law firm has more than 3,000 lawyers advising clients across more than 50 locations worldwide, including London, Houston, New York, Toronto, Mexico City, Hong Kong, Sydney, and Johannesburg, covering Europe, the United States, Canada, Latin America, Asia, Australia, Africa, and the Middle East. With its global business principles of quality, unity and integrity, Norton Rose Fulbright is recognised for its client service in key industries, including life sciences and healthcare, technology, financial institutions, energy, infrastructure and resources, transport, and consumer markets.

www.nortonrosefulbright.com

NORTON ROSE FULBRIGHT

France

Catherine Mateu

Armengaud Guerlain

Pierre Camadini

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

French law does not provide a global definition of "digital health", either at legislative or regulatory level. Only the concept of "telemedicine" is envisaged by the French Public Health Code, which states that "telemedicine is a form of remote medical practice using information and communication technologies". Teleconsultation, tele-expertise, telemonitoring and telemedical assistance, the purpose of which is to enable a medical professional to provide remote assistance to another healthcare professional during the performance of a procedure, are all considered to be telemedical acts.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Currently, France is expanding on the foundational need for telemedicine as an essential tool in post-pandemic Europe – saving doctors time with administrative tasks, reducing missed appointments and increasing the number of patients cared for. To this end, artificial intelligence (AI) software is being developed to help doctors save time, in particular by automating administrative tasks. "Thiana", for example, takes care of writing medical reports and prescriptions.

1.3 What is the digital health market size for your jurisdiction?

In 2019, the French "health unicorn", Doctolib – the largest digital health service in Europe – raised 150 million euros through funding, raising the company's value to over a billion euros. Recently, research conducted by the Institut Montaigne and McKinsey suggests that the digital health sector has the potential to yield an annual revenue from 16 to 22 billion euros in France.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

The five largest digital health companies in France, as far as we know and subject to evolution, are Doctolib, Santéclair, Qare, Medaviz and Livi.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

The digital healthcare sector is booming, with rapidly evolving rankings, but as far as we know, certain companies dominate the market, such as Doctolib, Dassault Système (in the health division), Cegedim, Cerner France (Oracle subsidiary) and Medtronic (digital health technologies division).

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

In France:

- The French General Directorate of Health is one of the departments of the French Ministry of Health, responsible for preparing and implementing public health policy, health monitoring and health safety.
- The National Health Authority (HAS) aims to develop quality in the health, social and medico-social fields. It works alongside public authorities, whose decisions it informs, and with professionals to optimise their practices and organisations.
- The National Agency for the Safety of Medicines and Health Products (ANSM) is the public body that provides access to healthcare products (medicines and medical devices (MDs)) in France and ensures their safety throughout their life cycle via authorisation procedures.
- The Data Protection National Commission (CNIL) is responsible for ensuring the protection of personal data contained in computer files and processing, whether public or private.
- The Digital Health National Agency (ANS) sets out frameworks and best practices to facilitate the sharing and exchange of healthcare data (general security policy for healthcare information systems, guidelines, cybersecurity support and healthcare data).

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

In France, these authorities regulate various aspects of digital

health such as approval of MDs, AI and combination products (via CE marking and validation procedures), data compliance (especially personal data protection through the GDPR), as well as data security and cybersecurity. Rules against anti-competitive practices are also applied.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

Digital health legislation focuses on the protection of personal health data, telemedicine oversight, cybersecurity of healthcare platforms and the regulation of connected MDs. It also applies to emerging technological fields such as AI, blockchain, public e-health and mobile health applications, aiming to ensure accessibility and quality of care.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

If a software product qualifies as a medical device, it must comply with commercialisation and monitoring requirements under EU Regulation 2017/745 (MDR) or Regulation (EU) 2017/746 on *in vitro* diagnostic MDs and in France specifically, by the French Public Health Code. These regulations also apply to devices with no medical purpose and include cybersecurity as a new essential requirement.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

In 2024, the EU passed Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on AI, referred to as the AI Act.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Regulations are becoming more flexible, with regular updates to incorporate emerging technologies. The EU has specific AI regulations in place, including transparency and explainability requirements, and France is following these directives while developing harmonisation approaches for the digital marketplace.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation data are crucial for AI/ML-based health solutions. These data are used to demonstrate the efficacy and safety of products before market entry. ANSM requires clinical evidence to assess the risks and benefits of digital health devices. Additionally, MDR regulations mandate clinical trials for high-risk devices.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Digital health products are regulated both by the State (via ANSM) and through European regulations (via MDR/IVDR). There are some differences at regional and national levels, particularly in terms of innovation support and specific requirements for certain product categories. However, France follows a unified approach at the national level while aligning with EU practices.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Regulatory enforcement in France is tailored to the specific characteristics of digital health products. For example, ANSM and CNIL work together to ensure compliance with both safety standards and data privacy regulations (GDPR). Enforcement actions also focus on post-market surveillance and traceability to ensure continued compliance.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Telemedicine, including teleconsultation, tele-expertise and remote assistance, requires minimal legal protection for patients' personal information. Platforms must ensure data security and the competence of doctors while complying with applicable laws.
- **Robotics**
  Robotics raises issues related to product responsibility and legal regulation to ensure the robots' capabilities and liability. The question of financial compensation for patients harmed by robotic medical errors remains inadequately addressed.
- **Wearables**
  Wearables such as smartwatches, fitness trackers and smart technology clothing are used to detect the health and wellness of people.
  However, by providing personal health information on their users, this digital health technology gives rise to legal issues such as data privacy, security and compliance with MD regulations.
- **Virtual Assistants (e.g. Alexa)**
  Virtual assistants can help nurses schedule visits or remind patients to take their prescriptions. However, at the same time, they also bring about issues such as legal liability and invasion of privacy if the personal health information is leaked out, and other legal risks.
- **Mobile Apps**
  Mobile apps are a tool for telemedicine and help patients access medical consults in a more effective way at anytime and anywhere in the world. However, the apps' liability and the protection of patients' information are to be taken into consideration.
- **Software as a Medical Device**
  Assigning responsibility in the event of a chain of liability is an important issue. Typically, the regulation on MDs

and the provisions protecting health data apply. Social and public health issues related to the development of new devices will need to be addressed, and will probably be partly addressed in the forthcoming regulation on AI.

- **Clinical Decision Support Software**
  As far as legal issues about clinical decision support software are concerned, a few provisions can apply: the MDR to ensure compliance with the French regulations for MDs; the GDPR for personal data protection; and ethical considerations to ensure ethical principles during the decision-making phase.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  Data protection, MD regulation and ethical principles are always the key issues when AI technology or a machine process with a great number of personal data provide solutions based on an algorithm. Inevitably, to avoid any litigation, it is necessary to have an individual's consent when an AI or machine processes their information.
- **IoT (Internet of Things) and Connected Devices**
  Apart from legal issues such as data protection, product liability and user consent, which are mentioned above, cybersecurity is also to be taken into consideration and must be compliant when the connected devices are put into use.
- **3D Printing/Bioprinting**
  3D printing or bioprinting involves several legal issues and must comply with MD regulation, GDPR for data protection, ethical principles (since human organs may be reproduced by a printer) and product safety provisions.
- **Digital Therapeutics**
  Concerning digital therapeutics, data protection, ethical considerations, user consent and MD regulation, and the issue of liability in case a wrong treatment occurs are key issues.
- **Digital Diagnostics**
  As mentioned above, there are always legal issues such as MD regulation, data protection, user's consent and liability of digital diagnostics results to comply with. The regulation measures should also be taken to ensure that the collected data and used patients' data are not abused.
- **Electronic Medical Record Management Solutions**
  As mentioned above, data protection, preventing abuse of patients' information, users' consent and liability are the key issues. It is necessary to inform patients of the use, preservation and destruction of their information after a certain period of time.
- **Big Data Analytics**
  Data protection (GDPR), preventing abuse of collected data, consent of users (use of their data or information during a specified period then destruction) and the issue of liability. It is also necessary to strengthen the protection measures of personal information to prevent it from leaking.
- **Blockchain-based Healthcare Data Sharing Solutions**
  The user's consent is the most important thing. Making sure that the data is shared with a credible partner to avoid any abuse or leaking of data, especially as there may be some very sensitive information that are strictly personal. Liability and data protection are also legal issues.
- **Natural Language Processing**
  Personal data protection with GDPR and user's consent are key issues. Compliance with specific regulations or guidelines issued by authorities such as the CNIL and ethical considerations are also mandatory.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Ensuring that everything on the platform is legal, there is no misleading information, no information against public order and good morals. Security measures are to be taken to prevent privacy information invasion, misuses or leaking of personal data.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Ensuring that personal data is perfectly protected and could not be easily leaked nor consulted by the public, and that consent is provided by the concerned individuals for the use of any personal data. In this area, the GDPR applies and apart from that, there are a few regulatory requirements such as the Data Protection Act (DPA, *Loi Informatique et Libertés*), other specific regulations or guidelines by the authority CNIL and the Telecoms and Electronic Communications Code.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In France and Europe, health data is regulated by the GDPR, which sets strict rules. France also has complementary laws like the French DPA, and regulation is centralised at the national level, although regional authorities may intervene in specific cases.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The GDPR allows some derogations in certain situations. However, it applies regardless of the nature of the entities involved.

4.4 How do the regulations define the scope of personal health data use?

The regulation especially defines the lawful practice of collection of data, the illegal use of collected data, and sanctions, in order to ensure that the collection is not used for the collector's own interest only, or illegally.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

To ensure comprehensive rights regarding the use and collection of personal health data, key considerations include user consent, data usage aligned with contractual purposes, security measures to prevent misuse, a limited duration for data

retention, and the individual's right to legal action in case of contractual breaches by the platform or organisation.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Transparency requirements, under the GDPR and the newly adopted AI Act, aim to address data inaccuracy, bias and discrimination by requiring data controllers to inform individuals about automated decision-making and its foreseeable consequences. The AI Act also prohibits AI systems that rank people's trustworthiness based on their social behaviour or personal traits, which could result in harmful treatment.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

In France, the collection and use of personal health data are governed by the GDPR, overseen by the CNIL, and complemented by the "*Informatique et Libertés*" law. Specific frameworks like the shared medical record (DMP) and the "*Ma Santé 2022*" law regulate the digitalisation of healthcare while ensuring personal data protection.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Key legal and regulatory issues when sharing health data in France include compliance with the GDPR, which sets strict conditions for the processing of personal data. The French DPA complements the GDPR with specific rules for health data. Other laws, such as public health laws and data security regulations, may also apply. Additionally, considerations related to cybersecurity and the confidentiality of personal data are important, regardless of the technology sector.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

There are no significant differences in regulation at the national and European levels, as rules are harmonised. However, national authorities may intervene in specific cases, especially regarding data security or compliance in certain public sectors.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

The nature of the entities involved rarely matters. Most of the time the same provisions apply, whether the entities are public or private. The nature of the data is more important, since specific requirements can apply to medical data, as mentioned above.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

The European Health Data Space (EHDS), created in 2022, aims to provide a secure and efficient framework for the use of health data through common rules and standards. In France, the Health Data Hub, launched in 2019, facilitates the sharing of healthcare data and promotes standardised norms for their use.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

When it comes to federated models of healthcare data sharing, it is essential to inform patients and to facilitate the exercise of their rights. It is also essential to ensure data protection as well as data interoperability, especially for research and innovation. In that respect, the elaboration of standards and repositories can be very useful.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Contrary to what one might believe, exclusions from patentability are not an insurmountable obstacle to the patentability of e-health innovations.

If diagnosis methods are unpatentable *per se* in European law, this exclusion does not apply to the devices implementing these methods. Therefore, MDs or recording media are substantially patentable. Consequently, when it comes to connected health, the device itself can be protected, such as a wearable that measures blood flow and uses the data to diagnose cardiovascular problems.

Likewise, even though mathematical methods and computer programs are unpatentable as such, a computer program is patentable if it produces an additional technical effect (beyond the normal physical interactions between the program and the computer). In other words, a software controlling a dialysis machine or processing physiological data from sensors can be patented.

Finally, inventions incorporating AI can benefit from patent protection under certain conditions: their designated inventor must not be an AI system; their description must be sufficient; and their finality must be technical (concrete).

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Only original works in a fixed form can benefit from copyright protection. As concerns digital health, the design and multimedia elements of a device can be protected, as well as the expression of a software (their code and preparatory design material can be protected).

Regarding data, copyright can easily protect databases structures, not their content. Indeed, copyright protection of the data itself, which is at the heart of the valuation of e-health companies, is anything but obvious: raw data cannot be protected and processed data can be protected by copyright only if it is original, more precisely if it reflects free and

creative choices. Besides, open data and open source may also limit copyright protection as connected health companies use a lot of open-source building blocks to develop their solutions. Indeed, improvements made from open-source software are generally subject to the conditions of a free licence, which implies a loss of value of the technology.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Raw or processed data, as well as databases, can be protected by trade secrets. E-health companies can therefore benefit from protection on the corpus of learning data used in their AI systems. Trade secrets may also protect algorithms, code, processes, parameters, etc. However, in those cases, trade secrets are more difficult to defend and promote; for example, it is not possible to prohibit a competitor from independently producing the same AI system.

To benefit from trade secret protection on data, whatever its nature, digital health companies must ensure that it meets three conditions: (1) it must be secret, that is to say confidential; (2) it must be subject to reasonable protective measures to maintain its secret nature; and (3) it must have commercial value. This last condition can be an obstacle, as in e-health innovations, the value results more from the combination of data than from the isolated data. In such cases, a contract controlling data access and use can be a complementary protection tool.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

In 2014, the European Commission enacted Regulation (EU) No. 316/2014. This regulation aims to guarantee that that technology transfer agreements respect competition rules. Its provisions create a safe harbour for most licensing agreements by providing guidelines and creating a so-called "block exemption" regulation. Besides this regulation, there are no specific rules applying to academic technology transfers in France.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

As mentioned above, a software as a MD can be protected and is patentable if it produces an additional technical effect. Patents offer strong protection but are limited in time (20 years). It is also important to note that this protection requires public disclosure of the invention as patent applications are published 18 months after being filed.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

According to EU law, an AI device cannot be named as an inventor of a patent according to EU law. In 2022, the Legal Board of Appeal of the European Patent Office (EPO) issued a decision in case J8/20, which confirmed that under the European Patent Convention the inventor designated in a patent application cannot be an AI machine. It can only be a human being with legal capacity, as a machine cannot defend and/or transfer any rights.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

Beyond any rules or laws, it is the specific contract executed between the inventor and the government sponsor that determines intellectual property rights allocation. This is why public authorities must be careful and ensure that the contract enables them to use the products they ordered as they want to. For this reason, standard intellectual property provisions, adapted to the different public contracts, are made available by the government.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

In a renowned case, T 844/18, concerning a patent related to CRISPR-Cas9 technology (genetic scissors), the EPO had revoked the patent in question because the original applicants were not identical to those wishing to claim the right of priority. Recently, the EPO has softened its stance and now acknowledged that there is a rebuttable presumption that the applicant is entitled to claim priority (EPO Grand Chamber decisions, 10 October 2023, G1/22 and G2/22).

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

When dealing with collaborative improvements, parties should define a clear plan regarding the potential commercial results of their partnership, especially respecting intellectual property rights and their allocation to each party. For instance, joint ownership of results should be provided for when relevant.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

As the healthcare industry is a highly regulated sector, parties must ensure regulatory compliance and guarantee continuity and traceability throughout the production and/or distribution.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

As personal data transfers are highly regulated, parties must implement adequate security measures during transmission. They should also investigate possible data breaches and agree on the correlative financial compensation.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Parties must make sure that the generative AI system presents sufficient guarantees in order to maintain control of the liability risks linked to its use. For instance, they could ask for the implementation of measures limiting the risks of violation of third-party rights via content filters or abuse detection mechanisms. More generally, parties must ensure that the supplier is able to offer a solid guarantee on possible third-party recourse in matters of intellectual property. Likewise, parties must ensure that the supplier does not provide in its contract for an assignment or licence on the content generated for its benefit, as this would likely hinder the free disposal of this content.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

In France, the main authorities are the CNIL, the Competition Authority and the *Autorité des Marchés Financiers* (AMF). The CNIL oversees data protection, the Competition Authority monitors anticompetitive practices, and the AMF regulates AI applications in financial markets.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

In France, key AI/ML regulations are governed by European frameworks such as the GDPR, overseen by the CNIL for data protection, and the Trust in Digital Economy Law (LCEN). For AI in healthcare, regulation is primarily through the Medical Devices Directive and the MDR, supervised by the ANSM.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

The author automatically owns the rights to such algorithms. However, if the author is an employee who acted within his duties or under instructions, his employer and/or company may acquire his rights.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

In France, licensing data for AI/ML requires compliance with the GDPR, ensuring consent, data security and transparency. Contracts should define the scope, duration and liability for data misuse. When licensing healthcare data, stricter conditions apply due to its sensitive nature under Article 9 of the GDPR and specific public health laws, requiring enhanced data protection and safeguards against misuse or discrimination.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

In France, regulatory bodies such as the CNIL and the European Commission differentiate standard AI from generative AI based on their functionality and potential risks. While standard AI typically involves data analysis and decision-making, generative AI creates new content. The EU AI Act places stricter regulations on high-risk AI systems, which include generative AI, due to the increased risks of bias, misinformation and misuse.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Generative AI technologies raise specific issues regarding intellectual property, data protection and liability. In France, the lack of clear legislation on AI-generated works creates challenges regarding copyright. The GDPR regulates data use, while AI liability remains unclear. At the European level, the AI Act aims to establish a legal framework for regulating risks, and in France, the National AI Strategy and institutions like the National Institute for Research in Digital Science and Technology (INRIA) are developing relevant standards and regulations.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

In France, the use of data in AI/ML models is primarily governed by GDPR, which requires data controllers to ensure that the data used in their AI/ML models is legally sourced and that the appropriate data rights are respected. If these obligations are not met, the data controller can be held liable and face administrative penalties, including fines of up to 20 million euros or 4% of global annual turnover. While France does not have specific data disgorgement laws, the control and sanction mechanisms under the GDPR, along with the transparency and accountability requirements, ensure that data is processed in compliance with European law.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Regulatory, civil and criminal theories of liability can apply to adverse outcomes in digital health solutions, depending on the case.

Regulatory liability often applies, as manufacturers failing to meet requirements can be sentenced to administrative sanction by regulatory authorities.

Civil liability also frequently applies, as manufacturers or distributors are liable for provisioning defective products in case of harm to the users.

More rarely, criminal liability applies, as manufacturers, distributors and other actors are held liable for ordinary offences or specific offences described in the French Public Healthcare Code.

9.2 What cross-border considerations are there?

E-health companies must consider the cross-border healthcare issue, especially if they wish to operate internationally within the EU. There are indeed specific conditions under which a patient may receive medical care from an HCP located in another EU country. Companies must therefore comply with the rules regarding the prescription, and the delivery of medications and MDs, as well as the healthcare costs. Likewise, companies should ensure their capacity to transfer data in compliance with the rules of the EHDS.

On top of this, non-EU companies should consider the specific rules applying to them. For instance, non-EU manufacturers must designate an authorised representative within the EU if they want to place one of their MDs on the EU market.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Implementing staff awareness measures and internal procedures can help minimise those risks. It is therefore important to monitor internal uses and to implement preventive measures. Training actions for staff should be carried out and a general use policy should be adopted. This policy could specify the basic points of vigilance.

Besides, evaluating the practices and guarantees applied by the AI suppliers is essential in controlling liability risks. The existence of sufficient technical and contractual guarantees must indeed be ensured.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

In French law, misuse of health data in AI/ML models may lead to a GDPR violation, particularly regarding unauthorised processing of sensitive data (Article 9) or failure to ensure security (Article 32). Civil liability could also arise from medical malpractice if AI causes harm to a patient. Additionally, sanctions may apply for non-compliance with future AI regulations in healthcare.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based services for digital health must comply with the GDPR and guarantee ethical governance and sufficient security. They also have to enhance data assets and facilitate efficient data exchanges, in particular by promoting data interoperability. The key challenge is thus to find a point of balance between data sharing and protection of patient privacy.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Before entering today's digital healthcare market, non-healthcare companies should study the specificities of the sector, as it is a very complex industry. They should also review the applicable regulations, since compliance with the French and European norms is crucial.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Venture capital and private equity firms should study the market carefully before investing in digital healthcare projects. They should especially pay attention to the market needs and requests, to provide adequate and useful services.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

One of the key barriers in France is the lack of a comprehensive regulation with a body of dedicated norms. Other important barriers are the long and complex methodologies used regarding the assessment and reimbursement of medical health technologies. Although, the efficiency of these processes may improve in the future.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In addition to the HAS (certifying), the ANS (public but non-certifying) influences the clinical adoption of digital health solutions. Besides, professional associations such as the SNITEM (*Syndicat National de l'Industrie des Technologies Médicales*) or the APIDIM (*Association pour la Promotion des Dispositifs Médicaux*) also encourage the certification of such solutions.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

In France, digital health solutions can be reimbursed under the "Health Innovation" reimbursement model, which includes telemedicine, remote patient monitoring and certain digital health apps. The government provides reimbursement through the French Social Security system, under specific conditions. To be eligible for reimbursement, digital health solutions must be certified as MDs by the ANSM and registered on the National Digital Health Platform. Additionally, these solutions must demonstrate clinical effectiveness and be approved by the French National Authority for Health.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Due diligence gaps for digital health solutions, particularly AI/ML-based, include algorithm transparency, data quality (especially GDPR compliance) and clinical validity. Legal liability is unclear, and interoperability with existing systems and data security (regulated by ANSSI) remain key concerns.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

The pandemic has shown that innovation, alongside research and industry players, is key to bring out the best solutions for patients. Consequently, digital health actors are currently forming academic and industrial partnerships and developing new tools and practices, especially with the progress of AI. Legislators will certainly produce new norms to regulate these innovative strategies.

Catherine Mateu was admitted to the Paris Bar in 1999 and has over 15 years of experience in French and European intellectual property law. Defending the interests of all types of companies, her strategic analysis, litigation and contract practice encompass all intellectual property and related rights law.
A recognised expert, Catherine Mateu's work is regularly cited by *Who's Who Legal*, *Managing Intellectual Property*, *IP Stars*, *Chambers*, *The Legal 500*, *Décideurs*, *Women in Business Law*, etc.
Fluent in English and bilingual in French and Spanish, Catherine Mateu has developed extensive international expertise.

Armengaud Guerlain
12 Avenue Victor Hugo
75116, Paris
France

Tel: +33 1 47 54 01 48
Email: c.mateu@armengaud-guerlain.com
LinkedIn: www.linkedin.com/in/catherine-mateu-40330812

Pierre Camadini practises in all areas of intellectual property, providing legal advice and carrying litigation in trademarks, patents, copyrights and designs rights. Fluent in English, he regularly works for foreign clients on international cases.
Pierre previously worked in law firms specialised in intellectual property law, in France and abroad, and at the 3rd Civil Chamber of the Paris Judicial Court.
He holds a degree in Law from the Aix-en-Provence University, as well as a Master's degree in industrial and artistic property from the Paris I Panthéon-Sorbonne University. Pierre also holds a degree in comparative law from the Chongqing Southwest University of Political Science and Law in China.

Armengaud Guerlain
12 Avenue Victor Hugo
75116, Paris
France

Tel: +33 1 47 54 01 48
Email: p.camadini@armengaud-guerlain.com
LinkedIn: www.linkedin.com/in/pierre-camadini-191b05149

Germany


Jana Grieb


Steffen Woitz


Dr. Claus Färber


Dr. Christian Lebrecht

McDermott Will & Emery Rechtsanwälte Steuerberater LLP

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

German law does not define "digital health" specifically. Generally, the term is interpreted broadly and includes, *inter alia*: (i) digital healthcare services, including telemedicine; (ii) medical software applications for smartphones; (iii) medical devices that include artificial intelligence ("AI"); and (iv) other medical products that involve digital features, such as digital pills. Moreover, digital health is an umbrella term for the new markets in which the providers of the aforementioned products and services are active. Similar to "e-health", the term is symbolic of the rapidly advancing digitisation of the German healthcare sector.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Prescription and reimbursement of medical apps: In 2021, a new system for the reimbursement of medical smartphone apps (*Digitale Gesundheitsanwendungen* – "DiGA") has been introduced under the statutory health insurance ("SHI"). The DiGA concept originally applied to apps that are CE-certified medical devices under the Regulation (EU) 2017/745 on medical devices ("MDR") risk class I or IIa. In 2024, class IIb medical devices were added to the DiGA system. DiGA can be prescribed by physicians and psychotherapists and are then reimbursed by SHI funds. In order to obtain reimbursement for a medical app, the manufacturer must file an application with the German Federal Institute for Drugs and Medical Devices (*Bundesinstitut für Arzneimittel und Medizinprodukte* – "BfArM"). Once approved, the applicable reimbursement thresholds are determined by and negotiated with the Federal Association of the SHI Funds (*Spitzenverband Bund der Krankenkassen* – "SpiBu").

To obtain approval for reimbursement, the manufacturer must prove that the medical app meets the requirements for safety, functional capability and quality and that it complies with data protection requirements. Additionally, the manufacturer must show that the app has positive effects in patient care.

At present, BfArM has approved 65 medical apps. Twenty of these medical apps have obtained temporary approval subject to further proof of positive healthcare effects.

In March 2024, the Digital Act (*Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens*) came into force. It aims at integrating DiGA further into the process of care and enhancing transparency. With the inclusion of class IIb medical devices, it will become possible to use DiGA in more complex treatment schemes such as telemonitoring.

Similar to the DiGA concept, a new system for the reimbursement of digital care applications (*Digitale Pflegeanwendungen* – "DiPA") was introduced in December 2022 under the statutory and private long-term care insurance regime (*Pflegeversicherung*). DiPA are intended to provide support to care recipients at home and designed to help alleviate the care recipient's loss of independence or capabilities or prevent their need for care from progressing further. Reimbursement is obtained under the same procedure that applies to DiGA.

Liberalisation of telemedicine: For many decades, telemedicine was largely restricted under German physicians' professional law. This had already started to change before the COVID-19 pandemic. In 2019, Germany set the legal basis for telemedicine, including video consultation by physicians, and their coverage by private and public payers.

Telemedicine is still subject to numerous regulatory restrictions. According to German professional laws, remote treatment can only take place if, among other things, the use of the telecommunication medium is medically justifiable, i.e. no further medical examinations are necessary to obtain a direct and comprehensive picture of the patient and his or her disease. Moreover, telemedicine business models are subject to high data protection and IT security standards, as they involve the processing of a significant amount of health data.

Electronic patient record: Since January 2021, Germany has been in the process of implementing the so-called electronic patient record (*elektronische Patientenakte* – "ePA"). The ePA is a central element of digital and networked healthcare. From 2025, the ePa will become available gradually to all SHI-insured patients in Germany. After a trial phase in model regions, the ePa is supposed to become available throughout Germany. Functions will also become available in stages, with medication lists and diagnostic reports becoming available in the first half of 2025, while at a later stage, the ePa is expected to include medication plans and lab reports.

1.3 What is the digital health market size for your jurisdiction?

The market for digital products and services in the healthcare sector is growing rapidly. There are various estimates on the market size, depending on the notion of digital health (as outlined under question 1.1 above) and the relevant key figures. The size of the market is already estimated today to be in the tens of billions, with a strong upward trend.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

It is not possible to make a blanket statement in this regard. Many of the companies specialising in digital health are also active in other health or technology markets. As in other countries, the global tech companies such as Apple, Google or IBM play a significant role in the digital health market. At the same time, university spin offs and other early stage companies are making their mark in this emerging sector as well. In the telemedicine sector, there are a number of promising platform operators that use their e-commerce and IT expertise to connect patients and physicians online.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Germany's digital health sector has witnessed significant growth in the last few years, with companies like Climedo Health, Noventi Health SE, Dyrad Networks GmbH and Avi Medical making notable strides.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The BfArM regulates the market clearance and reimbursement for most digital health products. Market surveillance for medical devices, including medical apps, is carried out by supervisory authorities at a regional level.

The SpiBu and the Federal Assembly of the SHI and the Federal Panel Doctors' Association (*Gemeinsamer Bundesausschuss*) are the highest bodies of the SHI and are involved in the majority of reimbursement decisions for digital health products and services.

Federal and Regional Data Protection Commissioners (*Datenschutzbeauftragte des Bundes und der Länder*) are responsible for the supervision of data protection efforts.

The Telematics Society (*Gesellschaft für Telematik*) was created specifically with regard to the task of developing a suitable and functioning healthcare telematics infrastructure, including an electronic patient health card, electronic patient files and e-prescriptions.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

Digital health products, including medical apps, often qualify as medical devices or *in vitro* diagnostics and, therefore, fall within the scope of the MDR and Regulation (EU) 2017/746 on *in vitro* diagnostics ("IVDR"). As EU regulations, the MDR and IVDR are directly applicable in Germany and do not have to be transposed into national law. The regulations are complemented by the German Act on the Implementation of EU Medical Devices Law (*Medizinprodukte-Durchführungsgesetz*).

Digital health services are subject to German healthcare regulations on the inpatient sector (e.g., hospitals and care homes) and outpatient sector (e.g., medical offices and home care providers). In these sectors, services are typically reserved for physicians or other healthcare professionals ("HCPs") who may be entitled to provide healthcare services. Physicians are subject to the requirement of a German approbation or other permit to provide physician-only services, and bound by strict regulations under their professional codes.

Reimbursement of digital health products and services under the SHI regime is predominantly governed by the Fifth Book of the Social Insurance Code (*Fünftes Buch Sozialgesetzbuch* – "SGB V").

The laws on data privacy, in particular the GDPR and the German Federal Data Protection Act (*Bundesdatenschutzgesetz* – "BDSG"), are particularly relevant to digital health products and services. It is key for any digital health company to ensure that patient data are treated in line with these legal frameworks and protected against undue third-party access. Furthermore, depending on the respective health product or service, additional data protection regulations may apply, e.g., for the approval of medical apps or telemedicine services.

In Germany, the cooperation between the health industry and HCPs is subject to various healthcare compliance regulations. Their purpose is to protect independent medical decisions of HCPs, patient health and fair competition among healthcare providers. To this end, the regime in particular seeks to prevent any undue influence on HCPs. The applicable healthcare compliance provisions are manifold and complex. They equally apply to any cooperation and business activities in the digital health sector.

On 1 August 2024, the Regulation (EU) 2024/1689 (the "AI Act") entered into force. As an EU regulation, it is directly applicable in Germany. The AI Act provides additional requirements for medical applications that include or are AI systems.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The key areas of enforcement for digital health are still the compliance of products that constitute medical device software ("MDSW") with the sector-specific laws and regulations and the compliance of any digital health services with the laws on the provision and reimbursement of physician services, as well as pharmacy laws and restrictions that are relevant to digital health applications and websites that offer medicinal products.

Where digital health products or services require the transfer and processing of personal health data, data protection authorities supervise the market as well. Failure to meet data protection requirements may result in severe sanctions, such as an injunction to stop the processing, and/or fines of up to EUR 20 million or 4 per cent of the total worldwide annual turnover, which can be publicly issued.

In future, the enforcement of the AI Act will become relevant. According to Article 70 AI Act, Member States have to appoint competent authorities by August 2025. In Germany, the Federal Ministry of Economics and Climate Protection and the Federal Ministry of Justice are jointly responsible for implementing the AI Act. The competent authorities for Germany have not been determined to date. While some areas of enforcement are presumed to lie with data protection authorities, others will likely be supervised by the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – "BSI").

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

MDSW is regulated under the MDR or IVDR, under which it must be certified as conforming to safety and other requirements before being placed on the market. To obtain a CE-mark in accordance with the MDR or IVDR, MDSW must undergo a conformity assessment procedure that, depending on the risk class, can be passed through by the manufacturer (self-certification) or requires the involvement of a notified body. Upon successful completion of the conformity assessment procedure, the CE-mark can be affixed to the MDSW product.

Before the MDR came into force, MDSW was generally classified under risk class I and subject to self-certification under the Medical Device Directive 93/42/EEC ("MDD"). Under the MDR, many MDSW are now subject to higher risk classes. Therefore, manufacturers must regularly obtain their CE certificates from notified bodies.

The transition scheme under the MDR allows for manufacturers of class I MDSW to benefit from a grace period. Initially, the transition periods were set to expire in May 2024. However, the European Commission acknowledged by the end of 2022 a significant threat to the availability of medical devices in the EU and thus extended transition periods with Regulation (EU) 2023/607. Under the new transition scheme, manufacturers of up-classified former class I MDSW may continue to market their products under the previous MDD regime until 2028. For MDSW in higher risk classes, transition periods vary according to the risk class. To benefit from the extended transition periods, manufacturers must have initiated measures to comply with the MDR before the expiry of the original transition period. In particular, manufacturers must by then have implemented a quality management system in accordance with the MDR and lodged a formal application for conformity assessment with a notified body. A written agreement among manufacturer and notified body must be signed by September 2024.

The Medical Devices Coordination Group of the European Commission issued several guidelines on qualification and classification of MDSW.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Germany has not enacted a specific law on AI or machine learning ("ML") so far. Products that include AI/ML are subject to the same regulations as other products, including medical devices law and data protection, as well as cybersecurity regulations. As part of a medical device, AI/ML software must comply with the requirements of the MDR or IVDR.

However, as the AI Act is directly applicable in Germany, the regulatory requirements under the AI Act apply even without implementing laws. The requirements under the AI Act depend on the risk the AI systems present in the specific use case. According to Article 70 AI Act, there will be three types of competent authorities in the Member States under the AI Act: the Market Surveillance Authority; the Notifying Authority; and the National Public Authority. These authorities have yet to be named in Germany.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Notified bodies will in future have to adapt their review of medical devices to reflect the dynamic nature of AI/ML to a certain extent. Guidance comparable to the US FDA AI/ML discussion paper is not yet available. Applicable standards such as EN/IEC 62304 and EN/IEC 82304-1 provide a framework for software lifecycle development including device architecture and detailed design.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Where AI/ML systems are medical devices, the MDR requires rigorous clinical evaluation that includes validation data. Clinical validation data also informs the design of post-market surveillance plans, which monitor the AI/ML system's performance in real-world scenarios after deployment.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

While such products are predominantly regulated on EU and national levels, there are certain state level laws, such as laws on data protection, that affect digital health products.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Besides overseeing compliance with the EU MDR, GDPR and now the AI Act, German regulators are increasingly scrutinising cybersecurity practices in digital health products to safeguard patient data and system integrity.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Despite being liberalised to a substantial extent (see question 1.2 above), telemedicine and virtual care services are still considerably restricted. Remote treatment of patients must be medically justifiable, i.e. the treatment case may not require further medical examination in the doctor's practice.
- **Robotics**
  Robotics are machines that have the capacity to (partly) substitute HCPs. Such machines will mostly qualify as medical devices (see question 2.6).
- **Wearables**
  Wearables, such as smartwatches or smartglasses, often serve multiple purposes, and their primary purpose may

not even be of a medical nature. However, if wearables come with health-related features, they might qualify as medical devices and require CE-certification.

- **Virtual Assistants (e.g. Alexa)**
  Virtual assistants (such as Amazon's Alexa, Microsoft's Cortana, or Apple's Siri) usually have not been designed with health-specific features and are thus not considered medical devices.
- **Mobile Apps**
  Mobile apps that implement health-related features may be considered MDSW and, thus, may require CE-certification. Medical apps of MDR risk class I or IIa may be approved for reimbursement (see question 1.2 above).
- **Software as a Medical Device**
  As with mobile apps, other software that implement health-related features may equally qualify as MDSW (see above).
- **Clinical Decision Support Software**
  As with other software that implements health-related features, clinical decision support software may qualify as MDSW (see above).
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  Digital health solutions powered by AI and ML can be a powerful tool for medical diagnostics and monitoring. The training of neural networks and similar AI/ML algorithms necessarily requires a large amount of personal health data that must be obtained in compliance with data protection laws. At the same time, the results are often not sufficiently protected by intellectual property rights (see question 8.3).
- **IoT (Internet of Things) and Connected Devices**
  Connected medical devices such as long-term EKG or blood pressure metres are subject to the MDR and thus require CE-certification.
- **3D Printing/Bioprinting**
  3D printing and bioprinting can be used to manufacture prosthetics and tissues. In the future, this technology might even be used to create whole organs. The use of 3D templates for prosthetics and tissues also raises new intellectual property and licensing questions.
- **Digital Therapeutics**
  Digital therapeutics are treatment procedures based on digital technologies. Such technologies may, depending on their specific features, qualify as MDSW (see above).
- **Digital Diagnostics**
  The same applies to diagnostic procedures based on digital technologies. These technologies may, depending on their specific features, qualify as MDSW (see above).
- **Electronic Medical Record Management Solutions**
  Electronic medical record management solutions have been used for decades as stand-alone systems. With the implementation of the e-health/telematic infrastructure currently launched by the German Federal Government, healthcare providers who treat patients insured under the SHI must adapt and connect their practice management software.
- **Big Data Analytics**
  Big data are key to successful research and development in the life sciences sector. A major challenge is to collect, use and commercialise large amounts of health data in compliance with the GDPR, either through anonymisation or based on consent of the relevant data subjects.
- **Blockchain-based Healthcare Data Sharing Solutions**
  The current Federal Government's e-health/telematic infrastructure is not based on blockchain technology but on a more traditional public-key scheme. Furthermore, the use of public or semi-public blockchains for digital health is a no-go because on that basis, it would not be possible to adequately protect health data.
- **Natural Language Processing**
  Natural Language Processing ("NLP") describes techniques and methods for automatic analysis and representation of human speech. NLP is, *inter alia*, used in pharmaceutical research. If used for digital health, the confidentiality of spoken text needs to be preserved under data protection and professional secrecy laws.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Platforms that facilitate transactions between healthcare providers and patients are subject to the requirements of Regulation (EU) 2019/1150 (Platform-to-Business Regulation), which sets out minimum standards for terms and conditions, transparency and fairness. Furthermore, large health platforms could in the future reach the thresholds for a designation as a gatekeeper under Regulation (EU) 2022/1925 (Digital Markets Act). As such platforms do not qualify as licensed healthcare providers, they are not authorised to process health data under Article 9(2)(h) of the GDPR but will often need to obtain valid consent from end-users.

Increased data security requirements for health data means that they cannot rely on unencrypted e-mail but need to establish a more secure channel with patients.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The use of personal data is governed by the GDPR. Health data qualifies as a special category of personal data; its collection and further processing is generally prohibited unless a special exemption applies (Article 9 of the GDPR).

In addition to the requirements of the GDPR, the unauthorised disclosure of personal secrets of patients by HCPs and their auxiliaries is subject to criminal liability under Sections 203 and 204 of the German Criminal Code (*Strafgesetzbuch*).

For connected medical devices and other equipment, the Telecommunication-Digital Services Data Protection Act (*Telekommunikation-Digitale-Dienste-Datenschutzgesetz*), which transposes certain parts of Directive 2002/58/EC, imposes additional restrictions on remote access to data, even if it is not personal data.

The EU Data Act (Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data) will apply from 12 September 2025 and cover digital health products and services. It will require the vendors to make available both personal data and non-personal data to the user and third parties requested by the user. Additional design requirements for connected (medical) devices will apply one year later, from 12 September 2026.

Under the GDPR, every entity responsible for the processing of personal data (data controller) is subject to transparency and documentation obligations. In particular, the data controller must:

- inform the individuals (data subjects) how their data is processed;
- maintain a record of processing activities; and
- conduct data protection impact assessments ("DPIA") and possibly consult with the competent authority prior to certain risky types of data processing – this will often apply to digital health applications that involve sensitive health data and new technologies.

Under the BDSG, an entity is required to appoint a data protection officer ("DPO") if it employs 20 or more persons with the processing of personal data, or if it needs to conduct a DPIA. Hence, digital HCPs in Germany will usually require a DPO.

HCPs are also required to take additional measures to ensure that their staff and service providers are warned of their potential criminal liability and thus maintain confidentiality. Furthermore, HCPs that are medium-sized enterprises or bigger must comply with the requirements of the Directive (EU) 2022/2555 (NIS 2 Directive) once it has been transposed into German law (as of January 2025, Germany is still in the process of doing so).

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

While the GDPR and federal laws apply throughout Germany, different state laws apply to the processing of personal health data by public healthcare providers operated by the State or by local authorities. These vary in the exact requirements and security standards for the processing of personal health data by these entities, and whether and under which conditions they allow engaging a data processor outside the EU/EEA.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The GDPR sets out different requirements for health data, depending on the nature of the entities involved and the purposes for which personal data is processed.

Licensed HCPs are permitted to process special categories of personal data for the purpose of occupational and preventive medicine, diagnosis and treatment (Article 9(2)(h) of the GDPR). This covers laboratories and other HCPs that cooperate with physicians, as well as medical and non-medical service providers acting on behalf of these professionals, and organisations that manage insurances and social security systems.

Research organisations, conversely, may rely on a permission to process personal data for scientific and historical research purposes under Article 9(2)(j) of the GDPR and Section 27 of the BDSG.

Data processed by public payors enjoys additional protection as "social security data" (*Sozialdaten*) under Section 35 of the Social Insurance Code I (*Sozialgesetzbuch Erstes Buch – Allgemeiner Teil*; "SGB I"). Sections 67a *et seq.* of the Social Insurance Code X (*Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz*; "SGB X") imposes stricter requirements on the processing compared to those of the GDPR.

For private organisations that are neither involved in the provision of healthcare nor in scientific research, the use of health data is more challenging. In many cases, such organisations must obtain explicit consent as set out in Article 9(2)(a) of the GDPR, as no other exception from the ban on the processing of special categories of personal data applies. This includes suppliers of medical equipment or diagnostic services that wish to re-use personal data for their own purposes, such as product improvements, as well as entities that provide health-related products and services, such as vendors of wearables that record health data, or digital platforms that facilitate finding the best doctor who is an expert for specific ailments.

4.4 How do the regulations define the scope of personal health data use?

Under the GDPR, the scope of data use is limited by the purpose for which the data was originally collected, and the legal basis used.

Health data as a special category may only be processed for certain purposes. By way of example, HCPs can use health data for the provision of medical services and related administrative purposes. However, if they exceed this scope – even if they just want to share anonymised data with the vendor of their equipment – they will need to obtain consent from their patients.

Under Regulation (EU) 2022/2065 (Digital Services Act), digital platforms – whether health-related or not – are not permitted to target advertisements based on the profiling of health data or other special categories of data (Article 26(3)).

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

Regarding compliance with the GDPR, one of the key considerations is identifying the roles of the parties in relation to the processing of personal data:

- if an entity (processor) processes personal data on behalf of another (controller), a data processing agreement is required under Article 28 of the GDPR;
- if two entities are jointly responsible for the processing of personal data, they need to enter into a joint controller agreement under Article 26 of the GDPR; and
- between independent controllers, the GDPR does not directly require specific contractual provisions; however, the parties may want to restrict the re-use of data in order to minimise the risk of non-compliance with the GDPR.

Liability and indemnification obligations are two of the key considerations for every contract. For the use of health data, this is amplified due to the potential for high fines under the GDPR.

Under the EU Data Act, providers are also required to inform the users about the non-personal data generated by a product or service before entering into a contract.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Data inaccuracy is currently not in the focus of data protection authorities. There have been a small number of investigations or warnings reported where data was inaccurate. Due to the fact that automated decision-making is limited by the GDPR, there is a relatively low risk of bias and discrimination based on profiling and data use.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The German BSI publishes various technical standards regarding IT security for handling personal health data. This includes mandatory technical standards for participation in the health telematic infrastructure as well as common standards such as the C5 (Cloud Computing Compliance Criteria Catalogue), which are made mandatory for healthcare providers and public payors by Section 393 of the Fifth Book of the Social Insurance Code (SGB V).

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Under the GDPR, there must be a legal basis for sharing personal data. In digital health markets, this often means that the HCP collecting health and other personal data for purposes of diagnosis and treatment must obtain explicit consent from his or her patients in order to share data for other reasons, such as research or product improvement. This applies even when the professional aggregates or anonymises the data before sharing, as this preparation of data is already a processing activity outside the scope of the provision of healthcare. When data must be made available under the EU Data Act, e.g., when a user requests this, such data must be shared under fair, reasonable and non-discriminatory terms and in a transparent manner.

When sharing data outside the EU, the GDPR imposes additional restrictions to ensure that the personal data remains adequately protected. If the target jurisdiction is not subject to an adequacy decision of the European Commission, adequacy must be ensured through effective contractual undertakings. For transfers to the United States, the new Data Privacy Framework (DPF) allows the transfer of personal data to participating entities. However, it remains to be seen whether this new framework will – unlike its predecessors – hold up to the scrutiny of the Court of Justice of the EU.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

While the GDPR and federal laws apply throughout Germany, different state laws apply to the processing of personal health data by public healthcare providers operated by the State or by local authorities. These vary in whether and under which conditions they permit data sharing and transfers outside the EU/EEA.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

The GDPR sets out different requirements for health data depending on the nature of the entities sending and receiving the data.

Sharing data between HCPs for the purposes of diagnosis or treatment is usually covered by an authorisation stipulated in Article 9(2)(h) of the GDPR. Similarly, professionals can share information with the health insurance for the purposes of billing under this provision. However, these entities must also take professional secrecy into account, and must ensure that patients' secrets will only be shared with others who are subject to professional secrecy or written confidentiality undertakings.

For public payors intending to cooperate with others, Sections 67d to 76 SGB X contain an exhaustive list of the purposes for which health data and other social data may be disclosed to third parties. Section 77 SGB X also bans most transfers to jurisdictions outside the EU/EEA for which no adequacy decision exists. For recipients in the United States, this means that they can only receive social data under the EU–U.S. DPF.

For private payors, these rules do not apply. However, according to Section 213 of the Insurance Contracts Act (*Versicherungsvertragsgesetz*), they may only receive personal health data from HCPs, public payers and certain public bodies, and only with the patient's consent. This limits the cooperation with third parties, such as the providers of digital health products and services.

In order to be able to share data with research organisations, one may rely on the permission to process special categories of personal data for scientific and historical research purposes under Article 9(2)(j) of the GDPR and Section 27 of the BDSG.

Public healthcare providers (e.g., a municipal hospital) and research organisations (e.g., a state university), as well as private hospitals, may be subject to additional restrictions from state data protection laws and governmental policies when sharing health data.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

When sharing personal data, one of the key requirements is ensuring that there is a legal basis for the disclosure of personal data. For health data in particular, one of the exceptions set out in Article 9(2) of the GDPR must apply. In many cases, this requires obtaining the patient's or data subject's consent. For this consent to be valid, the data subject must be informed how their personal data will be used, and with whom it will be shared. The EU Data Act would also require data to be shared with government bodies under certain circumstances.

The ePA has been available since 2021 for patients covered by public health insurance. Patients who opt-in can store or have their healthcare providers store medical reports, standardised medication plans, x-rays and other documents. These documents are currently not machine-readable, although this is planned. As of July 2023, there is also a system for electronic prescriptions (*E-Rezept*), which is secured using the electronic medical data card (*elektronische Gesundheitskarte*).

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

With the ePA, the governmental system already provides for a federated model of data sharing. As this system is designed around the public health insurance models, one of the key issues is the inclusion of private health insurers.

Furthermore, the Health Data Use Act (*Gesundheitsdatennutzungsgesetz*) which was recently passed by the German Federal Government, provides a legal basis for pharmaceutical companies in Germany to access and use patient health data for research purposes.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Patent protection is granted – upon application – for any invention having a technical character, if it is new, involves an "inventive step" and is suitable for industrial application. In digital health markets, the core technology (e.g., sensors and hardware) is generally patentable, even if patents remain mostly used in this rapidly developing environment. The number of worldwide IoT patent applications has increased substantially; the health sector is contributing significantly to this development.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Copyright law has the purpose of granting exclusive, non-registered rights to the author or creator of the original, non-technical work. The work can also take the form of a computer program, e.g., a statement, program language or mathematical algorithm, provided that it is an individual work and therefore the result of the author's own intellectual creation. However, efficient protection of an invention can only be achieved with the help of a patent; at most, copyright law can offer accompanying protection. Data created by digital health programs, however, can never be subject to copyright, because they are not an individual work and therefore, not the result of an author's own intellectual creation.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secrets can be a useful tool to generate value for digital health companies if patent protection is not available, e.g., regarding software source codes or algorithms. The prerequisite of trade secret protection is that it relates to something that can be kept secret and actually is kept secret through reasonable efforts. For example, obvious elements of technology (design, etc.) or business strategies will not remain secret once placed on the market. In order to actually maintain secrecy, companies must – in accordance with the new Trade Secrets Law (*GeschGehG*) – implement a confidentiality programme that includes organisational (e.g., trade secret policies), technical (e.g., IT security) and legal steps (e.g., extensive confidentiality clauses). Only the trade secret as such is protected, not the results achieved with it. This is relevant in the context of data protection, since, for example, a trade secret covering data processing means it does not cover generated data.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Academic technology transfer from university employees to their university employer is subject to certain employee privileges under the German law on employee inventions because of the freedom of teaching and research. As opposed to other employees, a university employee does not have an obligation to report or to disclose a service invention. If a university employee wishes to disclose his or her invention, he or she must notify the university employer of the invention. If a university claims a service invention which was disclosed by its employee, the inventor retains a non-exclusive right to use the service invention within the scope of his or her teaching and research activities. If the university exploits the invention, the amount of the remuneration is 30 per cent of the income generated by the exploitation. This percentage is much higher than the employee invention remuneration of a normal employee.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

In the healthcare sector, the main question is whether intellectual property protection is available for software inventions, e.g., MDSW. If MDSW represents an abstract idea and, therefore, protection is sought for computer programs as such, there is no protection according to patent law. Under German and European patent law, protection is only possible for algorithms and methods underlying the programs that have an inventive step over the prior art – one that is found based only on features that contribute to the technical character. According to German case law, however, programs that immediately trigger a technical effect or directly optimise data-processing hardware are considered patentable. The same rules apply to copyright, since the underlying concept is never fully protected. Trade secret protection for MDSW is only possible under the restrictions described in question 6.3.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

So far, an AI device has not been named as the inventor of a patent in Germany. Several applications for the registration of patents "invented" by an AI device have already been rejected in Germany. The German Patent Act requires an invention to have a human inventor. On a deeper level, the "inventive step" is still seen as an intellectual achievement of a human and product of their personality, which AI is not capable of. The Federal Supreme Court confirmed this view in a recent court order of 11 June 2024 (file number X ZB 5/22) but also stated that AI-generated inventions are, in general, patentable.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

The contractor may be obliged to grant a back licence under the EU, federal or state level funding regulations on publicly funded research and development projects. In general, public grants contain ancillary provisions that must be fulfilled to avoid a possible revocation of the funding decision and the reimbursement of the grant. In addition to exercise and exploitation obligations, the funding conditions include obligations to grant access and utilisation rights in favour of the funding agency, as well as the subcontractors. The Subsidiary Conditions for Grants from the German Federal Ministry of

Research and Education (*Bundesministerium für Bildung und Forschung*) for Research and Development Projects (NKBF 2017), for example, require that the results be made available to research and teaching in Germany and in the EU free of charge.

In addition, inventions that are the result of publicly financed research and development or innovation activities are subject to the EU regulatory framework for state aids according to Articles 107 and 108 of the Treaty on the Functioning of the European Union and the corresponding EU Commission Communication on State aid rules for research, development and innovation (2022 RDI Framework). Under these rules, any transfer of funded inventions to commercial undertakings must be remunerated at the market price.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

According to the case law of the Federal Supreme Court, AI-generated inventions are patentable but AI-devices cannot be named as an inventor (*cf.* Federal Supreme Court, order dated 11 June 2024, file number X ZB 5/22). The Federal Supreme Court is of the opinion that currently no systems exist that can make inventions without any human influence. Therefore, it is always possible to deduce a human being as the inventor, even if an invention was developed by an AI device.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

Collaborations in the digital health sector typically require comprehensive contractual frameworks. These agreements must carefully balance the allocation of intellectual property and commercialisation rights with the delineation of regulatory responsibilities and product liability.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

When entering agreements with healthcare companies or HCPs, non-healthcare companies should refrain from providing any benefits, whether unilaterally (e.g., gifts) or as part of bilateral or multilateral cooperation agreements. Such agreements must ensure that services and consideration are equivalent, with remuneration reflecting arm's-length terms, in accordance with the principle of equivalence.

Any benefits provided must not create the impression of commercial expectations or incentives influencing procurement or therapy decisions. Benefits should serve legitimate, objective purposes and remain entirely separate from other business or commercial interests, adhering to the principle of separation.

All details of cooperation with healthcare companies or HCPs should be documented in clear, written agreements, ensuring maximum transparency. Verbal agreements or other non-transparent arrangements should be avoided, as they risk creating an impression of secrecy, in line with the principles of transparency and documentation.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

When dealing with federated healthcare data-sharing agreements, companies must address data protection requirements, as processing personal data for algorithm training requires a legal basis under the GDPR. For healthcare or patient data, explicit consent is typically required for such processing activities. Additionally, parties must assess whether the algorithm's training results still qualify as personal data or can be deemed anonymised, allowing for unrestricted sharing.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

The use of generative AI is governed by the AI Act, which also applies to providers and deployers of AI systems established outside the EU, insofar as the AI system's output is used within the EU. Providers of generative AI in digital health solutions must ensure compliance with the phased implementation of the legal framework, including proper employee training in AI literacy, the prohibition of certain AI practices, completion of necessary conformity assessments, adherence to transparency requirements and the establishment of a compliant intellectual property strategy.

Moreover, given the absence of clear case law on the ownership of AI-generated results, contracts should explicitly define ownership rights. Parties must also carefully address data protection considerations when integrating generative AI into digital health solutions.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

The primary regulatory authority for AI in the EU is the AI Office, established by the European Commission to oversee the implementation, monitoring and supervision of general-purpose AI and to promote AI governance.

In Germany, the oversight of other AI systems, particularly high-risk AI systems, is expected to fall under the responsibility of the *Bundesnetzagentur* (Federal Network Agency). The agency is anticipated to play a pivotal role, not only in regulatory supervision but also in fostering innovation within the AI sector.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

The core regulatory framework for AI/ML in the EU is the AI Act, which is directly applicable across all EU Member States without requiring national implementation measures. To date, no additional implementing acts have been adopted under the AI Act.

On 9 September 2024, the European Medicines Agency issued a Reflection Paper on the Use of AI in the Medicinal Product Lifecycle, which outlines specific requirements for companies leveraging AI in this sector. Additionally, on 10 September 2024, the first formal meeting of the AI Board, established with the AI Act's entry into force on 1 August 2024, took place.

One of the AI Board's priorities in Phase 1 (2024) is addressing the interplay between the AI Act and the MDR and IVDR, with a strong focus on harmonising these regulatory frameworks for AI applications in healthcare.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

As a general principle, intellectual property rights can only be created and owned by humans, not machines. Therefore, improvements made by AI/ML without active human involvement typically do not qualify for protection under most intellectual property regimes.

In certain instances, the results may be eligible for protection under *sui generis* database rights, which safeguard substantial investments in data collection or management rather than intellectual creativity.

Additionally, such improvements might be safeguarded as trade secrets, provided they meet the legal criteria of being confidential, commercially valuable and subject to reasonable measures to maintain secrecy by the entity responsible for their creation.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Training data is often protected under *sui generis* database rights, as established in Sections 87a *et seq*. of the UrhG, implementing Directive (EC) 96/9, and can be licensed like other intellectual property. However, licensing personal health data is challenging due to GDPR protections, typically requiring anonymisation and robust safeguards against re-identification through technical and contractual measures.

A key consideration is ownership and access to the trained algorithm, which may not be protected by intellectual property rights. Contracts must clearly define each party's rights and obligations regarding its use. Liability and indemnification provisions are essential to address potential GDPR violations, such as invalid patient consent or improper anonymisation.

When licensing healthcare data, compliance with AI Act standards is critical. Data used for training, validation and testing must be pre-assessed for availability, quality, quantity, relevance, representativeness, accuracy and completeness to ensure the AI system operates correctly and safely.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

The AI Act does not establish a separate concept for differentiating standard AI from generative AI, but instead adopts a risk-based approach. Obligations vary according to the risk level of the AI application: lower-risk AI systems face minimal requirements, while high-risk systems, which may include certain generative AI applications, must implement a risk management system, conduct conformity assessments and maintain detailed technical documentation.

Generative AI systems are specifically subject to transparency requirements under the AI Act, particularly regarding the disclosure of AI-generated content.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Germany does not have specific laws governing generative AI technologies. Regulatory issues related to generative AI are primarily addressed at the EU level under the AI Act, which imposes transparency obligations specific to generative AI systems.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

Germany does not have explicit data disgorgement laws, but unauthorised data use can lead to court-ordered deletion or cessation of processing under GDPR, intellectual property laws and trade secret law. Processing without appropriate data rights is unlawful and may result in fines, liability or injunctions.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Besides regulatory responsibility and potential criminal charges, civil law liability plays a significant role in digital health markets. Under German law, there is contractual liability on the one hand, and tort liability under the BGB, as well as product liability under the Product Liability Act (*Produkthaftungsgesetz* – "ProdHG") that each cannot be restricted by a contract on the other hand. MDSW is subject to liability under the ProdHG, even if not offered in a material object as data carrier. The EU AI Act (effective from 2 August 2026), the EU Directive on AI liability (currently in draft form; the timing remains uncertain), the new General Product Safety Regulation (applying since 13 December 2024) and the new EU Directive on liability for defective products of 23 October 2024 (to be transposed by 9 December 2026) are or will soon become relevant, in particular with regard to the use of generative AI in the provisioning of digital health solutions.

9.2 What cross-border considerations are there?

Liability rules are primarily governed by Member State law. In cross-border matters, the Regulation (EU) 593/2008 ("Rome I Regulation") and the Regulation (EU) 864/2007 ("Rome II Regulation") determine the applicable national legislation. Under Article 4 of the Rome II Regulation, the law of the place where the damage occurs applies, regardless of where the

harmful act took place. Exceptions include cases where (i) both parties reside in the same country, making that country's law applicable, or (ii) the tort is more closely connected to another country, in which case the law of that country applies.

For product liability, Article 5 of the Rome II Regulation may make the location where the product was acquired decisive. The Rome I Regulation allows parties, under certain conditions, to contractually agree on the applicable law. In the absence of such an agreement, the law of the service provider's residence generally applies to services, except in consumer contracts, where the law of the consumer's residence usually governs.

Cross-border liability cases carry significant legal and reputational risks. Digital health companies operating across borders should implement a global compliance regime and establish robust structures to address the specific legal requirements of each jurisdiction.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Risks posed by using generative AI can be mitigated by implementing, monitoring and enforcing adequate policies. Potential legal pitfalls and risks include, *inter alia*: the infringement of copyrights and other intellectual property; data security and privacy; confidentiality; contractual obligations; product liability; and AI- and sector-specific regulation. The use cases of generative AI should be carefully evaluated. One important question in this context is whether sufficient licences are in place. The use of dedicated AI models should be considered. It must be identified whether the use includes personal (or health) data.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Currently, there is no specific theory or concept of liability that would apply to misuse of healthcare data included in trained AI/ML models; therefore, the general theories and standards of liability apply.

According to the standard concept of liability, the user is always liable for the content/results generated by AI/ML models. This means the company or individual person that uses AI/ML model-generated contents/results in its own name or adopts the results of an AI/ML model as its own – be it as content on a website, in products or in documents – is liable.

AI/ML models themselves are not liable because they lack the necessary legal personality. The manufacturer of AI/ML models can only be held liable if, for example, the AI/ML model does not have the contractually warranted characteristics or if the manufacturer has not taken sufficient safety precautions within the AI/ML model, resulting in damage.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Healthcare organisations that transfer IT operations to Cloud-based services are facing, *inter alia*, technical and legal challenges. Security and confidentiality are key aspects for a wide-scale offering and use of Cloud-based services. To reduce the risk of cyber-attacks and the loss of personal data, healthcare organisations must ensure a safe system to transfer, maintain and receive health information. Confidentiality can be achieved by access control and by using encryption techniques. Healthcare data may be exchanged only in pseudonymised or even anonymised form. In certain legal regimes, it may be obligatory that Cloud-based services are carried out in Germany or the EU at the very least.

In Germany, the legislator enacted the Health IT Interoperability Governance Ordinance (*Gesundheits- IT -Interoperabilitäts-Governance-Verordnung*) to ensure the secure and fast Cloud-based transfer of patient data.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

As shown above, digital health products and services are strictly regulated and under a high level of surveillance. To offer such products and services on the market, companies must establish a comprehensive compliance organisation, including to meet the various regulatory, data protection and healthcare compliance requirements.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

There are restrictions to corporate ownership of certain healthcare service providers. While there are no ownership restrictions for hospitals, such restrictions exist in the outpatient health services sector with regard to physician practices and medical care centres (*Medizinische Versorgungszentren* – "MVZ"). As hospitals are entitled to hold MVZ, investors usually choose hospitals as their preferred vehicle to indirectly operate MVZ and thereby employ physicians.

In June 2023, the Federal Council (*Bundesrat*) formally requested the Federal Government to issue a draft MVZ Regulation Act (*MVZ-Regulierungsgesetz*) introducing labelling obligations for MVZ owners on practice signs, an MVZ registry and territorial restrictions of the right to establish a dental MVZ with regard to physician group-related planning areas. The proposed regulations are subject to controversial discussions in practice.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The key barriers include stringent market entry, reimbursement and compliance requirements. The entry of MDSW is significantly restricted by certification procedures under the MDR and IVDR, which often necessitate the involvement of notified bodies. These challenges are expected to intensify with the AI Act, which introduces specific conformity assessment procedures for AI MDSW classified as Class IIa or higher. On the reimbursement side, while it may be difficult and time-consuming to convince SHI funds of new and innovative digital health products or services, recent legal developments have facilitated reimbursement, e.g., in the area of medical app prescriptions. Still, companies entering the German digital health markets must observe a number of regulations, including with respect to the processing and use of health data and cooperation with healthcare companies or

HCPs. In clinics, many healthcare services are still reserved to the physician by statutory laws and, hence, not or only partly replaceable by digital health solutions.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In Germany, all practising physicians are supervised by their respective State Physicians' Chamber (*Landesärztekammer*) competent at the federal state level. The German Physicians' Chamber (*Bundesärztekammer*), serving as the joint association of all State Physicians' Chambers, actively participates in legislative procedures by representing physicians' interests and issuing public statements on legislative drafts and proposals. The Panel Doctors' Associations (*Kassenärztliche Vereinigungen*) supervise doctors that are entitled to provide healthcare services reimbursed under the SHI regime. Medical societies (*Fachgesellschaften*) issue guidelines that determine whether a treatment is considered state of the art.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

In Germany, medical apps have recently become subject to a general reimbursement scheme (see question 1.2 above). Besides that, reimbursement depends on the legal status of the respective digital health product or service. Medical devices may be reimbursable as medical aids (*Hilfsmittel*) or – in certain cases after testing periods – as new treatment methods. Digital healthcare services provided by physicians are reimbursed in the same manner as traditional physician services: their reimbursement in the outpatient sector in the SHI is subject to the Uniform Assessment Measure, (*Einheitlicher Bewertungsmaßstab* – "EBM"). New digital health products or services must be listed in the EBM in order to obtain reimbursement. Where such listing takes too long, companies still have the option to enter into reimbursement negotiations with individual SHI funds.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

The primary due diligence challenges in evaluating digital health solutions in Germany include navigating complex regulatory frameworks, ensuring robust data protection and privacy measures and achieving seamless interoperability with existing healthcare systems. Addressing these challenges necessitates a multidisciplinary approach, engaging legal, technical and clinical expertise to ensure comprehensive evaluation and compliance within Germany's healthcare ecosystem.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

In August 2023, the German Federal Government passed the Digital Act and Health Data Use Act. Both aim to foster digitalisation in the healthcare sector, in particular with regard to the use of health data. Among others, the ePA shall be made available to all patients by 2025.

In future, the concept of e-prescription shall be extended to other healthcare products and services, such as physical therapy, medical aids or home care.

To strengthen cross-border patient safety, the national e-health contact point was established in mid-2023, in order to facilitate availability of social insurance data and electronic prescriptions to physicians in other EU countries.

Jana Grieb, Partner, based in Frankfurt, has been advising pharmaceutical and medical technology companies on all aspects of health law for over 20 years. She accompanies pharmaceuticals, medical devices and *in vitro* diagnostics throughout their entire life cycle – from research and development to market access, advertising and distribution. One main area of her work is providing legal and strategic advice on market entry and reimbursement paths in the EU, with a particular focus on the EU regulations on medical devices and *in vitro* diagnostics and the law governing statutory health insurance in Germany.

McDermott Will & Emery Rechtsanwälte Steuerberater LLP
Oberlindau 54–56
60323 Frankfurt/Main
Germany

Tel: +49 69 951145 252
Email: jgrieb@mwe.com
LinkedIn: www.linkedin.com/in/jana-grieb-58b33a135

Steffen Woitz, Partner, based in Munich, focuses his practice on litigation, intellectual property, antitrust and competition law and alternative dispute resolution. Steffen has in-depth litigation experience in all major German courts and assists clients in cross-border disputes and transactions. He represents German and international clients in patent infringement and other contentious matters relating to trademarks, unfair competition and antitrust law.

McDermott Will & Emery Rechtsanwälte Steuerberater LLP
Nymphenburger Str. 3
80335 Munich
Germany

Tel: +49 89 12712 181
Email: swoitz@mwe.com
URL: www.mwe.com/people/woitz-steffen

Dr. Claus Färber, Counsel, based in Munich, represents clients in all legal matters related to the telecommunications, media and information technology (IT) industries and has extensive experience advising international clients across industries on European data protection matters. Claus drafts and negotiates software licence agreements, other IT contracts, business process outsourcing agreements and significant procurement agreements in the telecommunications, e-commerce and IT industry, and assists with significant litigation in these industries. His transactional experience includes major cooperation and framework agreements, such as Internet access in aircraft, WiFi hotspots, roaming, Cloud platforms and machine-to-machine communications (M2M).

McDermott Will & Emery Rechtsanwälte Steuerberater LLP
Nymphenburger Str. 3
80335 Munich
Germany

Tel: +49 89 12712 151
Email: cfaerber@mwe.com
URL: www.mwe.com/people/frber-claus

Dr. Christian Lebrecht, Associate, based in Frankfurt, advises businesses in the life sciences sector. He focuses on medical devices, *in vitro* diagnostics and digital health solutions, guiding clients through complex, industry-specific challenges. Christian develops tailored legal strategies for market entry, distribution and commercialisation, ensuring regulatory compliance and strengthening competitive advantage. He regularly provides support to clients in product liability matters and interim injunction proceedings, especially in areas of unfair competition and medical advertising law.

McDermott Will & Emery Rechtsanwälte Steuerberater LLP
Oberlindau 54–56
60323 Frankfurt/Main
Germany

Tel: +49 69 951145 011
Email: clebrecht@mwe.com
LinkedIn: www.linkedin.com/in/christian-lebrecht

Greece


Evangelos Katsikis


Alexandra Asourmatzian


Filippos-Athanasios Misoulis

KKLegal

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

Digital health is not defined in Greek law. The term is widely used, however, to describe digital tools and services used in the provision of health services. These include telemedicine, electronic health records (EHR), and other digital health technologies such as e-prescription services that focus on the interoperability of the Greek healthcare ecosystem.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

a) Greece's Digital Transformation Strategy (2019–2023) aims to enhance public sector digital services but does not specifically address the reimbursement of digital health solutions.[1]
b) Telemedicine, with emphasis on remote medical imaging analysis, is the fastest growing sector due to a shortage of radiologists, remote consultations with specialists and appointment scheduling platforms. Many companies have launched e-health services in 2025, the most notable being the myAffidea (Greece) platform for primary healthcare services.
c) Interoperability: The National eHealth Interoperability Framework (NeHIF), which was established in 2021, has gained momentum with the main goal being to eliminate information silos. Although it is a government-driven initiative, there are still many companies that are active in the sector.

1.3 What is the digital health market size for your jurisdiction?

The Greek digital health market size cannot be determined given the level of fragmentation. Most digital health services are auxiliary to established healthcare methods and refer to B2B solutions. The total Greek healthcare market is about €17 billion. The digital health market should not exceed 2% of that according to our estimates, although it is expected to develop rapidly. It is estimated that Greek digital health startups raised approximately €80 million in investments out of €555 million in total investments in the Greek startup ecosystem. Overall, Greece ranks low on the Digital Economy and Society Index,[2] meaning that there is significant potential for growth.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

There are no annual revenue figures indicating the top five digital health companies in Greece. However, the digital health sector is experiencing significant growth and investment, indicating a vibrant market.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Given that the digital health sector is not represented in any market report, based on indications, we would assume that the following companies are among the fastest growing: Advantis Medical Imaging (https://advantis.io), which provides an AI-driven medical imaging cloud-based platform; and MRIcons (https://www.mricons.eu), which provides medical imaging enhancement analysis software using proprietary algorithms. Pharmathen is also a notable Greek pharma company that invests in digital health (relating to pharma products) (https://www.pharmathen.com/home). Gnomon Informatics (https://www.gnomon.com.gr) is an IT company with a focus on digital health applications that has developed an applications ecosystem. BIOPIX (https://biopix-t.com) focuses on Molecular Diagnostic products that can be incorporated in the digital ecosystem.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

- The Panhellenic Medical Association (PIS) is responsible for licensing medical professionals in Greece, which includes ensuring that physicians are qualified to provide digital health services such as telemedicine, and issuing guidelines that set the *lege artis* standard for provision of digital health services with emphasis on patient safety.
- Local Medical Associations are responsible for licensing primary care providers that deploy digital health services.
- The National Organization of Medicines (EOF) is responsible for the regulation of pharmaceutical products, including those that incorporate digital tools.
- The Hellenic Data Protection Authority (HDPA) is responsible for securing compliance of the digital health tools and services with the GDPR.

- The Greek Ministry of Health constitutes the general regulatory and supervisory authority for all electronic health in Greece, according to Article 23 of Greek Law 4715/2020.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

Key regulations for digital healthcare services in Greece include:

- Law 4213/2013 (Article 6): governing cross-border healthcare services.
- Articles 914 and 330 of the Greek Civil Code: addressing civil liability for digital healthcare services that also trigger Law 2251/1994 on Consumer Protection (reversing the burden of proof in medical malpractice (medmal) cases).
- Law 4961/2022 (Article 42): on information and communication technologies.
- EU Regulation and Directives: mainly Regulation 2017/745/EU (MDR) for medical devices including software, Regulation 2017/746/EU (IVDR) relating to *in vitro* diagnostic medical devices, Regulation 2024/1689 (EU AI Act) on the use of AI, Directive 2016/1148/EU on Network and Information Security systems, and Directive 2011/24/EU (Article 14) on patients' rights in cross-border healthcare.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

Key areas of enforcement include cybersecurity, data privacy, patient safety, and compliance with the MDR and IVDR. Emerging areas include interoperability, use of AI and transparency.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

- Greek patent law 1733/1987 regarding the intellectual property (IP) issues of digital health technologies, by the Greek Patent Office and the EUIPO.
- MDR, Article 2 of the Regulation: "medical device" includes software for medicinal use.
- GDPR, under the supervision of the HPDA.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

- Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024, regarding the use and development of AI, which is also applicable in the field of digital health.
- Law 4961/2022: Articles 8 and 10 relating to the obligation for the Registration of AI applications in the AI Registry for Public and Private Entities, respectively, are also applicable.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

The EOF, being a public entity primarily responsible for the regulation of the medical devices industry, focuses mainly on monitoring MDR and IVDR requirements. There is no authority responsible for AI use, but different stakeholders adopt different approaches. The PIS encourages innovation while focusing on patient safety. Compliance with GDPR remains a cornerstone of digital health regulation in Greece. The Greek National Commission for Bioethics & Technoethics proposes adapting terms and conditions for safe implementation and assessing successful international applications for potential integration into the Greek health system.[3] Greece fully adheres to the EU approach per European Medicines Agency (EMA) guidelines. The regulatory framework is obsolete, thus creating both barriers to entry and opportunities for innovation.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Per the EU regulatory framework (MDR, IVDR), any application must provide clinical validation data relating to safety, performance and efficiency. Any digital health application not compatible with the EU framework is illegal for use in Greece.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

All solutions are regulated at the national level. Local authorities are not competent.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

The fragmentation of the digital health regulatory framework in Greece means that priorities are differentiated. The Ministry for Health emphasises stakeholder engagement for providing digital health solutions to reduce costs. However digital therapeutics cannot be prescribed (unlike in Germany or the UK) and are not reimbursed by public payers. The Greek Data Protection Authority seeks to safeguard against patient data abuse by monitoring the data sources and emphasising data anonymity. Medical Associations provide emphasis on adapting the existing legal requirements to include digital health solutions.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Patient safety, patient data protection and best practices relating to online treatments by qualified medical professionals.

- **Robotics**
  Best practices relating to patient safety and systems reliability, product liability relating to medmal claims and informed patient consent for innovative treatments.
- **Wearables**
  Reliability and accuracy in relation to data collection for clinical purposes (CE marking and EMA clearance or FDA Use Authorisation based on clinical evidence), and user data privacy (relating to the use of the data collected for unauthorised uses).
- **Virtual Assistants (e.g. Alexa)**
  Security, consumer protection relating to the sources of information for medical conditions and the safeguarding of their privacy.
- **Mobile Apps**
  Strict compliance with data protection and cybersecurity requirements, ensuring reliability and safety for apps serving as medical devices, and adhering to IP and consumer protection regulations.
- **Software as a Medical Device**
  Compliance with regulations for medical devices (MDR/IVDR) and liability for defects, as well as privacy protection and cybersecurity, are the most critical issues.
- **Clinical Decision Support Software**
  Safety and accuracy of the software based on proven clinical results. Clarity of the context of use (supportive to doctors' evaluation only) and the terms of use. Must be error free and protected against malicious third parties that could harm patients while guaranteeing the lawful processing of data and compliance with medical device and cybersecurity regulations.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  Explainability of its decisions, often creating a "black box" effect. Specifically, it can be difficult to explain an AI decision, yet this is a requirement under Greek regulations and laws. All digital health solutions do not stand on their own but are supportive to a licensed medical professional.
- **IoT (Internet of Things) and Connected Devices**
  Privacy concerns through the collection of data from multiple devices. It is crucial to ensure the lawful and secure processing of data to protect patients' privacy and health. The WEEE Directive 2012/19/EU mandates e-waste disposal and recycling to minimise environmental impact.
- **3D Printing/Bioprinting**
  Product liability for defects based on consumer protection laws, IP rights, ensuring the proper disposal of electronic waste, and environmental management.
- **Digital Therapeutics**
  Only B2B applications. All digital health solutions are supportive to a licensed medical professional.
- **Digital Diagnostics**
  Only B2B applications. Accuracy and reliability of diagnostic algorithms, potential biases in AI-driven tools affecting clinical decisions, the need for ongoing training of healthcare professionals to use the technology effectively, the high costs of implementation and maintenance, and regulatory challenges in ensuring compliance with medical standards and certifications.
- **Electronic Medical Record Management Solutions**
  Data protection, challenges in the interoperability of different systems, particularly between public and private healthcare entities, as well as legal liability concerns in cases of errors or system failures.
- **Big Data Analytics**
  Privacy concerns relating to individual consent.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Transparency, traceability, interoperability and efficiency of processes.
- **Natural Language Processing**
  The main issues with the use of Natural Language Processing in healthcare are ensuring the accuracy of the data it generates, data protection and liability in case of errors. Language barriers and the use of accurate terminology are dealt with under consumer protection and product liability laws.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Digital health platforms currently focus on B2B solutions (namely services to doctors). B2B solutions emphasise the MDR and IVDR requirements. Any B2C platforms must be licensed medical practitioners or rely on fully licensed medical doctors in Greece. It is illegal for non-medical entities to offer medical services. Any medical entities registered and providing services in Greece must be registered with the relevant local Medical Association in Greece.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

- Privacy and data protection for sensitive health data: GDPR, Law 4624/2019.
- Confidentiality and informed consent: Code of Medical Ethics (Law 3418/2005).
- Security measures and breach accountability: ePrivacy Directives and GDPR provisions.
- Risk-based approach to high-impact data processing: Data Protection Impact Assessment requirements under GDPR.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

This is not applicable. Regulation is at the national level.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

GDPR and Law 4624/2019 set the general national regulatory framework, with case-specific variations, depending on the institution and the nature of the data. Public sector institutions enjoy more flexibility for public policy reasons, while private ones must prove strict adherence. Sensitive data requires strict protection, while anonymised data is used more freely. Digital health platforms are also subject to additional cybersecurity requirements.

4.4 How do the regulations define the scope of personal health data use?

The GDPR Greek application regulates health data use by type, purpose and legal basis, such as consent or necessity. Health data covers an individual's condition and may serve medical, public health or research purposes. Key principles based on the EU policy include minimisation, accuracy and security. Anonymised data, while exempt from some rules, must still ensure legitimacy and privacy. Local additional requirements relate mainly to informed patient consent.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

To ensure compliance with personal health data laws, agreements between a data controller and a processor must, at minimum, include the provisions of GDPR Article 28. These cover the purpose, duration, nature and scope of processing, data types, categories of data subjects, and the obligations and rights of both parties. Any sub-processors must be bound by the same terms. In joint controller arrangements, the parties must clearly and transparently allocate responsibilities to ensure GDPR compliance in all processing activities, particularly regarding data security, breach notifications and handling data subject requests.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

In Greece, the HDPA enforces GDPR to ensure accurate, unbiased handling of personal health data. It addresses complaints, monitors compliance and imposes penalties if violations occur. Healthcare providers must adopt safeguards against discrimination and maintain transparent data practices.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

GDPR and Law 4624/2019 primarily govern personal health data processing in Greece. The HDPA provides guidance and enforces compliance. The ePrivacy Directive applies to digital health data usage, while the upcoming European Health Data Space initiative sets new standards for secure data sharing.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Health data are classified as a special category of personal data. It requires a legal basis under Articles 6 and 9 of the GDPR. Data sharing shall be lawful, transparent, adequate, and for specific, legitimate purposes. Controllers bear the burden of proving compliance. For sharing outside the EU, Chapter 5 of the Regulation provisions must be followed.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Greece is a unitary state, so data protection (including health data) is centrally regulated under the GDPR and Law 4624/2019. The HDPA enforces compliance – no separate authorities exist at the state level. Regional or municipal bodies apply the same national guidelines for data sharing. In practice, central regulation ensures uniform standards across the entire country.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

The obligations arising from the data privacy laws may differ depending on whether they are applicable in the public or private sector. Public entities may process data for public interest reasons, while private ones usually rely on the legal basis of performing medical contracts (offering medical services).

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

National digital health initiatives like the ePrescription system and the NeHIF define technical specifications and secure interconnection procedures, fostering seamless and secure health data exchange. The Code of Medical Ethics (Law 3418/2005) imposes confidentiality obligations and sets conditions for the transmission of patient information, while the privacy frameworks (GDPR and Law 4624/2019) establish fundamental standards for health data sharing. The HDPA oversees compliance.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

The key issues are ownership and consent, cross-border data sharing in the EU, interoperability and data sovereignty. The provisions of Law 3471/2006 on electronic communications and Law 4238/2014, which mandates the creation of EHRs for all citizens under the Ministry of Health's oversight, are the key laws to consider.[4]

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Under Law 1733/1987, patentability requires technical character, industrial application and novelty. The patent holder has the right to introduce to the market, the product, the method protected by the patent and the product whose production is the result of use of the method protected by the patent. Finally, the holder has the right to prohibit any third party from commercially exploiting the invention protected by the patent.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Law 2121/1993 protects original works of authorship, including software programs and databases. Creators of digital technology tools own exclusive rights to their creations, including the right to distribution, reproduction and public display. However, only source code, object code and certain aspects of the software's functionality are protected, and not the underlying ideas or algorithms that led to its development.

Copyright protection lasts for a duration of 70 years after the death of the author, ensuring the long-term protection of digital health technologies.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Under Law 4605/2019, transposing Directive 2016/943, trade secrets are defined as non-publicly known or accessible information of economic value, that is subject to secrecy.

Trade secret protection is broader than copyright protection covering a wider range of information. It includes not only the developed technology, but also its methods, business practice and any other confidential information that contributed to its development. Trade secret protection lasts indefinitely, as long as the protected information remains confidential.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

- Law 4310/2014 focuses on the promotion of research and technological development. It regulates technology transfer by establishing a cooperation framework between universities and the private sector.
- Law 4485/2017 governs the organisation and operation of higher education institutions and research organisations, regulating technology transfer and collaboration between universities and the private sector.
- The Greek Patent Law is crucial for the protection of innovations resulting from academic research.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Software as a medical device is protected by copyright law as a literary work, covering source code, object code and functionality, preventing unauthorised use. However, underlying ideas and algorithms are not protected, allowing similar software development if the code is not copied. Patent protection is possible if the software meets the criteria of novelty, inventive step and industrial applicability, typically requiring a technical solution. Non-patentable elements, such as algorithms, can be protected as trade secrets, but regulatory approvals may limit this protection by requiring disclosure of technical details. Thus, software protection combines copyright, patents and trade secrets, each with limitations and subject to compliance with regulatory obligations in the healthcare sector.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

No. Only a natural person can be recognised as an inventor.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

Government-funded inventions are subject to the general terms governing IP protection in Greece, and in particular Article 6 of the Greek Patent Law.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

Greek and European courts have addressed IP rights protection of digital health innovation in several cases. The most significant case in EU case law is case C-329/16, which is the CJEU's first decision on software as a medical device.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

- Determine the titles to both the existing IP and the one under development, and the terms of use of respective IP.
- Determine the commercialisation terms of the innovations and improvements that are jointly developed.
- Use non-disclosure agreements to guarantee the protection of all confidential information exchanged between them during their collaboration.
- Establish fast and accurate dispute resolution mechanisms (Greek legal system lags).
- Ensure compliance with the regulatory framework.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

- Scope of Services: Clearly define the scope of services. Include performance metrics and quality standards to ensure accountability and manage expectations.
- Payment Terms: Clear payment structures, including fees for services rendered, payment schedules and conditions for any adjustments.
- Alignment of Goals: Both parties should have aligned objectives.
- Monitoring and Evaluation: Establish a framework for ongoing monitoring of the partnership's effectiveness.
- Medmal Risk Allocation: Clearly define the relative obligations.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

- Data Governance and Ownership: Clearly define data ownership rights and governance structures within the agreement.
- IP Rights: Define the ownership of IP generated from the collaborative efforts. Roles, AI model ownership and dispute resolution mechanisms must be outlined.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

- Scope of Services: Clearly outline the respective parties' scope of work related to generative AI applications.
- IP Rights: Clearly define ownership of IP created through the use of generative AI.
- Compliance with Regulatory Standards: Ensure that all parties commit to complying with applicable healthcare regulations and standards and the end product does as well.
- Scalability and Future Integration: Consider how the generative AI solution can connect to existing solutions in the Greek ecosystem and can be scaled in the future.
- Liability and Indemnification: Include clauses that define liability in case of breaches or failures.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

The main regulators that will gain enhanced powers from August 2026 under the European AI Regulation, checking that organisations comply with the requirements of the Regulation, will be:

1) The HDPA (APDPX): Enforces data protection laws and safeguards individuals' privacy rights.
2) The Greek Ombudsman: An independent authority investigating maladministration and protecting citizens' rights.
3) The Hellenic Authority for Communication Security and Privacy (ADAE): Supervises and secures the confidentiality of communications.
4) The National Human Rights Commission: Promotes and protects human rights within Greece.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

- APDPX enforces GDPR compliance for AI/ML data processing and privacy by receiving complaints.
- The Greek Ombudsman investigates maladministration, including AI-based discrimination.
- The ADAE ensures confidentiality and security in AI-driven communications.
- The National Human Rights Commission addresses human rights concerns from biased or intrusive AI.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Companies rely on contractual clauses for IP protection, since laws do not protect AI-generated algorithms without human involvement. No specific legislation for AI-generated works exists, but future reforms may address this as copyright (Law 2121/1993) and patent laws recognise only human creators.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

In licensing data for AI/ML projects, it is crucial to define the licence scope, duration and permissible uses, while also establishing ownership rights and confidentiality obligations (including derivative works). Full compliance with the GDPR and Greek Law 4624/2019 demands clear delineation of data controller and processor roles, as well as robust protective measures. When licensing healthcare data, valid legal basis is required, complemented by effective pseudonymisation/anonymisation and heightened security safeguards. Financial arrangements can involve either lump-sum payments or royalties, typically with liability caps and audit provisions. Overall, this framework balances innovation with legal and ethical responsibilities.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

AI regulations do not differentiate between standard and generative AI. The EU AI Act uses a risk-based approach, with stricter rules for high-risk applications, including generative AI in sensitive areas. National regulators, like the HDPA, are addressing transparency, data protection and accountability challenges, hinting at future regulatory distinctions.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Generative AI raises unique issues around data privacy, IP rights, liability and risk of misinformation. In Greece, the HDPA ensures compliance with GDPR standards for AI-based data processing.

Authorities also align with the upcoming EU AI Act, adopting a risk-based regulatory approach. Academic institutions and tech consortia collaborate on guidelines, focusing on fairness, transparency and safety.

The National Strategy for AI fosters continuous development of ethical and legal frameworks for generative AI.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

The Data Privacy framework requires valid rights for data used in AI/ML. Although there is no formal "data disgorgement" regime, the Greek Data Protection Authority can require deletion or cessation of illegal data processing and impose fines for non-compliance. This covers both personal data issues and broader liability for using data without proper authorisation.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

- Under Article 914 of the Greek Civil Code, liability arises in case of wilful misconduct or negligence. The latter includes the case of a party's failure to meet the scientific and industry standards and best practices.
- Under Law 2251/1994 on Consumer Protection, developers may be found liable for defective products, including both manufacturing and design defects, as well as the case of inadequate warning regarding potential risks that may occur from the improper use of the product (reversing the burden of proof).
- Article 371 of the Greek Civil Code addresses the breach of contractual obligations.
- Under Article 922 of the Greek Civil Code, the scope of liability is expanded to include employers in case of a negligent act by their employees or agents.
- In case of unauthorised access to or disclosure of personal health information, liability may stem from violations of GDPR.

9.2 What cross-border considerations are there?

Cross-border considerations include compliance with the GDPR, the MDR and the IVDR. Furthermore, the Brussels Regulation (EU 1215/2012) is applicable, defining the applicable jurisdiction and establishing the enforcement of cross-border disputes, including contract enforcement and liability.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

The best practices are as follows: ensure adherence to the GDPR; implement policies for data protection, privacy rights and patient consent; constant clinical and real-world testing of AI/ML systems in use to ensure their accuracy, unbiased results, applicability, reliability and precision; ensure that the design and operation of AI systems minimise the bias, to avoid potential false results; adopt the highest level of cybersecurity measures to prevent breaches, such as encryption, anonymisation and secure cloud storage solutions; and transparency, accuracy, sensitivity and specificity of all data in connection to the use of AI systems.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Misuse of healthcare data in AI/ML models can trigger civil, contractual, employer, product and criminal liability under Greek law.

- Article 914 of the Civil Code imposes liability for negligence by healthcare providers or AI developers.
- Article 371 addresses contractual liability for breaching parties.
- Article 922 extends liability to employers for negligent acts by employees.
- Law 2251/1994 on Consumer Protection classifies defective AI tools as products, holding manufacturers liable, with the burden of proof reversed.
- Article 386 of the Criminal Code imposes criminal liability for fraud if healthcare data misuse is intentional and aims to deceive patients.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

In addition to the general issues outlined, other key issues also include: data sovereignty; service availability and reliability; provisions to avoid vendor lock-in; and regulatory compliance with Chapter 5 of the GDPR.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Key issues include: ensuring use and/or partnership with licensed medical providers and/or practitioners; and ensuring compliance with a stringent regulatory environment, robust data security and obtaining clinical validation.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

The key issues are as follows: ensure the target's regulatory compliance – digital health is not regulated *per se*, although parts of it are subject to a complex regulatory framework, including but not limited to, the MDR, IVDR, GDPR and national telemedicine laws; confirm the target's ownership of IP, including software and algorithms, and assess risks of infringement or disputes; consider the long-term exit strategy and make provisions in the financing agreements; and utilise expert advisors in healthcare.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The most significant challenge is the lack of a clear regulatory framework, as digital health solutions are subject to a multitude of legal and regulatory categories, such as software,

medical devices or telemedicine platforms. Furthermore, there is neither national nor European definition and regulation of digital health *per se*.

Moreover, the adoption of digital health solutions is impeded by interoperability issues. Digital health solutions are often incompatible with the existing digital infrastructure of the healthcare systems.

Furthermore, public and private insurance schemes have not yet adopted reimbursement models for digital tools.

Finally, the adoption of digital health on a larger scale requires the enhancement of cybersecurity standards.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The key clinician certification bodies are as follows: the PIS, which licenses medical professionals; specialty societies such as the Hellenic Society of Radiology, the Hellenic Cardiological Society and the Hellenic Society of Medical Informatics; and the Ministry of Health.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

In Greece, reimbursement for digital health solutions in terms of social security is limited and managed case-by-case by the national Health Insurance fund (EOPYY). Digital health services are not reimbursed. Telemedicine saw partial coverage during COVID-19, but digital tools remain under EU MDR and GDPR compliance. Future guidance from the Ministry of Health or medical bodies may formalise reimbursement criteria as healthcare trends evolve. Private insurance companies mainly utilise platforms for remote clinical screening.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Digital health struggles with gaps in standards, algorithmic bias, data quality, transparency and GDPR compliance. Many lack clinical validation, cybersecurity and post-market surveillance. Governance issues include weak data use policies, inadequate patient consent and missing privacy-by-design frameworks. Clear guidelines, certifications and evidence-based benchmarks are crucial for responsible digital health solutions.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

The success of digital health solutions heavily depends on patient adoption and engagement rates. Investors should consider the usability and accessibility of technologies to ensure broad patient uptake, especially among vulnerable populations. The Greek digital health ecosystem is expected to grow at an increased pace given the geographic limitations of the country (thousands of islands) and the aging population. Doctor shortages and the aging population make the use of digital health solutions imperative.

Endnotes

1 https://digitalstrategy.gov.gr/website/static/website/assets/Digital_Transformation_Strategy_2019.pdf

2 https://digital-strategy.ec.europa.eu/en/policies/desi-greece

3 *O P I N I O N on The applications of Artificial Intelligence in Health in Greece*, National Commission for Bioethics & Technoethics, December 2023. Available at: https://bioethics.gr/api/files/download/2355/OPINION%20AI%20IN%20HEALTH%20EN.pdf

4 Ioannis Kotsiopoulos, *Digital Transformation of the Healthcare Sector in Greece*, October 2022. Available at: https://www.ihe-europe.net/sites/default/files/PDF%20EXP%2022/1-IHE_ExP_DAY_PPT_Kotsiopoulos_v2.pdf

Evangelos Katsikis is an accomplished Lawyer and Managing Partner at KKLegal, a leading law firm representing private healthcare providers, public hospitals and health institutions across Greece. With over two decades of experience, he serves as Legal Counsel to the Panhellenic Medical Association, playing a key role in shaping healthcare legislation.
Evangelos's legal practice spans a wide range of health-related sectors, including primary and secondary care providers, medical technology companies and pharmaceutical firms. He provides legal counsel on matters such as medical liability, health data protection (GDPR compliance), telemedicine, AI/ML applications in healthcare and public procurement for health services. He is also experienced in handling litigation related to medical malpractice and healthcare disputes, representing both healthcare professionals and institutions.
He has significant cross-border transactions experience in both Europe and the United States and is active in M&As, having advised on over 300 successful deals. He serves at the Board of Directors of several corporations and is entrusted by the most prominent multinational healthcare providers for representing them in Greece.
He has contributed to key legal reforms, including the COVID-19 immunity provision for healthcare professionals, protecting medical staff from liability during the pandemic. His expertise in drafting legal opinions, legislative proposals and regulatory policies has made him a trusted advisor to both healthcare institutions and government bodies.

KKLegal
7 Patriarchou Ioakeim Str., Athens, 10675
Greece

Tel: +30 210 822 4775
Email: katsikis@kklegal.eu
LinkedIn: www.linkedin.com/in/evangelos-katsikis-209764b

Alexandra Asourmatzian is a highly experienced Lawyer specialising in corporate law, commercial law and regulatory compliance.
As a member of the Athens Bar Association since 2011, she brings more than a decade of legal proficiency to her practice. She began her journey at KKLegal in 2017, steadily advancing to her current leadership role in 2022. As a Partner, she heads a corporate legal team, providing strategic legal counsel to companies, particularly in the healthcare sector. Her responsibilities include conducting due diligence for M&As, drafting commercial and employment contracts, managing regulatory compliance and offering day-to-day legal support to clients navigating complex regulatory frameworks.
Alexandra's academic credentials underpin her professional expertise; she holds a Law Degree (LL.B.) from the National and Kapodistrian University of Athens, and a Master of Laws (LL.M.) in French and European Law from the prestigious University of Paris I Panthéon-Sorbonne. This advanced education provided her with a deep understanding of European legal systems and transnational legal issues.
Certified as a Data Protection Officer by TÜV AUSTRIA, she is a member of KKLegal's project team handling significant Data Protection Officer projects for major institutions both in the public and private sector.

KKLegal
7 Patriarchou Ioakeim Str., Athens, 10675
Greece

Tel: +30 210 822 4775
Email: asourmatzian@kklegal.eu
LinkedIn: www.linkedin.com/in/alexandra-asourmatzian-53a16483

Filippos-Athanasios Misoulis is a highly qualified Greek Attorney and a member of the Athens Bar Association. He holds a Bachelor of Laws (LL.B.) and an LL.M. in Law of the European Union from the National and Kapodistrian University of Athens, Faculty of Law. With extensive expertise in civil, corporate and contract law, Filippos has handled a diverse range of legal issues, gaining in-depth knowledge and hands-on experience in navigating complex legal environments. In his professional practice, Filippos has advised clients on a broad spectrum of legal matters, including drafting and negotiating agreements, ensuring compliance with both national and European legal frameworks, and representing clients in litigation and alternative dispute resolution proceedings. Filippos has also contributed to the legal field through authorship, having published articles in legal journals on issues related to International and European law.
Filippos is fluent in Greek (native), English, French, German and Russian, and possesses a basic command of Mandarin Chinese. This multilingual ability, coupled with his intercultural communication and negotiation skills, enables him to work effectively with clients and legal counterparts from diverse cultural backgrounds.

KKLegal
7 Patriarchou Ioakeim Str., Athens, 10675
Greece

Tel: +30 210 822 4775
Email: misoulis@kklegal.eu
LinkedIn: www.linkedin.com/in/filippos-athanasios-misoulis-bb846b166

KKLegal is a pioneering law firm with a sharp focus on health law, digital law and technology-driven legal solutions. Since its establishment in 2000, the firm has become a trusted partner for leading healthcare providers and tech companies, offering precise, results-driven legal advice in highly regulated sectors. KKLegal is the leading advisor to healthcare corporations and practitioners in Greece.
The firm stands out for its cutting-edge approach to digital transformation, integrating advanced legal tech tools to streamline processes and deliver cost-efficient, high-value solutions.

www.kklegal.eu

India

Manisha Singh

Dr. Pankaj Musyuni

LexOrbis

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

Digital healthcare is a multidisciplinary concept that is located at the intersection of healthcare and digital technology. Digital healthcare revolutionises the delivery of healthcare services for providers through the use of comprehensive platforms, tools and services. Mobile health applications, telemedicine, enterprise resource planning (ERP), customer relationship management (CRM), electronic health records (EHRs) and health information systems (HIS) are among the numerous technologies that contribute to the transparency of patient data. "Digital health" is a comprehensive concept that entails the integration of digital technologies with the healthcare sector to improve efficiency and provide more personalised patient care. The Digital Information Security in Healthcare Act of 2018 (DISHA) defines "digital health data" as an electronic record of an individual's health-related information, despite the fact that the terms "digital health", "digital medicine" and "digital therapeutics" lack specific definitions in India. The term "said data" generally refers to relevant information about an individual's physical and mental health, the therapies they have received from healthcare providers, any donated body parts or biological materials, as well as the results of their testing and examinations. The integration of genetics and digital technologies exemplifies the concept of digital health, facilitating the early diagnosis and treatment of diseases. The World Health Organization (WHO) and the G20 India presidency introduced the Global Initiative on Digital Health (GIDH) during the Health Minister's Meeting at the G20 Summit, which the Government of India convened on August 19, 2023. The new GIDH initiative will function as a network and infrastructure under the WHO's supervision to facilitate the implementation of the Global Strategy on Digital Health 2020–2025.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Digital healthcare is a multidisciplinary concept that lies at the intersection of healthcare and digital technology. It incorporates a diverse array of technologies, such as telemedicine, ERP, CRM, EHRs and HIS, all of which enhance the transparency of patient data. The most significant emerging technologies in the field of digital health include m-health, digital pathology, telemedicine, health wearables, digital and social connectivity, big data analytics, virtual reality, ambupods, blockchain and electronic medical records. Increased awareness and adoption for the Internet of Things (IoT) and telehealth have made health-monitoring technology more accessible and cost-effective. The healthcare sector of India has undergone significant transformations as a result of the Digital India initiative. Initiatives like the Ayushman Bharat Digital Mission, CoWIN App, Aarogya Setu, e-Sanjeevani and e-Hospital have extended healthcare facilities and services to every corner of India.

1.3 What is the digital health market size for your jurisdiction?

The favourable legislation in India and the growing prominence of the digital healthcare industry have significantly improved the country's use of digital technology. Industry experts anticipate the digital health industry in India to expand at a compound annual growth rate (CAGR) of approximately 29.5% from 2024 to 2032. Leading experts anticipate that the digital health sector in India will reach a valuation of USD 3.88 billion in 2023 and rise to USD 39.7 billion by 2032. It is anticipated that the Indian digital health market will experience growth due to the increasing prevalence of chronic conditions during the projected period. According to a customer market insights survey, it is expected that the Indian digital health market will reach USD 8.7944 billion in 2024 and expand at a CAGR of 17.67% between 2024 and 2033, ultimately reaching USD 47.8069 billion. The objective of digital health is to enhance the quality, accessibility and delivery of medical services by integrating technology with healthcare. It encompasses a diverse array of applications, such as telemedicine, mobile health applications, EHRs and data-driven, AI-powered personalised care. Insights10, a healthcare-focused market research agency, anticipates that the Indian digital health market will experience accelerated growth in the coming years as a result of its size and favourable government policies.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

Among the top five largest digital healthcare technology enterprises are Novartis, Stryker, Edwards Lifesciences, Centura Health and Hologic.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

The more promising digital health start-ups and the fastest growing in India include 1mg, HealthifyMe, Netmeds, Cult.fit, Onsurity, HealthKart, PharmEasy and Innovaccer.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The Central Drugs Standard Control Organisation (CDSCO) is the primary regulatory body responsible for the enforcement of the Drugs and Cosmetics Act, 1940, and "rules made thereunder" (DCA). Furthermore, the Medical Council of India oversees the practice of medicine. Additionally, the Copyright Office is responsible for copyright, while the Office of the Controller General of Patents, Designs and Trademarks is responsible for intellectual property protection. The Department for Promotion of Industry and Internal Trade comprises both divisions. The Indian Council of Medical Research has also made significant contributions to the promotion of research in support of the National Digital Health Blueprint from the Ministry of Health and Family Welfare (MoHFW).

The following key acts typically govern the legal and regulatory framework:

- In 2011, the Information Technology Act (IT Act), consisting of the Information Technology Rules (IT Rules) of 2011 and the Sensitive Personal Data or Information (SPDI) Rules, came into effect.
- Requirements for other service providers under the New Telecom Policy of 1999.
- The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations of 2002 and the Indian Medical Council Act of 1956.
- The Drugs and Magic Remedies Act of 1954 and the Drugs and Magic Remedies Rules of 1955.
- The Unsolicited Commercial Communications Regulations of 2007 and the Commercial Communication Customer Preference Regulations of 2010.
- The Clinical Establishments Act of 2010.
- The Digital Personal Data Protection Act (DPDP Act).

The Indian government is responsible for enforcing rules regarding digital health. These rules come from: the DCA; the IT Act and Rules, especially Sections 2(w), 43A and 79; the Clinical Establishments (Registration and Regulation) Act, Section 38(1) and 38(2); and Rules 3, 4(1), 5(1), 5(3), 5(7) and 7 of the IT Act. The regulatory authorities are responsible for enforcing reasonable security practices and procedures for SPDI, as outlined in: the Data Protection Rules; Rule 3 of the IT (Intermediaries Guidelines) Rules; the Medical Devices Rules; the DNA Technology (Use and Application) Regulation Bill; and the DPDP Act.

In order to protect the confidentiality of health-related information, it is imperative that medical professionals and patients implement data security measures. This information includes recommendations and outcomes. The Intermediaries Guidelines of 2011, the Data Protection Regulations of 2011 and the IT Act of 2000 are all intended to address this need and should be consulted in all circumstances. However, the rigorous compliance requirements have led to the establishment of no standards mandating the implementation of data security and protection. The rise of digital and other healthcare technology has raised patient privacy and data security concerns. When transmitting personal data, the most critical factors to consider are the preservation of confidentiality, the regulation of data transmission, the assurance of security and privacy, and the consideration of knowledge, trust, accountability and responsibility.

The MoHFW has proposed the National Digital Health Authority (NeHA) to facilitate the development of India's Integrated Health Information System (IHIS). On August 11, 2023, the ratification of the DPDP Act, 2023, transformed India into a legal nation. India has implemented a new law to govern the administration of personal data. In addition to establishing a framework for the governance and accountability of data, one of its objectives is to preserve the privacy of individuals. The DPDP Act will have a substantial impact on the Indian healthcare industry, despite the fact that it is still in the early phases of digital transformation. The DPDP Act primarily focuses on digital personal data and does not address non-personal data. The implementation of the DPDP Act will render Section 43A of the IT Act and the IT (Reasonable Security Practices and Procedures and SPDI) Rules, 2011. These pieces of legislation address the legal and ethical concerns related to digital health.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

The IT Act and the SPDI Rules govern the current legislative framework for e-health protection in India, offering some protection for the acquisition, disclosure and transmission of sensitive personal data, including medical records and histories. The government and the MoHFW published a blueprint, recommending the establishment of a National Digital Health Ecosystem, and announced the National Digital Health Mission (NDHM). This ecosystem will enable the interoperability of digital health systems at the patient, hospital and ancillary healthcare provider levels. The MoHFW implemented the Health Data Management Policy for the ecosystem. Furthermore, the MoHFW implemented the DPDP Act in India with the primary goal of promoting accountability and responsibility among enterprises operating within the country. Reproductive Child Healthcare, the Integrated Disease Surveillance Program, the IHIS, e-Hospital, e-Sushrut, the Central Government Health Scheme, the Integrated Health Information Platform, the National Health Portal, the National Identification Number and the Online Registration System are among the numerous digital health initiatives that the MoHFW is currently implementing. As health is a state responsibility, the National Health Mission provides funding to states for related services, such as hospital information systems, telemedicine, teleradiology, tele-oncology and tele-ophthalmology.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

It is imperative to establish regulations that safeguard the privacy, confidentiality and security of patients' medical and health records. Monitoring data protection and violations

is crucial, as confidentiality agreements safeguard private health information and records solely for data interpretation in market analysis, marketing and regulatory sharing. In India, telemedicine and teleconsultation, wearable devices, online pharmacies and artificial intelligence (AI) are among the most significant emerging technologies in the field of digital healthcare.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

The CDSCO, a part of the Directorate General of Health Services (MoHFW), is India's major medical device and diagnostics regulating organisation. The Drug Controller General of India (DCGI) leads the CDSCO. The DCGI approves specific medications (vaccines, large-volume parenterals, blood products and r-DNA-derived products), medical devices and novel drugs. The DCA governs the manufacture, importation, sale and distribution of medical equipment in India. Only the following notified medical devices listed below as "drugs" are currently under the DCA's control in India:

(i) substances used for *in vitro* diagnosis and surgical dressings; surgical bandages, surgical staples, surgical sutures, ligatures, blood, and blood-component collection bags with or without anticoagulant; and

(ii) substances, including mechanical contraceptives (condoms, intrauterine devices and tubal rings).

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

There are currently no official provisions.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

There are currently no official rules.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

There are currently no official provisions.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

There are currently no official rules.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

There are currently no official rules.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  - A. Adoption of technology.
  - B. Evidence.
  - C. Technical training.
  - D. Record-keeping and data management.
  - E. Data privacy.
- **Robotics**
  - A. Energy storage.
  - B. Ethics and security.
  - C. Confidentiality.
- **Wearables**
  - A. Cost of device.
  - B. Battery life.
  - C. Safety, security and privacy.
- **Virtual Assistants (e.g. Alexa)**
  - A. Lack of accuracy.
  - B. Lack of analytical interpretation.
  - C. Data privacy and confidentiality.
- **Mobile Apps**
  - A. Competitive market.
  - B. Promotion and marketing.
  - C. Data management and privacy.
- **Software as a Medical Device**
  - A. Software development lifecycle.
  - B. Product safety and security.
  - C. Data collection, analysis and privacy.
- **Clinical Decision Support Software**
  - A. Development lifecycle.
  - B. Product safety and accuracy.
  - C. Data analysis.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  - A. Lack of precision.
  - B. Lack of interpretation.
  - C. Irregularity in analytics.
  - D. Reliance.
  - E. Transparency and governance.
  - F. Long-term cost.
- **IoT (Internet of Things) and Connected Devices**
  - A. Compatibility of operating systems.
  - B. Identification and authentication of devices and technologies.
  - C. Integration of IoT products and platforms.
  - D. Connectivity.
  - E. Data analytics, security and privacy.
  - F. Consumer awareness.
- **3D Printing/Bioprinting**
  - A. Piracy.
  - B. Misinterpretation of results.
  - C. Lack of training skills.
- **Digital Therapeutics**
  - A. Lack of accuracy.
  - B. Lack of interpretation and understanding.
- **Digital Diagnostics**
  - A. Lack of accuracy.
  - B. Lack of interpretation and understanding.
  - C. Misinterpretation of results.
  - D. Lack of training skills.

- **Electronic Medical Record Management Solutions**
  A. Lack of training skills.
  B. Data collection, analysis and privacy.
  C. Data privacy and confidentiality.
- **Big Data Analytics**
  A. Lack of interpretation and understanding.
  B. Misinterpretation of results.
  C. Lack of training skills.
- **Blockchain-based Healthcare Data Sharing Solutions**
  A. Lack of interpretation and understanding.
  B. Lack of training skills.
  C. Data collection, analysis and privacy.
- **Natural Language Processing**
  A. Understanding of natural language.
  B. Reasoning about multiple documents.
  C. Identification of data and evaluation of problems.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

In general, digital platform providers are preoccupied with the assessment and supervision of the transitional phase of introducing new technologies to the market, as well as the mitigation of risk. Consequently, digital platform providers should prioritise personnel training, understand the importance of market demand and in-line supply, improve IT systems and exhibit strong leadership.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

A fragmented and ambiguous legal and regulatory framework currently governs digital health in India. Additionally, there is a scarcity of legal scholarship on digital health in India. This is particularly challenging because digital health encompasses a wide range of aspects, such as data aggregation and processing, business models and technological advancements. Consequently, the regulatory system is fragmented. In the utilisation and application of personal data, data privacy is of the utmost importance. India implemented the initial EHR Standards in 2013. The importance of international EHR standards in India facilitated their incorporation through the selection of the most qualified candidates. Consequently, healthcare organisations and providers disseminated and made the 2016 EHR Standards paper accessible for deployment in national IT systems. The MoHFW is fostering the adoption of standards, including the Systematised Nomenclature of Medicine-Clinical Terminology in India by providing them at no cost and establishing an interim National Release Centre to oversee the clinical terminology standard. Global healthcare IT stakeholders are gradually acknowledging this standard. The MoHFW is committed to the regulation of the storage and exchange of EHRs, the enforcement of privacy and security protocols for electronic health data, and the promotion and implementation of e-health standards.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Indian law does not control health data management. The IT Act, 2000, and the IT (Reasonable Security Practices and Procedures and SPDI) Rules, 2011, are important laws. The Computer Emergency Response Team, an Indian cybersecurity regulator, has released rules. The rules apply to all body corporates, including sole proprietorships, companies and other professional groupings. Most healthcare providers – hospitals, clinics and independent practitioners – are body corporates and are regulated.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

Research organisations, hospitals and technology service providers are among the entities that are involved in the exchange of information, record-keeping and data collection. Furthermore, these procedures further may be adjusted in response to continuing issues and experiences that arise during the consumer–service provider transition, latency period and linkage.

4.4 How do the regulations define the scope of personal health data use?

These regulations outline the standards for "sensitive health-related information" and "sensitive personal information", setting the extent of information use with the approval of both the beneficiary and the service provider.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

Contracts serve as the most effective method to ensure the confidentiality and concealment of all aspects of the investigation, including the acquisition and utilisation of data, from public view. It is advised that employees and other influential individuals who participate in the research sign personal privacy and non-disclosure agreements. Moreover, if participants breach predetermined contractual obligations, they should have access to a wider range of alternatives. Conversely, there are no specific laws or regulations that govern the collection or utilisation of personal health data.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

It is essential to establish a comprehensive legislative framework that regulates the acquisition and dissemination of personal data in order to resolve concerns regarding data

inaccuracy, bias and/or discrimination. The DPDP Act now regulates the processing of digital personal data in India, irrespective of its original digital or non-digital format before digitisation. Nevertheless, the practical insights are not yet apparent in practice.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

Regulations designed to safeguard sensitive personal data include the EHR Standards for India, 2016, and the IT (Reasonable Security Practices and Procedures and SPDI) Rules, 2011. Disclosures under these regulations are contingent upon consent. The Data Security Council of India has developed the DSCI Privacy Guide for Healthcare, which outlines a range of data categories, including personal health data and information. The National Ethical Guidelines for Biomedical and Health Research Involving Human Participants, the Assisted Reproductive Technology (Regulation) Act, 2021, the ICMR Guidelines for Good Clinical Laboratory Practices, the Telemedicine Practice Guidelines and the Indian Medical Council's (Professional Conduct, Etiquette and Ethics) Regulations, 2002, are additional sector-specific guidelines. The objective of these regulations is to guarantee the privacy and protection of personal health information in India.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Critical legal and regulatory considerations in the exchange of personal data include the adaptability of data collection and transfer, the protection of personal information and privacy during the transformation process, the dissemination of information, trust, responsibility and accountability.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

There is no uniform handling of personal health data sharing regulations, and all the provisions are under the purview of the IT Act, 2000, and the IT (Reasonable Security Practices and Procedures and SPDI) Rules, 2011.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

The total number of participants, patient data and scientific entities significantly influence these critical variables. In addition, the objective of utilising data protection and privacy to expedite the acquisition of answers may affect data sharing, a critical factor that all parties should consider at each stage of the process.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

There are no specific provisions and standard regulations set by the government yet. However, the Indian government has launched the NDHM, which aims to digitise all of the country's medical information. The National Institution for Transforming India (NITI Aayog) has proposed the National Health Stack, a forward-thinking digital platform.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Ensuring data sovereignty, meeting regulatory standards and enhancing trustworthiness are critical concerns for healthcare data sharing.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

India adopted and enacted the Patents Act of 1970, which provides patent protection and complies with the Agreement on Trade-Related Aspects of Intellectual Property Rights. To qualify for patent protection in India, an invention must satisfy the criteria of novelty, innovative steps and industrial applicability and must also be exempt from Sections 3 and 4 of the Patents Act. Section 3(k) of the Patents Act precludes the patenting of a computer program in isolation, as digital health applications are dependent on software and computer programs. Additionally, the Delhi High Court asserted that not all computer programs are exempt from Section 3(k), and that an innovation can receive patent protection if it demonstrates a "technical effect" or "technical contribution". Section 3(i) of the Patents Act says that you cannot get a patent for a program or method that is "a process for the medicinal, surgical, curative, preventative, or other treatment of human beings or any analogous treatment of animals to render them disease-free or enhance the economic value of their products". Nonetheless, the apparatus and methodology for executing an *in vitro* mechanism are eligible for patent protection.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

The Copyright Act of 1957 safeguards intellectual property in India. Copyright safeguards original literary, dramatic, musical or artistic works, cinematographic films and audio recordings. Although copyright registration is not mandatory, it serves as primary evidence to support a legal claim. Copyright laws protect digital health apps and technology, which are fundamentally software, as "computer programs".

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

India lacks a specific statute regulating the management of sensitive information and trade secrets pertaining to digital

health technologies. The emerging digital health sector frequently utilises non-disclosure and confidentiality agreements to safeguard sensitive information.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

The concept of academic technology transfer is still in its infancy in India. The overwhelming majority of enterprises have not adopted this methodology, despite the fact that colleges and certain corporations have established guidelines for the strategic implementation of innovations and the recognition of inventors. The digital health sector is currently in the early phases of intellectual property protection; however, it is experiencing rapid growth, and academic and research organisations are becoming more aware of its significance. It seems that this approach is acquiring momentum and resulting in improved results. The intellectual property of the proposed invention is safeguarded, and the most suitable partner is identified for the licensing and commercialisation of the technology and its functionalities. Additionally, the invention is evaluated for patentability and commercialisation. The dissemination of academic technology is a component of these endeavours.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Section 3(k) of the Indian Patents Act prohibits the patentability of computer programs in general. The Delhi High Court has elucidated that Section 3(k) does not apply to all computer programs, allowing for their patentability if they exhibit a "technical effect" or "technical contribution". Section 3(i) of the Patents Act prohibits the granting of a patent for a program or process that involves "a medicinal, surgical, curative, prophylactic, or other treatment of human beings or any process for a similar treatment of animals to render them disease-free or to increase their economic value or that of their products". The *in vitro* mechanism's apparatus and method of use are patentable.

Since digital health applications are essentially software, Indian law should classify them as "computer programs" and grant them copyright protection. Class 9, which encompasses computer software and computer programs, also allows for trademark registration.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

In India, it is not possible to identify an AI device as the inventor of a patent. The Indian Patents Act and associated patent forms explicitly acknowledge humans as inventors, and they do not apply to AI applications or devices unless explicitly stated.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

There are currently no specific regulations for government-funded inventions.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

There are no specific cases for digital health innovations yet.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

In order to guarantee the success of collaborative improvements, it is possible to evaluate a number of factors, such as the primary objectives of the collaboration, information regarding all eligible members and parties involved, governance and contract management, confidentiality, an evaluation of the current intellectual property and technology transfer procedures, and data on existing intelligence.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

Healthcare and non-healthcare organisations adhere to profoundly distinct workflow methodologies and principles with respect to internal communication and the provision of services externally. However, client fulfilment is the primary concern in both sectors. It is imperative to assess the confidentiality protocol for data exchange, data protection, security and privacy, in addition to the approaches to information sharing, when reviewing agreements.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

It is essential to monitor and analyse the design, consistent protocols for data collection, structured reporting, and advanced methodologies for detecting bias and concealed stratification. Furthermore, it is imperative to execute a non-disclosure agreement.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Companies should avoid integrating sensitive information or personal data into generative AI tools. Data protection regulations may prohibit the input of such data into a generative AI tool, or it may violate a third-party confidentiality agreement. Furthermore, it is imperative to safeguard the privacy of data and its interpretation.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

India currently lacks a regulator with a specific focus on AI/machine learning (ML). As a result, the Ministry of Electronics & Information Technology serves as the executive agency responsible for AI-related strategies and has established committees to establish a policy framework for AI. India has programmes and recommendations for responsible AI development, but no AI legislation exists. The NITI Aayog provides guidelines, and the National Strategy for Artificial Intelligence outlines AI research for various sectors. The DPDP Act was passed in 2023, and the Global Partnership on Artificial Intelligence includes India. Indian authorities are developing AI rules and drafting AI standards, focusing on climate change, global health and societal resilience.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

There are currently no regulatory schemes that are specific to the situation. No specific legislation addresses AI in healthcare. We anticipate that the implementation of the DISHA in India will address certain issues. The legal system, clinicians and patients may interpret the law contextually and hold varying perspectives in the final analysis.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

This is not currently applicable in India. Furthermore, algorithms are not patentable in India.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

The authenticity of licensed data, permission for multiple users and beneficiaries, consideration for purposes such as "know your customer", restriction and limited access across multiple locations and multiple users, data privacy and security, quality, user rights, and term and termination are all important factors to consider.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

There are no specific regulations yet and accordingly the practical insights have yet to come.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Companies should refrain from incorporating sensitive information or personal data into generative AI tools. Data protection regulations may prohibit the entry of such data into a generative AI tool, or it may contravene a confidentiality agreement that was granted to a third party. Additionally, it is crucial to preserve the privacy of data and its interpretation. There are no specific regulations for generative AI yet.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

Though there is no specific model or guidelines yet, the usual rules under data protection are applicable, such as operations that involve these technologies must adhere to standard IT laws and regulations in India, as there are no specific AI, cloud computing or ML regulations. It would be advantageous to establish a confidentiality agreement between the licensee and the data proprietor, as well as a strategy for the data's utilisation.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

The liability for negative consequences may be civil or criminal, and it varies between service providers, such as institutes and internet service providers, and service practitioners. In addition to filing a legal complaint, the Consumer Protection Act can implement its remedies in civil proceedings. In the event of a doctor's negligence, a consumer may also submit a complaint to the ethics committee of the Medical Council of India. The Indian Penal Code, an essential component of digital health solutions, also addresses criminal responsibility.

9.2 What cross-border considerations are there?

It is important to use data programs and customise data.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

The process entails the following: the establishment of work groups to supervise it; the education and training of leaders; the definition of AI policy; the revision of privacy policy; and the execution of security assessments. Confidentiality and privacy should also be maintained.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

There are no specific models/theories yet.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

A persistent concern in the field of digital health is the exorbitant cost of developing and maintaining health information technology, as well as the preservation of confidentiality and privacy when storing data. Another factor to consider is the security and privacy of data management during the different stages of the transformation process.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

It is imperative that non-healthcare businesses comprehend the healthcare industry's commitment to secure manufacturing and marketing standards, as well as its exceptional financial planning and data protection and security measures. Additionally, the healthcare sector is subject to consumer protection laws.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Venture capital and private equity firms should evaluate numerous critical factors prior to investing in digital healthcare enterprises. These encompass a comprehensive business plan, strategic relationships, market opportunities, an understanding of the company's financial and key metrics, potential risk, an estimated valuation, regulatory compliance and intellectual property protection.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The key impediments to the widespread implementation of digital health technology in clinical settings are data interoperability, particularly for health records, data security and privacy.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

Currently, there are no such certifying bodies.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

There are currently no explicit reimbursement standards or formal accreditation for solution providers.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Some of the primary obstacles to the successful implementation of digital transformation in healthcare organisations include data security, resistance to change, high implementation costs and a remote workforce.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

India is anticipated to experience growth in a diverse range of industries, such as genomics, wearables, telemedicine and personalised medicine. Healthcare providers and organisers are adopting advanced technologies, including AI, cloud computing, extended reality and the IoT, in order to create and distribute innovative treatments and services. These technologies facilitate the development of personalised and data-driven medical remedies, as well as improved healthcare delivery and patient experiences. The government is actively building a fully integrated digital health ecosystem.

Digital health records necessitate effortless accessibility without the need for paper. Government initiatives in India, such as the NDHM and Made in India, are accelerating the pace of healthcare digitisation. As the government prioritises digital innovation, healthcare manufacturers and companies will benefit from an increase in opportunities, which will further enhance patient outcomes. The NDHM dedicates itself to developing the necessary infrastructure for the establishment of the nation's integrated digital health ecosystem. The healthcare industry in India is currently experiencing a digital revolution, as evidenced by these patterns. They have the capacity to enhance the delivery of healthcare, patient outcomes and care access. It is imperative to resolve concerns such as infrastructure shortages, data protection, legislative frameworks and equitable access.

Manisha Singh is the Founder Partner of LexOrbis. Manisha is known and respected for her strong expertise in prosecution and enforcement of all forms of IP rights and for strategising and managing global patents, trademarks and designs portfolios of large global and domestic companies. She is also known for her sharp litigation and negotiation skills for both IP and non-IP litigations and dispute resolution. She is involved in a large number of IP litigations with a focus on patent litigations covering all technical fields – particularly pharmaceuticals, telecommunications and mechanics. She is an active member of many associations such as INTA, APAA, AIPLA, AIPPI, LES and FICPI, and is actively involved in their committee work. She is an active writer and regularly authors articles and commentaries for top IP publications.

LexOrbis
709–710 Tolstoy House
15–17 Tolstoy Marg
New Delhi 110001
India

Tel: +91 11 2371 6565
Email: manisha@lexorbis.com
LinkedIn: www.linkedin.com/in/manisha-singh-509b698

Dr. Pankaj Musyuni is an Advocate registered with the Bar Council of India and a Patent Agent. Having over 13 years of experience in handling taxonomy of invention, particularly in portfolio management such as the life cycle of the invention, including preliminary patentability assessment, drafting, filing, prosecution, oppositions and pre-grant representations and leading efforts for understanding requirements of domestic and international clients. Pankaj has experience in handling patent applications in the areas related to chemical, pharmaceutical, agrochemical and biotech domains. He also has experience in handling documentation and assisting in regulatory audits related to GMP, ISO and FDA requirements for the pharmaceutical, veterinary, FMCG and pesticide sectors.

LexOrbis
709–710 Tolstoy House
15–17 Tolstoy Marg
New Delhi 110001
India

Tel: +91 11 2371 6565
Email: pankaj@lexorbis.com
LinkedIn: www.linkedin.com/in/pankaj-musyuni-b34631258

Indonesia


Marshall Situmorang


Andhitta Audria Putri


Mia Sari


Albert Barnabas

Nusantara Legal Partnership

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

While there is no legal definition of "digital health" in Indonesia, the concept of "**Health Technology**" is generally introduced in Law No. 17 of 2023 on Health ("**Health Law**"), and is further implemented under Government Regulation No. 28 of 2024 on the Implementing Regulation of Health Law ("**GR 28/2024**"). These regulations define Health Technology as all forms of tools, products and/or methods to support the diagnosis, prevention and treatment of health problems (e.g. biomedical technology and precision medicine).

Such Health Technology includes providing and facilitating health services (including information on public health, health services and self-services) through telecommunication and digital communication technology or "**tele-health/telemedicine**", which cover: (i) tele-consultation; (ii) tele-pharmacy; (iii) other related services that align with advance science and technology; and (iv) the management of electronic medical records by health providers.

Health Technology also comprises telesurgery in practice, whereby surgery is conducted remotely using robotic technology, and pharmacy/drugs marketplace operation, where drugs are distributed through an electronic system.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

In Indonesia, the use of tele-health/telemedicine in providing health services can be identified as a key emerging digital health subsector.

1.3 What is the digital health market size for your jurisdiction?

No official release of statistics on the digital health market size of Indonesia has been published as of mid-2024. However, data published by East Ventures in 2023 shows that the gross transaction value of health tech startups in Indonesia was estimated to reach USD16 billion (IDR253.8 trillion) in 2023. The figure is projected to rise to reach USD34 billion (IDR539.4 trillion) in 2027. Telemedicine has become the health-tech solution with the highest transaction values reaching around USD11.3 billion (IDR179.3 trillion).

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

Based on data published by *Tech In Asia* in October 2024, Indonesia's largest digital health providers are Halodoc, Alodokter, Good Doctor, Klinik Pintar and Asa Ren. However, there is no publicly available information on the revenues of these companies.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Please see our response to question 1.4 above.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

Below are the relevant authorities in charge of the digital health industry in Indonesia:

a. The Ministry of Health ("**MoH**"), Provincial Health Offices and Regional Health Offices. They are authorised and responsible for the development and supervision of health services including telemedicine.

b. The Ministry of Communication and Informatics (now the Ministry of Communications and Digital Affairs) ("**MoCI**"). Digital health providers and operators are considered as Electronic Services Organisers ("**ESOs**"). As ESOs, digital health industry providers are subject to the MoCI Regulation on Private Electronic System Organizers.

c. The Council of Health Workers in Indonesia (*Konsil Tenaga Kesehatan Indonesia*) ("**KTKI**"). Health providers, including digital health providers, are required to have a Registration Certificate (*Surat Tanda Registrasi*) issued by the KTKI and a Practice Licence (*Surat Izin Praktik*) issued by the MoH.

d. The Food and Drugs Supervisory Agency (*Badan Pengawas Obat dan Makanan*) ("**BPOM**"). The BPOM is authorised to supervise the distribution of drugs.

e. The Ministry of Trade ("**MoT**"). Distribution of drugs through the electronic system can be conducted by ESOs and Electronic Trading System Operators (*Penyelenggara Perdagangan Melalui Sistem Elektronik*) supervised by the MoT.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

Below are the main healthcare regulatory schemes related to digital health in Indonesia:

a. The Health Law.
b. Law No. 27 of 2022 on Personal Data Protection ("**PDP Law**").
c. Law No. 11 of 2008 on Electronic Information and Transactions as lastly amended by Law No. 1 of 2024 ("**EIT Law**").
d. Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transactions ("**GR 71/2019**").
e. Government Regulation No. 80 of 2019 on Trading through Electronic Systems.
f. MoH Regulation No. 20 of 2019 regarding Organization of Telemedicine Services through Health Service Facilities ("**MoH Reg. 20/2019**").
g. MoH Regulation No. 14 of 2021 on Standards for Business Activities and Products in the Implementation of Risk-Based Business Licensing in the Health Sector.
h. MoCI Regulation No. 5 of 2020 on Private Electronic System Organizers as amended by MoCI Regulation No. 10 of 2021.
i. MoCI Regulation No. 20 of 2016 on Protection of Personal Data in Electronic Systems.
j. MoT Regulation No. 31 of 2023 on Business Licensing, Advertising, Guidance, and Supervision of Business Actors in Trade Through Electronic Systems.
k. BPOM Regulation No. 14 of 2024 on Supervision of Foods and Drugs that are Distributed Online.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

In Indonesia, the key area of enforcement in digital health personal data protection is based on the PDP Law. The PDP Law categorises health information and/or data as specific (sensitive) personal data. As such, the law requires any transfer of personal data in health information/data systems be conducted only for one specific and limited purpose upon receiving approval from the MoH, in addition to compliance with the transfer requirements.

Starting from October 2024, the PDP Law became officially effective. Improvements on the enforcement of personal data protection are expected to happen, as the previous law was more lenient in dealing with breaches of personal data protection.

In practice, we noted that the emerging areas of enforcement are related to the use of artificial intelligence ("**AI**") or machine learning ("**ML**"), and tele-surgery for providing health services or diagnoses.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

There are no specific regulations on the application of digital health software for clinical use. However, in practice, private health providers are required to register their software applications to the MoH.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

There are no specific regulations that govern the application of AI/ML-powered digital health devices or software solutions for clinical use. However, AI applications are generally regulated under the EIT Law and GR 71/2019, whereby AI is deemed as an "electronic agent" (a device of an electronic system operated by a person made to automatically perform an action on certain electronic information). In addition, AI applications are also regulated by MoCI Circular Letter No. 9 of 2023, dated 19 December 2023, regarding the Artificial Intelligence Code of Ethics. AI applications are regulated and supervised by the MoCI.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

In handling the evolution of AI/ML application in the future, the Indonesian Agency for the Assessment and Application of Technology (*Badan Pengkajian dan Penerapan Teknologi*) has published the roadmap "Indonesia National Strategy for Artificial Intelligence 2020–2045 – *Strategi Nasional Kecerdasan Artifisial Indonesia 2020–2045*" ("**Stranas KA**"). Based on Stranas KA, the application of AI/ML for medical/health purposes is designated as a priority sector to improve health services through (i) telemedicine (tele-radiology, tele-pathology, tele-dermatology and tele-psychiatry), (ii) maintaining efficient health services (e.g. interoperability of health data), (iii) providing diagnoses, and (iv) developing drugs and medicines that eradicate stunting conditions, detect infectious and non-infectious diseases in the early stages, etc.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Medical/clinical data validation plays a significant role in AI/ML-based digital health solutions as it is defined as sensitive personal data under the PDP Law, which is highly enforced in the application of AI/ML-based digital health solutions, to prevent any breach of personal data rights.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

The Indonesian Government does not distinguish nor differentiate regulations on digital health applied on the national, provincial and/or municipal/regional levels.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

In general, the Indonesian Government has attempted to regulate all aspects of digital health products and solutions by amending the Health Law in 2023 and issuing the

implementing regulations (GR 28/2024 and MoH Regulation No. 20 of 2019 regarding the Organization of Telemedicine Services through Health Service Facilities) to facilitate digital health development in Indonesia.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  The implementation of personal data protection of patients is done by the stakeholders, including health providers. Furthermore, the lack of regulatory provisions relating to telemedicine/virtual care activities has become a growing issue as this field is still developing in Indonesia. Other issues are related to, among others: the accountability and reliability of diagnoses for patients; and the absence of responsibility for health service providers, as they have no doctor–patient relationships.
- **Robotics**
  The unavailability of specific regulations on robotics activities has become the core legal and regulatory issue in this field. Further, no protections can be obtained in performing these robotics activities (i.e. robotic tele-surgeries).
- **Wearables**
  In Indonesia, wearable devices such as smartwatches that have health tracking/information features are common in daily use. These devices are used to provide general information on health. At the time of writing, there are no regulations on the use of such wearables in medical practice.
- **Virtual Assistants (e.g. Alexa)**
  In Indonesia, the use of virtual assistants, including in medical practice, is uncommon. Hence, there are no regulations on the use of virtual assistants in medical practice. Virtual assistants can be considered as electronic agents under the EIT Law.
- **Mobile Apps**
  Most telemedicine operators and medicine distributors provide their services through mobile apps (e.g. Halodok, SehatQ, etc.). These apps are subject to the relevant regulations as mentioned above. The current issues are related to the tele-health industries. No comprehensive implementing regulations serve as the technical regulations on the tele-health industries using mobile apps.
- **Software as a Medical Device**
  There are no specific regulations governing Software as a Medical Device ("**SaMD**"). SaMD faces the same legal issues as mentioned under "Robotics".
- **Clinical Decision Support Software**
  There are no specific regulations governing Clinical Decision Support Software; they face the same issues as mentioned under "Robotics".
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  There are no regulations on AI and ML in general or in the specific health sector. Some issues related to AI/ML have been addressed in our response to question 2.5.
- **IoT (Internet of Things) and Connected Devices**
  IoT and connected devices in the digital health sector provide and collect data for patient monitoring. As such, IoT and connected devices face data protection issues as mentioned under "Telemedicine/Virtual Care".
- **3D Printing/Bioprinting**
  There are no specific regulations governing 3D printing/bioprinting; they are considered to face similar issues as those mentioned under "Robotics".
- **Digital Therapeutics**
  Based on MoH Reg. 20/2019, digital therapeutics can be deemed as other telemedicine consultation services in accordance with the development of science and technology. Digital therapeutics face issues similar to those mentioned under "Telemedicine/Virtual Care" and "Mobile Apps".
- **Digital Diagnostics**
  Digital diagnostics can be deemed as other telemedicine consultation services as explained above. Therefore, they face issues similar to those mentioned under "Telemedicine/Virtual Care" and "Mobile Apps".
- **Electronic Medical Record Management Solutions**
  In Indonesia, the Government has introduced the Health Information System managed by the health services providers at their respective national, provincial and regional levels, integrated into the National Health Information System (*Sistem Informasi Kesehatan Nasional*) ("**SIKN**") for managing patients' data. SIKN serves as a platform on which the One-Data Health Sector (*Satu Data Bidang Kesehatan*) is implemented, which is also integrated into the One-Data Indonesia (*Satu Data Indonesia*) system. SIKN faces data protection issues similar to those mentioned under "Telemedicine/Virtual Care".
- **Big Data Analytics**
  In Indonesia, big data analytics is used in AI/ML application for medical practice. As such, it would face data protection issues similar to those mentioned under "Telemedicine/Virtual Care".
- **Blockchain-based Healthcare Data Sharing Solutions**
  Like big data analytics, blockchain-based healthcare data-sharing solutions are used in AI/ML applications for medical practice in Indonesia. As such, they would face data protection issues like those mentioned under "Telemedicine/Virtual Care".
- **Natural Language Processing**
  In Indonesia, natural language processing correlates with the use of chatbots in providing health services. As such, it would face data protection issues similar to those mentioned under "Telemedicine/Virtual Care".

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

The key legal and regulatory issues of digital health platform providers are, among others: (i) the enforcement of patients' data protection; (ii) that in functioning as a market place, the digital health platform may be responsible for the health providers' negligence (i.e. malpractice, wrong diagnosis, invalid doctors' licences, etc.); (iii) the lack of reliable diagnostics based on virtual consultation with health providers; (iv) the prohibition against certain medical services and the lack of adequate management of patient-owned medical records, creating difficulty in providing suitable healthcare services; and (v) the lack of specific regulations for performing digital health platforms activities.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The enforcement of personal health data protection is mandated in the following regulations: the PDP Law; the Health Law; GR 28/2024; and MoCI Regulation No. 20 of 2016 on Protection of Personal Data in Electronic Systems, especially relating to the breach of personal health data protection.

Based on the PDP Law, the use of personal health data must be based on: (i) an appropriate lawful basis; (ii) purpose limitation; (iii) data minimisation; (iv) accuracy; (v) integrity, security and confidentiality; (vi) lawful retention; (vii) ensuring data subjects' rights; and (viii) accountability.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

The Indonesian Government does not distinguish nor differentiate regulations on personal health data applied on the national, provincial and/or municipal/regional levels.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

In general, the PDP Law categories personal data into general data and specific (sensitive) data, which includes:

a. health information and data;
b. biometric data;
c. genetic data;
d. criminal records;
e. children's data;
f. personal financial data; and/or
g. other data in accordance with provisions of laws and regulations.

"Specific/sensitive data" requires a different procedure. For instance, a transfer of health information and data may be conducted only for one specific and limited purpose based on MoH approval and in compliance with the transfer requirements.

The PDP Law, Health Law and other implementing regulations do not consider the nature or types of the entities (i.e. individuals, companies and public institutions). They only consider the nature of the data. To the extent that it is a data controller or processor, it is subject to these laws and regulations.

4.4 How do the regulations define the scope of personal health data use?

In general, the use of personal health data must go through processing and transfer (data processing). According to the Health Law, data processing includes: (i) planning; (ii) collecting; (iii) storing; (iv) verifying; (v) transfer; (vi) utilisation; and (vii) destroying.

Any use of personal health data must have the prior consent of the data owner.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

In relation to the protection of personal health data, any contractual terms are prepared based on the principles as set out in the PDP Law. The contract, for example, must include, at least:

a. the explicit consent as the basis for data processing;
b. the purpose/scope;
c. the period of processing/retention;
d. the personal data subject's rights (i.e. to claim information, to access or update information, to request for deletion, to have protection from data breach, and other rights); and
e. the intended type of personal data to be processed.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Any inaccuracy shall be verified, rectified and addressed by the data controller. To provide context on the relevant law, the PDP Law regulates that the data controller shall update or fix any inaccurate data no later than three days since the request by the personal health data subject, who is given the notification update. Thus, all issues or problems on the personal health data shall follow the stipulation of the PDP Law.

The PDP Law and Health Law do not specifically address issues on bias and/or discrimination of personal health data.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

In Indonesia, the standard of using and collecting personal health data will be subject to the PDP Law, Health Law and GR 28/2024, as well as other relevant implementing regulations.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The enforcement of personal health data protection is regulated under the PDP Law, Health Law, GR 28/2024 and MoCI Regulation No. 20 of 2016 on Protection of Personal Data in Electronic Systems, especially in relation to the transfer of personal health data to other jurisdictions, in which case it must be ascertained that:

a. the recipient country has an equivalent or higher standard of personal data protection;
b. there is the existence of an adequate and binding personal data protection instrument; or
c. the data subjects' consent is obtained.

Moreover, any transfer of health information and data may be conducted only for one specific and limited purpose and based on MoH approval. The Health Law defines a specific and limited purpose as (i) an extraordinary event response,

(ii) an outbreak/plague, (iii) a pilgrimage, (iv) a material transfer agreement, (v) an international collaboration in the sector, or (vi) any other intended purpose on health data and information.

The regulatory framework is generally agnostic; however, based on MoH Regulation No. 24 on Medical Records ("**MoH Regulation 24/2022**"), medical records can usually only be transferred between healthcare providers. Any transfer to a non-healthcare provider must be assessed on a case-by-case basis.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

The Indonesian Government does not differentiate the applicable regulations on personal health data sharing or medical records sharing applied in national, provincial and/or municipal/regional levels.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Please see our response to question 4.3 above.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

In Indonesia, the standard for sharing personal health data will be subject to the PDP Law, Health Law, GR 28/2024 and other implementing regulations, such as MoH Regulation 24/2022.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

In Indonesia, "federated models" in the practice of healthcare data sharing is relatively unknown. Generally, any healthcare data sharing is subject to the PDP Law and Health Law, including their implementing regulations. The issue at hand is similar to our response to question 5.1.

The closest example of health data sharing in Indonesia is SIKN. As previously mentioned, SIKN serves as a platform on which the One-Data Health Sector (*Satu Data Bidang Kesehatan*) is also integrated into One-Data Indonesia (*Satu Data Indonesia*).

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Patent protection in Indonesia is determined by Law No. 13 of 2016 on Patents as lastly amended by Law No. 65 of 2024 ("**Patent Law**"), whereby an invention should be novel, inventive and industrially applicable to be eligible for patent protection. In general, computer programs cannot be patented. However, based on a recent regulation, inventions that can be installed into a computer (i.e. computer software/program), and involve the use of problem-solving processes, can be patented. For example, GPS navigation programs, automatic vehicular distance-control programs and remote electrical connectivity programs.

Therefore, to the extent that a digital health technology contains a computer program/software that is utilised to solve a problem, it can be patented and protected based on the Patent Law.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Law No. 28 of 2014 on Copyright ("**Copyright Law**") defines copyright as an exclusive right that automatically arises to the creator, based on the declarative principle after a "Creation" is manifested in a tangible form without restriction in accordance with the laws and regulations.

The Creation, as elaborated above, also includes computer programs as they are deemed protected creations under the Copyright Law. Considering that digital health technology mainly comprises usage of computer programs, it may be protected under the Copyright Law.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Law No. 30 of 2000 on Trade Secrets ("**Trade Secret Law**") defines a trade secret as information undisclosed to the public pertaining to technology and/or business that has economical value to a company. Trade secrets are not required to be registered with any government institution, as it is naturally sensitive and confidential information. Trade secrets can, however, be assigned by the owners to another party in the form of a licence, under an agreement or a contract.

To the extent that digital health technology contains a confidential trade secret, it may be protected under the Trade Secret Law. In practice, the owner can enter into a licence agreement with another party using it, and obtain protection from non-disclosure clauses or a separate non-disclosure agreement.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

In Indonesia, the prevailing law regarding academic technology transfer is Government Regulation No. 20 of 2005 on Transfer of Intellectual Property Technology and Result of Research and Development Activities by Universities and Research and Development Institutions. This regulation emphasises the role of universities, Research and Development institutions, as well as the Government to transfer the intellectual property technologies for the purpose of disseminating and developing public understanding on science and technology.

A transfer of intellectual property technology can be conducted through licence agreements, cooperation, publication, and Science and Technology services. Moreover, the Government may own the intellectual property rights under the condition that the transfer is funded by the Government.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Please see our response to question 6.1.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

This matter has been discussed among practitioners and legal experts in technology. AI (specifically generative AI) can be considered as the person that can be named as the inventor of a patent. On the other hand, AI can also be deemed as the object of invention and hence cannot be designated as an inventor, with the consideration that AI is not a human. In general, it is acknowledged that intellectual property is a property that arises from human intellectual abilities, not a computer program imitating a human.

In light of the above, there are currently no specific regulations on the legal standing of AI in Indonesia.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

Please see our response to question 6.4.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

There are currently no key precedential legal cases or decisions on this matter.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

To affirm their legal standing, parties need to have the capacity to enter into an agreement, comply with the laws and regulations, not be involved in litigation or bankruptcy cases, and have the adequate coverage of services, time period, dispute settlement and indemnity.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

Please see question 7.1 above.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Parties must comply with the PDP Law and Health Law, including the rules and regulations on data security and have no cases of infringement of personal data (including personal health data), and consider the ownership of the intellectual property rights associated with the use of federated learning healthcare data sharing.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Parties must comply with the PDP Law and Health Law, including the rules and regulations on data security, and have no cases of infringement of personal data (including personal health data) occur, and consider the ownership of the intellectual property rights associated with the use of generative AI.

In addition, parties must comply with the rules and regulations on the use of generative AI, adopt the prudential principles, have the security and integration of information technology systems, have the security control over the electronic transaction activities, be cost-effective and efficient, and provide the consumer protection in accordance with the applicable laws and regulations.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

Please see our response to question 2.5 above.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

Please see our response to question 2.5 above.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

As this field is still being developed, intellectual property rights associated with AI/ML are not yet regulated.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

The important considerations in any commercial contract of licensing data for use in AI/ML are, among others: (i) the compliance of the processed data with the PDP Law and Health Law, including the rules and regulations on data security and prohibition on infringement of the personal data (including personal health data); and (ii) the ownership of the intellectual property rights associated with use of AI/ML.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

At the time of writing, there is no distinction of applications overseeing AI/ML technologies in general.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

As it is being developed, there is the argument that "generative AI" can be deemed as a legal subject, instead of an object. This argument is supported where AI is within the interpretation of an "electronic agent" under the EIT Law. The law defines an electronic agent as a device in an electronic system that is made to take any action on electronic information in an automatic way by a person. The phrase "automatically by a person" can be interpreted as natural persons or legal entities. Further, there remains the issue on the form of intellectual property rights of AI in general due to the undefined status of AI as a legal subject/object; therefore, it is currently unknown which forms of intellectual property can be assigned to their products (patent, copyright, trademark or industrial design).

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

Despite the lack of specific regulations on AI/ML, any inappropriate data collecting or processing will become subject to the PDP Law and Health Law. Failure to secure personal data (including personal health data) is subject to the following administrative sanctions:

a. a written warning letter;
b. temporary suspension of data processing activity;
c. removal or destruction of personal data; and/or
d. an administrative fine in the maximum amount of 2% of the annual income or annual revenue of the violation variable.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

No theory of liability specifically defines the adverse outcomes in digital health solutions. However, as a data controller, a digital health solution provider is liable for the security of personal health data through the implementation of organisation and technical measures to protect personal data from disruption. A data controller is also responsible for deciding the security level of personal data by considering the nature and risks, and using a reliable, secure and responsible electronic system.

In general, any failure to secure personal data (including personal health data) is subject to the administrative sanctions as mentioned above in question 8.7.

9.2 What cross-border considerations are there?

The PDP Law applies on an extraterritorial basis, hence any data processing outside Indonesia will have legal consequences within Indonesia's jurisdiction and/or to Indonesian health data subjects/owners outside Indonesia.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Please see our response to question 9.1.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Please see our response to question 9.1.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

The key issues mainly concern the enforcement of personal health data protection, especially with regard to data storing and transfer activities, as to whether it has been made with sufficient and lawful written consent of the personal data subjects/owners. As there are no specific regulations on cloud-based services for digital health, data storing and transfer will be subject to the PDP Law and Health Law.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

The key issues would revolve around securing the relevant licences and maintaining the regulatory compliance as a digital health provider (i.e. ESO registration, MoH registration), especially those relating to the personal health data protection.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

The key points that must be considered before investing in digital healthcare ventures are, among others: (i) the sufficient licences, approvals and permits in establishing the company and conducting the business; (ii) the competency and experience of key persons and management; (iii) the cooperation of existing shareholders; (iv) no outstanding significant liabilities; (v) no outstanding and/or potential material dispute; and (vi) an adequate system or operational policies in managing the company on a day-to-day basis (e.g. compliance policies, IT policies, personal data protection policies, etc.).

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

From our understanding, the main barriers for the implementation of digital health solutions in Indonesia are, practically: access to internet; computing abilities; technology familiarity; physical (non-digital) medical records and personal data; literacy of personal health data protection; lack of implementing regulations of digital health solution practice; and insufficient enforcement of cyber security.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In Indonesia, the key certification body that influences digital health solutions is the KTKI. In 2020, the KTKI issued Regulation No. 74 of 2020 concerning Clinical Authority and Medical Practice Through Telemedicine during the COVID-19 pandemic in Indonesia.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

Reimbursement models are an uncommon practice in Indonesia. However, there is current discourse that such reimbursements/incentives provided by the Government can be integrated into the expenses covered by the national health security program, known as *BPJS Kesehatan*. For private insurers, we are not aware of any similar business models being made available.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Considering that digital health is a developing field in Indonesia, it is difficult to assess the possible gaps in the healthcare ecosystem for analysing digital health solutions, except relating to enforcement towards breaches of data protection/security.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

According to the Blue Print of Digital Health Transformation 2021–2024, the expected improvements in this sector are, among others: integrated health data on an individual basis; simplification and digitalisation of health services; and development and support in the health innovation ecosystem. Following the recent Prabowo-Gibran Presidential Cabinet's Inauguration in October 2024, there may be possible policy changes in the future relating to digital technology in the health sector.

Marshall Situmorang is the founding partner of Nusantara Legal Partnership. He regularly advises Global Telecommunication Services Providers and Global Tech Sourcing Companies on various regulatory issues, IT contracts, compliance, data protection/privacy, payments, cloud data, tech sourcing, payments, supply chain transactions, licensing and interconnection.
Marshall also has particular expertise in various sectors, including logistics, financial services, digital media, marketing and communications, food and beverage, and consumer goods. Marshall's clients are household names, multinationals, technology majors and Indonesian conglomerates. He has spent more than 14 years working in private legal practice.

Nusantara Legal Partnership
Sampoerna Strategic Square, North Tower, Level 14
Jl. Jend. Sudirman Kav. 45-46, Jakarta Selatan, 12930
Indonesia

Tel: +62 21 5098 0355
Email: marshall.situmorang@nusantaralegal.com
LinkedIn: www.linkedin.com/in/mss3008

Andhitta Audria Putri (Audria) is an Indonesian-qualified lawyer and an experienced legal professional focusing her practice on TMT (Telecommunication, Technology and Media), M&A and general corporate practices. Audria has extensive experience in various legal works of providing regulatory and compliance advisory and advising clients in personal data protection compliance, as well as representing and advising clients in M&A transactions. Audria has acted for various clients of major technology companies, venture capital firms, early-to-late-stage start-ups, Indonesian and Southeast Asian unicorns, telecommunication companies and payment system providers, as well as fintech and multinational companies in various sectors.

Nusantara Legal Partnership
Sampoerna Strategic Square, North Tower, Level 14
Jl. Jend. Sudirman Kav. 45-46, Jakarta Selatan, 12930
Indonesia

Tel: +62 21 5098 0355
Email: audria.putri@nusantaralegal.com
LinkedIn: www.linkedin.com/in/audria-putri-5bb8a044

Mia Sari is an Indonesian-qualified lawyer and an experienced legal professional focusing her practice on capital market, M&A and general corporate practices including public listed companies and other financial service companies. She has many years of experience handling matters relating to Indonesia's Financial Services Authority (OJK) and is very familiar with OJK laws and regulations.
Before joining the firm, she worked for almost 10 years at Hiswara Bunjamin Tandjung, an associated firm of Herbert Smith Freehills, with her latest position being the Senior Associate of Capital Market Practice Group.

Nusantara Legal Partnership
Sampoerna Strategic Square, North Tower, Level 14
Jl. Jend. Sudirman Kav. 45-46, Jakarta Selatan, 12930
Indonesia

Tel: +62 21 5098 0355
Email: mia.sari@nusantaralegal.com
LinkedIn: www.linkedin.com/in/mia-sari-60687797

Albert Barnabas is a Trainee Associate with extensive experience in the legal field over the last three years of his legal career, providing support in a variety of legal matters pertaining to legal research and counterparty negotiations, as well as litigation proceedings for a variety of cases and client matters. Albert has assisted various clients, both local and international, in a wide range of legal matters from workers' rights to unpaid wages and investment in hydroelectric infrastructure, to shipping insurance disputes and criminal defence for embezzlement.

Nusantara Legal Partnership
Sampoerna Strategic Square, North Tower, Level 14
Jl. Jend. Sudirman Kav. 45-46, Jakarta Selatan, 12930
Indonesia

Tel: +62 81 1143 0313
Email: albert.barnabas@nusantaralegal.com
LinkedIn: www.linkedin.com/in/albert-barnabas-65b629214

Nusantara Legal Partnership ("**NLP**") is a premier boutique law firm based in Jakarta, Indonesia. Established in 2018, we thrive on providing in-depth advisory and representation in a comprehensive range of legal services tailored to each client across all industry sectors.
Our team consists of highly skilled lawyers with proven experiences and having the ability to cater to the clients' legal needs.
NLP provides services in the following core practices: General Corporate & Commercial Law; Mergers & Acquisitions; Foreign Direct Investment; Banking, Finance & Fintech; Technology, Media & Telecommunication; Labour, Employment & Industrial Relations; Property & Real Estate; Insurance; Pharmaceutical; Intellectual Property; and Commercial Litigation & Dispute Resolution.

NLP has been recently named as one of Indonesia's Law Firms to Watch in 2023 by *Asia Legal Business*, and has been acknowledged as one of the up-and-coming and emerging boutique law firms in Indonesia.
www.nusantaralegal.com

Nusantara Legal Partnership

Israel


Adv. Eran Bareket


Adv. Alexandra Cohen

Gilat, Bareket & Co., Reinhold Cohn Group

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no general definition of "digital health" in Israel. However, the definition can be derived from the government's "National Digital Health Plan as a Growth Engine" approved on 25 March 2018, which defines digital health as follows: "*The vision of the digital health strategy as published by the Ministry of Health is to enable a leap in the healthcare system so that it will be a sustainable, advanced, innovative, renewable and constantly improving health system, by leveraging the best available information and communication technologies.*"

In the framework of a Supervisory Report on the digital health sector issued by the Privacy Protection Authority ("PPA") in 2024, the term "digital health" was defined as referring to the integration of technology into healthcare services to improve the delivery of medical services, diagnosis, treatment and monitoring of patients' health conditions.

Although there is no legal definition, the digital health sector is very developed in Israel and there are hundreds of innovative companies – including start-ups – dealing with digital health and developing technologies in different digital health sectors. The Ministry of Health ("MOH") established a division dealing with digital health, which is aimed at implementing innovative technologies and improving the quality of treatment, medical services and economic efficiency. Collaborating with governmental partners, the division is engaged in crafting a robust digital health ecosystem. This ecosystem is designed to foster synergies among health organisations, industry stakeholders and academia, fostering innovation and advancement in the realm of healthcare.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

The key emerging technologies in digital health in Israel include digital tools and platforms that enable consumers to proactively track, manage and treat their own medical conditions, as well as digital tools of remote monitoring, decision support, clinical workflow, diagnostics, patent engagement and assistive devices.

For example, ContinUse Biometrics Ltd. is an Israeli company that developed methods using artificial intelligence ("AI") techniques for nano-level detection and analysis of vibrations associated with the movement of internal organs and molecules. This technology enables the continuous measurement of vital signs and other bio-parameters (such as heart and respiration rates and blood pressure) from a distance and with high accuracy.

1.3 What is the digital health market size for your jurisdiction?

According to the Startup Nation Central Finder Annual Report for 2023, Israel's health tech sector accounts for 22% of the ecosystem, with over 1,600 companies – making it the largest sector in the Israeli ecosystem by company count. The sector showed relative resilience in the first three quarters of 2023 compared to the second half of 2022, maintaining around $0.4 billion in private funding per quarter. However, there was a decline in Q4, attributed to the war that began on October 7, which impacted all markets similarly – except for the medical devices subsector, where private funding remained stable and did not decline.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

Private companies are not required to publish their financial results; therefore, there is no detailed information regarding the revenue of private digital health companies in Israel. However, based on the *Calcalist* article "*Full list of Israeli high-tech funding rounds in 2024*", several Israeli healthcare companies secured significant funding rounds in 2024, underscoring the sector's resilience and innovation. Notable examples include:

1. **Insightec**: In June 2024, Insightec raised $150 million to enhance its MRI-guided focused ultrasound technology for treating neurological disorders.
2. **CytoReason**: In July 2024, CytoReason secured $80 million in a funding round led by Nvidia and Pfizer to advance its AI-based disease modelling platform.
3. **Magenta Medical**: In August 2024, Magenta Medical raised $105 million to develop its heart pump technology, aiming to compete with established players in the cardiac device market.
4. **Scopio Labs**: In July 2024, Scopio Labs secured $42 million in a Series D funding round to advance its digital microscopy solutions for haematology.
5. **Sensi.AI**: In June 2024, Sensi.AI raised $31 million in a Series B funding round to expand its audio-based monitoring solutions for elderly care.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

As mentioned above, private companies are not required to publish their financial results; therefore, there is no detailed information regarding the revenue of private digital health companies in Israel.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The principal regulatory authorities enforcing regulatory schemes related to digital health in Israel are:

- The MOH – responsible for registration and marketing approvals, regulates the approval of clinical trials and regulates secondary use of health data. In addition, uses of health data and collaborations involving health data are also regulated and monitored by the MOH.
- The PPA – regulates maintenance of databases containing personal data (including health data) and enforces privacy requirements for the use of such data. The privacy protection commissioner has enforcement authority in cases of unauthorised use of data. In 2024, the PPA released a Supervisory Report on the digital health sector, evaluating entities providing digital health services across three main criteria: organisational control and corporate governance; data repository management; and data security. The report found that most entities demonstrated a high level of compliance in these areas.
- The courts have jurisdiction over all issues.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

In Israel, the core healthcare regulatory schemes related to digital health include:

- Healthcare and patient rights: National Health Insurance Law (1995); Patients' Rights Law (1996); and the Public Health Ordinance, 1940.
- Medical devices and technology: Medical Devices Law (2012); and the MOH Director General circulars.
- Privacy and data security: Protection of Privacy Law (1981); and Data Security Regulations (2017).

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

Since the field is new and not comprehensively governed by Israeli legislation, it is still unclear how enforcement of legislation governing the digital health industry will evolve.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

Software medical accessories and devices ("MADs") are registered by the MOH as medical accessories, e.g., CoroFlow Cardiovascular Measurement System & Accessories (software that assists in measuring flow changes in coronary arteries), as well as Insulin Insights (measurement software for diabetes patients). Other medical devices were once registered as software MADs, such as 3D medical image processing, simulation and design software or Neurosurgical Navigation Software.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

In Israel, there is no specific regulation dedicated exclusively to AI/Machine Learning ("ML")-powered digital health devices or software solutions. However, such devices are generally regulated under existing medical device laws and standards, such as the Medical Devices Law, 2012, overseen by the MOH Medical Devices Division.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

The MOH is adapting its regulatory framework to address the dynamic nature of AI/ML-based digital health solutions through several key initiatives:

- Guiding Principles for AI-Based Technologies: During 2023, the MOH published guidelines aimed to establish good ML practices for digital medical technologies (see here: https://www.gov.il/en/pages/digital-medical-technology-gmlp-1).
- Alignment with International Standards: The MOH is aligning its regulations with evolving international standards, such as those from the European Union, to ensure that Israel's regulatory framework remains current and effective. For example, the Health Information and Cyber Security Division of the MOH published a document on 30 April 2022, requiring healthcare organisations in Israel to comply with ISO 27001 and ISO 27799 standards for information security as a condition for obtaining and maintaining a licence from the MOH.
- Support for Innovation in Digital Health: Through programmes like the Support Program for Innovation in Selected Fields – Digital Health, operated jointly by the Innovation Authority, the MOH and the Headquarters for the National Digital Israel Initiative, the MOH supports Research and Development ("R&D") and pilot projects in digital health, fostering an environment conducive to the development and implementation of AI/ML solutions (https://innovationisrael.org.il/en/programs/support-program-for-innovation-in-selected-fields-digital-health/?utm_source=chatgpt.com#about_route).

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation data plays a critical role in regulatory approval for AI/ML-based digital health solutions in Israel. Products must demonstrate efficacy and safety through robust clinical studies to meet the requirements of the Medical Devices Division of the MOH.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In Israel, digital health products are regulated centrally by the MOH, with no differential regulation at state or regional levels.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

In recent years, Israel has started addressing digital health specifically in official publications. For example, the PPA issued guidelines to ensure telehealth services comply with privacy and data protection laws, safeguarding patient information during remote consultations.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  It is to be noted that the MOH has not yet published any guidance regarding the technologies below, creating vagueness for the entities active in the digital health field:
  - Regulation, ethics and jurisdiction of medical practice – the issue arises when practitioners are outside the country's jurisdiction.
  - Liability of misdiagnosis – the risk of misdiagnosis increases when medical services are provided without doctor supervision.
  - Health data privacy – collection, use and security standards for health data.
  - Software and hardware validation.
- **Robotics**
  Robotic technologies are considered as emerging technologies in the field of medicine, generally used for performing human surgical/medical operations. The incorporation of new technologies, such as AI or Internet connections in robotics, enhance the performance and flexibility of this technology.
  In Israel, the company Yaskawa developed medical rehabilitation robots, which help maintain the body's quality of movement and function, rehabilitate from injuries, wounds and traumatic events and maintain daily functioning.
  XACT Robotics also developed a robot designed to perform a variety of invasive medical operations such as biopsy, ablation (catheter insertion), drainage and medication in specific areas of the body.
- **Wearables**
  Unlike other devices, wearable devices are always close to the user and thus have additional data collection capabilities (walking and pulse rate, for example). Furthermore, most wearable devices are also capable of operating without the Internet and thus the scope of data collection is greater, as is the concern of leaking sensitive information. Examples of wearable devices developed in Israel are:
  - Orcam – a wearable assistive AI device for the blind and visually impaired, that instantly reads text, recognises faces, identifies products and much more.
  - Hip-Hope of Hip-Hope Technologies – a smart wearable device, designed as a belt, worn around the user's waist. A proprietary multi-sensor system detects impending collision with the ground. Upon detection, two large-size airbags instantly inflate and protect the wearer's hips. Fall alert notifications are automatically sent to pre-defined destinations.
- **Virtual Assistants (e.g. Alexa)**
  Since virtual assistants collect a broad spectrum of data about their users, they get a more complete, accurate and in-depth picture of the user. In view of this, the data is extremely sensitive, and any leakage may jeopardise the user's privacy, as is the case with wearables. Hence, the same general considerations apply.
- **Mobile Apps**
  Mobile apps are quite similar to wearables and virtual assistants and therefore raise similar issues. Moreover, mobile phone apps can incorporate additional hardware features (such as fingerprint, voice recognition or various sensors) that are integrated into the mobile device.
- **Software as a Medical Device**
  This technology raises at least two main questions:
  1. Can medical device software provide medical treatment? When does provision of medical information constitute medical treatment?
  2. When is medical device software classified as a medical device, as defined in the Medical Equipment Law, 5772-2012, thereby requiring to be MAD-registered?
- **Clinical Decision Support Software**
  Clinical decision support systems are currently being developed by various start-ups in Israel. At the time of writing, there is no regulation that sets conditions for the implementation of such systems. Some key issues are the need to convince physicians of the reliability of the system on the one hand and the need to prevent over-reliance on the system on the other hand.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  While systems that specialise in a particular field may support human judgment or serve as a basis for analysing a specific patient's case and determining a physician's findings, there are specialist systems that completely replace human judgment, namely, to simulate professionals' behaviour, by using ML. The K system, for example, is a personalised medical information search app designed to replace medical information Internet searches that are not individually customised. The system provides relevant information according to the case, while mentioning that such information is not a diagnosis or medical advice, and that medical attention should be sought if the symptoms are severe.
- **IoT (Internet of Things) and Connected Devices**
  Please see "Wearables".
- **3D Printing/Bioprinting**
  The 3D printing field is a flourishing industry in Israel, used, *inter alia*, for the manufacture of hearing and surgical aids, dental models and physical models of organs, as well as living cellular products and tissues, some of which are medically approved for human contact and transplantation.
  It is estimated that Israel is the manufacturer of approximately 40 per cent of all 3D printers worldwide, and more than 1,400 Israeli companies dedicated to life sciences. For example, the company Synergy3DMed designs and prints customised 3D models and surgical instruments.

Recently, Tel Aviv University researchers used a 3D bio-printer to create a heart that includes real cells, blood vessels, ventricles and chambers. Another example is the collaboration between Israel's CollPlant Biotechnologies and the US-based United Therapeutics Corporation to begin the production of 3D-printed kidneys.

While this technology significantly contributes to the development of healthcare, *inter alia*, by reducing global organ shortages, the different reactions of individuals to 3D-printed organ transplantations may raise an issue as to the efficiency of such organs.

- **Digital Therapeutics**
  The digital therapeutics sector, which includes software-driven medical interventions that provide validated, evidence-based treatments for a range of physical and mental health conditions, constitutes a significant portion of Israel's digital health industry. For example, Theranica, which specialises in wearable devices for migraine relief, integrating neuromodulation and smartphone technology, developed Nerivio, a remote electrical neuromodulation wearable for migraine treatment and prevention.
- **Digital Diagnostics**
  Digital diagnostics constitute part of the outputs arising from using digital technologies. The data used by digital diagnostics is collected from various sources, such as the user's electronic health records, medical imaging and real-time patient-generated data from wearables, requiring interoperability standards. It is essential to ensure that digital diagnostic tools can seamlessly integrate with existing healthcare systems and technologies. EFA Technologies developed the RevDx, a mobile end-point solution for performing automatic microscopy tests, including whole blood sampling and an automatic diagnosis of blood count. Ibex developed Galen, a clinical-grade, multi-tissue platform that helps pathologists detect and grade breast, prostate and gastric cancer, along with more than 100 other clinically relevant features.
- **Electronic Medical Record Management Solutions**
  The large access to electronic medical records based the need for digital systems designed to store, manage and retrieve user health data in order to provide the user with a comprehensive view of his data. Legal considerations arise in terms of the ownership of electronic medical records and the provision of access to third parties, demanding scrutiny and resolution. InvenTech developed HSM, a cloud-based clinic management system.
- **Big Data Analytics**
  Big data analytics is integrated into digital technologies through a large variety of means such as predictive analytics or clinical decision support systems (for example, the K system mentioned above) and constitutes an important part of the digital healthcare field.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Blockchain-based healthcare data sharing solutions allow exchange of data among healthcare providers, insurers, researchers and other stakeholders, leading to more efficient and timely healthcare services. For example, Brya developed a platform allowing hospitals, clinics and health systems to seamlessly and safely access and exchange data with researchers and life sciences.
- **Natural Language Processing**
  Natural language processing may be used as part of ML activities applied to electronic health records, whether text or audio. Usage of this technology is not regulated or standardised in Israel, and there are no provisions regarding its application in digital healthcare.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Among the various goals defined in the government's "National Digital Health Plan as a Growth Engine" is the goal to create a national digital platform for the purpose of sharing health data. However, this goal has not yet come to fruition. One of the issues in this regard is the data holders' willingness to share their data to the national central database and to agree to revenue-sharing arrangements that will allow research on data originating from multiple sources.

- Problems of uniformity and standardisation also arise, since different bodies collect the data and classify the types of data stored in their databases in different ways.
- Privacy protection of the data shared through the digital platform, including its security, is also a key issue.
- Obligation to present medical data to the patient (in accordance with the provisions of the Director-General ("GD") circular on patient access to personal health data, "*Healthcare under your Control*").

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The main legal and regulatory issues that must be taken into account at the time of using personal data are: ownership of data; scope and nature of the independent use and sharing of the data (including compliance with GD circulars regarding secondary uses of and collaborations based on health data and with the Medical Information Mobilization Law, 5784-2024, when sharing personal data between various health organisations); and privacy protection of the data (including compliance with the Protection of Privacy Law, 5741-1981). See further below.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In Israel, personal health data is regulated through the Privacy Protection Law, 1981, with no differential regulation at state or regional levels.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

Health Maintenance Organisations ("HMOs"), the entities holding most of the health data in Israel, are subject to strict regulation. For example, HMOs are limited in holding equity in start-ups and cannot invest the money generated by using health data other than for the advancement of treatment, medical service, public health or scientific research in the

health field. Privacy regulations apply always, regardless of the nature of the entities.

4.4 How do the regulations define the scope of personal health data use?

Circular provisions prohibit the use of health data for purposes that do not serve the advancement of treatment, medical service, public health or scientific research in the health field. Health data should also not be used for inappropriate social purposes, with an emphasis on discrimination in insurance or employment.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

The main key contractual terms to consider are: ownership of data; ownership of know-how products based on collaborations through which data is used; consideration for data sharing or know-how products based on use of the data, such as ownership in the outside organisation (if a company is concerned); right to use the know-how products; monetary compensation (such as royalties, licence fees and exit fees); period of use of the data; exclusivity of the data's use; reach through royalties/licences; royalty rate and stacking; and the need to use other databases.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

According to the Protection of Privacy Law, 5741-1981, a person may request the owner of a database (or the possessor thereof as applicable) to amend or delete data about himself that is not correct, not complete, not clear or not up to date. If the owner of the database refuses to comply with such request, the person requesting the amendment or deletion of his data may appeal to the Magistrate's Court, as regulated under the Privacy Protection Regulations (Conditions for Reviewing Data and Rules of Procedure for Appealing Refusal of Review Requests), 5741-1981. In addition, the Privacy Protection Regulations (Instructions Regarding Information Transferred to Israel from the European Economic Area), 2023, includes a duty of data accuracy, according to which the database owner must implement a mechanism – organisational, technological or otherwise – to ensure that the information in the database is correct, complete, clear and up to date.

The circular regarding collaborations based on secondary uses of health data, published by the GD of the MOH in January 2018, prohibits the use of health data for improper social purposes, with emphasis on discrimination in insurance or employment. According to this circular, a collaboration agreement shall include a provision that allows the health organisation to cancel or suspend the agreement if the CEO of the MOH orders so due to a violation of one of the guidelines set forth in the circular, including the prohibition to use health data for discrimination purposes.

It is worth noting that the World Medical Association Declaration of Helsinki sets forth provisions aimed to protect the health and rights of the subjects participating in medical research. For example, the declaration states that medical research involving a disadvantaged or vulnerable population or community is only justified if the research is responsive to the health needs and priorities of this population or community and if there is a reasonable likelihood that this population or community stands to benefit from the results of the research.

In addition, ISO 27799:2016 provides guidelines for medical organisations in order to ensure that the level of security used maintains the integrity, confidentiality and availability of health data.

As to bias, there is no express regulation.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The laws determining standards for using and collecting personal health data include the following:

1. The Protection of Privacy Law, 5741-1981, establishes the legal basis for safeguarding personal data in Israel.
2. The Protection of Privacy Regulations (Data Security), 5777-2017, set organisational mechanisms to integrate data security into the management routines of all entities processing personal data.
3. MOH GD circulars, such as: the Secondary Use of Health Data Circular (17 January 2018), which regulates the use of health data for non-medical purposes, ensuring that any secondary use is de-identified unless otherwise specified by law or approved through explicit opt-in consent; the Collaborations Based on Secondary Uses of Health Data Circular (17 January 2018), which provides guidelines for collaborations involving secondary health data use; and the Patient Access to Personal Health Data: "Healthcare Under Your Control" Circular (11 November 2019), which empowers patients by granting them access to their electronic health records, promoting transparency and patient engagement.
4. The Medical Information Mobilization Law, 5784-2024, enacts to facilitate the sharing of health data between health organisations; this law establishes standards for data interoperability and patient consent, ensuring that data exchange occurs securely and with respect for patient privacy.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The main legal and regulatory issues that must be taken into account at the time of sharing personal data are: ownership of data; scope and nature of the independent use and sharing of the data (including compliance with GD circulars regarding secondary uses of and collaborations based on health data and with the Medical Information Mobilization Law, 5784-2024, when sharing personal data between various health organisations); and privacy protection of the shared data (including compliance with the Protection of Privacy Law, 5741-1981).

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In Israel, personal health data sharing is regulated uniformly at the national level, with no differential regulation at the state or regional levels.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

HMOs, the entities holding most of the health data in Israel, are subject to strict regulation. For example, HMOs are limited in holding equity in start-ups and cannot invest the money generated by using health data other than for the advancement of treatment, medical service, public health or scientific research in the health field. Privacy regulations always apply, regardless of the nature of the entities. If the personal health data is shared between health organisations, the Medical Information Mobilization Law, 5784-2024, applies.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

During 2024, the MOH published a new plan aimed at establishing the infrastructure for implementing Fast Healthcare Interoperability Resources ("FHIR") standard interoperability in the healthcare system, in accordance with the provisions of the Medical Information Mobilization Law, 5784-2024.

In addition, the MOH has implemented a range of cutting-edge systems and infrastructures to facilitate the seamless exchange of healthcare data and enhance health promotion in Israel. The key initiatives include:

- The Innovative Healthcare Data Sharing System, which is a pioneering system facilitating the exchange and transfer of healthcare data among HMOs and hospitals.
- The "Tamna" system (Research Infrastructure for Big Data), which is a national platform dedicated to conducting extensive big-data research on health data. Data shared with researchers is anonymised, ensuring it remains untraceable and cannot be cross-referenced with other data that may lead to subject re-identification.
- The "Psifas" system (mosaic), which is a national platform with the overarching goal of advancing health in Israel by establishing and overseeing a comprehensive data infrastructure and biological sample repository for personalised medicine research. This collaborative initiative, managed through inter-university cooperation, includes vital partners such as HMO Klalit Health Services and its medical centres (Rabin, Carmel, Soroka and the Valley), along with medical centres Sheba, Ichilov, Sha'are Zedek and Hadassah.

The GD circulars regarding secondary uses of and collaborations based on health data set standards should also be mentioned. For example, the GD circular on secondary uses of health data states that the medical data shared for secondary use will be de-identified and sets detailed conditions for privacy, medical confidentiality and data security. This circular prohibits use for improper social purposes, with emphasis on discrimination in insurance or employment.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

The key issues to consider with respect to federated models of healthcare data sharing include the following: ownership of the federated shared data; the consent of the data subjects to federate and share such data and the scope of access granted; the privacy and security of the data, the standardisation of data, its quality and integrity; the trust and transparency among the data providers and users; and the legal and ethical frameworks for data sharing across different contexts, collaboration and innovation among the data stakeholders.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

The Patents Law, 5727-1967, shapes the scope of patent protection for digital health technologies by defining the criteria for patentable inventions. According to the law, a patentable invention must be a product or process in any area of technology that is novel, involves an inventive step, and is capable of industrial application. However, the law specifically excludes certain types of inventions, such as processes for human medical treatment, though diagnostic and veterinary methods are not excluded.

Additionally, discoveries, scientific theories, mathematical formulas, game rules and computer software *per se* are not patentable, as clarified by case-law precedents. However, if an invention addresses a technological problem with a technological solution – whether the solution involves software or not – it may be deemed patentable.

There is no specific legislation tailored to digital health technologies in Israel. Each application in this field is evaluated based on its individual merits under the general framework of patent law.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Copyright protection is governed by the Copyright Law, 5768-2007. Copyright law protection may be particularly relevant to software and certain compilations of data, but there is no protection of databases *per se*.

As of 2018, icons, graphical user interfaces and screen presentations are not protected by copyright but rather by the Designs Law, 5777-2017. Non-registered designs are protected for three years, and registered designs are protected for up to 25 years. There is no specific legislation applicable to digital health technologies. Consequently, the scope of protection for such technologies depends on how their components align with the existing frameworks for software, data compilations and design protection.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secret protection is governed by the Commercial Torts Law, 5759-1999, which defines a trade secret as "*business*

information, of all kinds, which is not in the public domain, is not easily disclosed by others lawfully, and whose confidentiality affords its owners a business advantage over competitors, provided that reasonable steps are taken to protect its confidentiality". This definition applies broadly, including digital health technologies. The law prohibits the misappropriation of trade secrets, which includes: (1) taking a trade secret without the owner's consent through improper means, or using the secret obtained this way; (2) using a trade secret without the owner's consent in breach of a contractual obligation or duty of trust; or (3) acquiring or using a trade secret knowing it was unlawfully obtained under (1) or (2). It should be noted that disclosure of a trade secret through reverse engineering will not, in itself, be regarded as improper.

Health data is a classic example of a trade secret due to its proprietary nature and potential to provide a competitive edge, but there is no specific legislation applicable to digital health technologies. This lack of specificity underscores the importance of implementing robust internal measures (e.g., access controls, encryption) to secure trade secrets in the digital health sector.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Israel is very active in this area and has been a world leader since the 1960s. All main academic institutions operate a tech transfer unit experienced in granting product-use licences and obtaining equity and/or royalties from commercialising products based on them.

Every academic institution has Intellectual Property ("IP") bylaws. Such bylaws bind the employees of the institution (including the researchers) by virtue of appropriate provisions in their employment agreements. Some institutions also require students to subject themselves to these bylaws. In general, academic institutions require ownership of any IP generated in the framework of the institution, and various provisions grant the inventors a certain share in the revenues of the academic institution's commercialisation company. It is common practice for the academic institutions that if the institution is not interested in patenting the technologies, then the inventors can own the IP in exchange for a revenue-sharing agreement with the academic institution.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Computer software is protected by copyright, and no specific reference is made to the software of a medical device. However, copyright protects a method of expression only; thus, protection over functionality requires patent protection. The limitations of copyright and the complexity of patenting software create challenges for comprehensive protection.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

This question was discussed in Israel in the framework of the examination of the patent applications nos 268604 and 268605, in which an AI machine (DABUS) was listed as an inventor. The Patents Registrar decided that an AI machine, claimed to have conceived the invention, lacks eligibility as an inventor, and thus cannot bestow patent ownership upon itself (Patents Registrar Decision regarding Patent Applications nos 268604 and 268605 of Applicant Dr. Stephen Thaler (15 March 2023)). The ruling is currently under appeal.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

The Law for the Encouragement of Industrial Research and Development, 5744-1984, establishes the Israel Innovation Authority ("IIA") (formerly the Office of the Chief Scientist), which provides, *inter alia*, funding platforms to various entities such as: early-stage entrepreneurs with technological initiatives; mature companies developing new products or manufacturing processes; and academic groups seeking to commercialise their ideas and turn them into revenue-generating products/services.

The government, through the IIA, typically funds up to 50% of the costs of development projects, including IP protection. There is no need to return the funding, unless the research generates revenue, and then the funding is returned by way of royalties.

In addition, IP developed through funding of the IIA should be exploited in Israel and cannot be transferred to a foreign entity without receiving prior permission from the IIA. While the government does not directly own the IP, it exercises control over its commercialisation and transfer, particularly regarding exploitation outside Israel. These restrictions aim to safeguard national interests and promote economic growth within the country.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

Since there is no specific legislation or landmark decisions tailored to digital health, the generally applicable laws and case law establish the framework for protecting digital health innovations (see question 6.1 above).

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

In general, the following points should be addressed:

- The R&D phase: responsibilities of the parties; goals; deliverables; and regulatory approval process. Technical details of access to data (whether copies will be made, or the data remotely accessed) and anonymisation thereof.
- IP: ownership and licences to background and foreground IP; and responsibilities and duty to collaborate in the enforcement of foreground IP.
- Arrangements for revenue sharing of commercialisation of the collaboration results: royalty bases; rate; definition of net sales; dilution; stacking; term; milestone payments; audits; and the like.

More considerations include: exclusivity; term of the agreement; anonymisation of the data; implications of the duty to call back; and opt in *v.* opt out.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

Agreements with public healthcare companies require special attention be given to the regulatory environment of the healthcare entity (e.g. an HMO).

- Public-regulated healthcare entities are limited in their ability to hold equity in non-healthcare companies.
- Public-regulated healthcare entities are restricted in their ability to accede to requests for non-compete/exclusivity arrangements.
- Healthcare organisations involved in the development of new technologies will typically consider implications on the operations, such as the duty to call back, the cost of adding a new technology to their basket of services, etc.
- In addition to access to data, healthcare organisations may serve as an alpha site for the development of new technologies.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

In addition to the points mentioned above (question 7.2), when dealing with federated learning healthcare data sharing agreements between companies, the following points should be addressed: ownership of the federated shared data; the consent of the data subjects to federate and share such data and the scope of access granted; the standardisation of the data; adherence to all pertinent healthcare regulations and the seamless integration of such compliance into operational frameworks; technical infrastructure compatibility for federated learning and agreement allowing future adaptability; and the liability scope of the parties.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

The considerations parties should take into account when dealing with the use of generative AI in the provisioning of digital health solutions include the following:

- IP – the content created by generative AI models may be similar or identical to existing contents protected by IP rights such as copyrights, trademarks and patents, raising questions of ownership and infringement. In light of the current case law in Israel, since an AI machine cannot be considered as inventor, the matter of ownership should be considered and addressed.
- Data privacy – since generative AI models use large amounts of data (including personal and sensitive data) to train and generate content, parties using generative AI must ensure compliance with all privacy protection laws and proper security measures in order to avoid any unauthorised access, misuse or theft.
- Content regulation – parties using generative AI must ensure that the contents generated by AI models are not harmful, misleading, offensive or illegal. In addition, the parties should ensure that the content they generate or distribute is accurate, authentic and ethical, including with regard to algorithmic bias and fairness.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

There is no specific regulatory authority dedicated to enforcing AI/ML-related regulatory schemes. The courts have jurisdiction over disputes or enforcement matters across all sectors.

For AI/ML products in digital health, regulatory oversight typically falls under the purview of health sector authorities and is addressed by applicable medical device or healthcare laws (see question 2.1 above).

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

See question 8.1 above.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Ownership of an enhanced AI/ML algorithm without human intervention may occur in respect of any of the following: the machine; the owner of the machine; the programmer of the code; the data scientist who created the algorithm; or the medical doctor who assisted in the characterisation of the algorithm.

Israeli law does not regulate the ownership of IP created by ML, and this should be regulated in collaboration agreements. However, it is generally accepted that the company conducting the research will have the rights to the resulting products, including their IP rights. It is important to note that in Israel, if the invention is a method in the field of healthcare (such as precision medicine), two problems arise: (1) a patent shall not be granted for a procedure for a therapeutic treatment on the human body (section 7 of the Patents Law); and (2) discovery, scientific theory, mathematical formula, game instructions and thought processes shall be considered abstract ideas or processes of a technical nature.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Some of the main commercial contractual and strategic considerations are:

- Restrictions on licensing: privacy laws may limit licensing rights, especially for sensitive data like healthcare records. De-identification is often required.
- Use and control of data: the permitted use should be defined and misuse prevented (e.g., unauthorised disclosure). Ownership of AI/ML outputs should be addressed.
- Remuneration models: fixed payment or revenue sharing of revenues received from exercising the licence; in the latter case, agreeing on the royalty base may sometimes be challenging.

- Data security and compliance: compliance with privacy laws should be ensured, particularly for healthcare data.
- Healthcare-specific considerations: in some cases, healthcare data should be anonymised.

In healthcare, stricter regulations and ethical implications require tailored agreements to address these challenges effectively.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

As of December 2024, Israel does not have specific regulations that distinguish between standard AI and generative AI technologies. The country's approach to AI regulation is characterised by a general framework that applies to all AI systems, without explicit differentiation between various types of AI technologies.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

The legal issues that are unique to generative AI technologies include the following: ownership (who is determined as the owner of AI-generated content – creators of the AI, the operators, the end-users that generate outputs?); copyright; privacy (generative AI models are often trained on large datasets, including personal data, which can conflict with privacy laws); ethical issues (generative AI can be used to create disinformation, harmful content and deepfakes); bias (generative AI systems can perpetuate or amplify biases present in training data). According to the Ministry of Justice's opinion from December 2022, except in exceptional cases, the use of copyrighted materials for the purpose of ML falls under fair use and therefore does not constitute a copyright infringement. However, the opinion does not make definitive determinations regarding the output of ML.

While Israel does not yet have generative AI-specific legislation, ongoing national initiatives and global collaborations aim to create a robust regulatory environment that balances innovation with ethical and legal responsibilities, such as:

- National AI strategy – In December 2023, Israel published its Policy on Artificial Intelligence Regulation and Ethics, underscoring a commitment to responsible innovation and addressing challenges associated with AI deployment across various sectors (https://www.gov.il/en/pages/ai_2023?utm_source=chatgpt.com).
- Global collaboration – Israel has engaged in international agreements on AI governance, such as signing the Council of Europe's AI Convention. This commitment aligns Israel's regulatory standards with global human rights and democratic values, ensuring that AI technologies, including generative AI, are developed and utilised responsibly (https://www.gov.il/en/pages/ai2024?utm_source=chatgpt.com).

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

In Israel, there are no specific laws or regulations directly addressing trained AI/ML models that include data for which the developer lacks appropriate rights. In such case, this issue would likely be governed under general property or IP (if proprietary or copyrighted data is used without authorisation), contract (if developers violate contractual obligations) and privacy laws (if personal data is used without proper consent).

Israel does not currently have explicit data disgorgement laws requiring the removal or destruction of AI/ML models built on improperly acquired data. However, courts have the authority to issue remedies in legal disputes, such as orders to cease the use or distribution of such models, delete improperly acquired data or provide financial compensation. Additionally, under the Unjust Enrichment Law, 5739–1979, if a party gains a benefit or service without legal entitlement, they may be obligated to make restitution of the benefits or its value, which could apply in cases involving improperly used data.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

There is no specific legislation on digital health; hence, general tort law applies. This includes, primarily, the tort of negligence and the regime of strict (no fault) liability under the Defective Products Liability Law, 5740-1980. Breach of contractual warranties may also come into play.

9.2 What cross-border considerations are there?

The laws of Israel are in principle limited to its territory. However, actions conducted outside the country's borders may be subject to the jurisdiction of Israeli courts if the foreign entity collaborated with a local entity, remotely provided service to recipients located within the territory, and possibly also when damages occur or are expected to occur in Israel.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

According to the Ministry of Justice's opinion, the use of content protected by copyright for the purpose of training a machine will be permitted even without obtaining the approval of the owners of the rights in the content. However, if generative AI ventures beyond training digital health technologies, it is advisable to adopt the following measures to mitigate potential legal complications: using content from databases wherein the content owners have granted explicit consent for such usage; employing technologies designed to minimise the probability of generating infringing content; adhering to pertinent healthcare regulations to ensure compliance with industry standards and legal requirements; implementing and maintaining sufficient administrative, technical and physical safeguards; documenting the development and the decisions taken with regard to the technology; including liability clauses in agreements with third parties; and establishing clear terms and responsibilities.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

In Israel, misuse of healthcare data in AI/ML models used in digital health solutions can give rise to liability under the following laws:

1. The Privacy Protection Law, 1981: since healthcare data is deemed sensitive information, unauthorised use or inclusion in AI/ML models without explicit consent breaches privacy and may lead to civil liability or enforcement by the PPA.
2. Copyrights: While raw healthcare data itself is not protected by copyright, the specific way in which this data is organised, curated or presented – such as in a database or a structured dataset – can be protected. According to the Ministry of Justice's opinion from December 2022, except in exceptional cases, the use of copyrighted materials for the purpose of machine training falls under fair use and therefore does not constitute a copyright infringement. In cases where the structure of the dataset significantly influences the outputs of the AI/ML model, there may be grounds to argue that the outputs constitute infringement.
3. Trade Secrets: Healthcare data can qualify as a trade secret due to its proprietary nature and its ability to provide a competitive advantage. The use of such data for training AI/ML models without the rightful owner's consent, or when improperly acquired or utilised, may be subject to legal remedies under the Commercial Torts Law, 1999.
4. Torts: Misuse of healthcare data in AI/ML models could be analogised to violations of ownership and possession rights under laws protecting property, such as sections 15–20 of the Real Estate Law, 5729-1969. If entities exercise unauthorised control over data, similar to a "holder" misusing property, they may face liability. In addition, the Movable Property Law, 5731-1971, supports extending these principles to healthcare data, treating it as intangible movable property, thereby reinforcing protections against misuse under privacy and contractual frameworks.
5. Patient Rights Law, 1996: Using patient data in AI/ML without informed consent breaches medical ethics and legal obligations.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

When using Cloud services, questions arise regarding the privacy and security of the data uploaded to the Cloud and its security.

When the Cloud is located outside of Israel, questions arise regarding the authority to transfer such data outside the country's borders. The Privacy Protection Regulations (Transfer of Personal Information to Databases Outside the State Borders), 5761-2001, set out conditions for transferring data abroad; for example, the party the data is transferred to must undertake to comply with the conditions for data retention and use applying to a database located in Israel (section 2 (4) of the Regulations).

In July 2019, the MOH authorised, for the first time, hospitals and healthcare organisations to use Cloud services. Alongside the benefits of using Cloud services (such as digital medicine upgrading and cutting back on computing costs), there is concern regarding stealing patient medical data and the risk of cyber-attacks.

Oracle recently decided to set up a data centre in Israel, which will include two Cloud servers: one designed for the government and security forces, with a particularly high level of security; and the other for the business sector, including corporate clients, as well as start-ups.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

The digital healthcare market's landscape is in constant flux and there are many areas of uncertainty, not to mention that it may vary among countries. Thus, partnering with an institution with experience in the field is advantageous. Special care must be paid to the regulatory schemes applicable to both the R&D stage as well as the commercial marketing and sales stage.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

The arrival time of a large part of digital medicine technologies (such as smart apps and medical devices) is significantly short (unlike in pharmaceuticals where the arrival time may take years).

The following are key factors that should also be considered:

- Maturity of the venture's product.
- Time to market ("TTM") (generally speaking, in digital health technologies TTM may be significantly shorter than in past traditional industries).
- Background of founders and major managers (serial entrepreneurs with proven track records are highly sought after).
- Collaboration with strategic partners (for example, having a leading HMO as a commercial partner or as the alpha site provider).
- Scope of required investment and expected return.
- Characteristics of the product's market and commercial and regulatory IP challenges.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

There are no specific key barriers in Israel, but rather general key barriers that may be relevant in other jurisdictions as well and include, *inter alia*, the following: regulatory requirements in the targeted market (which are evolving and constantly taking shape and form); the characteristics of the targeted market/population; the need to cooperate with additional entities (strategic partners); etc.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The sole clinician certification body in Israel is the MOH. The decision whether to adopt digital health solutions is dependent on clinical benefit and cost-effectiveness, regardless of the technology.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

The Israeli market is different from the American market, since it is nationalised – namely, most of the health services are provided by HMOs, which are budgeted by the State. The services provided by the HMOs (including services, drugs, medical equipment and devices) are those that are included in the "health basket". The "health basket" is based on the health services that were being provided by the Clalit HMO as of 1 January 1994 and the health services that were provided by the MOH as of 31 December 1994. Once a year, new drugs and medical technologies are added to the "health basket" following approval by the MOH and subject to additional budgeting allocated for this purpose by recommendation of a public committee. The decision regarding which drugs and medical services are to be added to the "health basket" are made based on clinical benefit and cost-effectiveness, regardless of the technology. It is to be noted that some digital technologies, especially applications, are not regulatorily defined as MADs, which is a basic condition for the inclusion of a technology in the "health basket". Nonetheless, the "health basket" includes digital technologies such as CGM systems (continuous glucose monitoring) or smart pacemakers.

The health insurance market, however, is completely private, and each company determines the terms of the reimbursement.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Due diligence gaps in the healthcare ecosystem for analysing digital health solutions, particularly those involving data-driven products like AI/ML-based solutions, can arise due to the complexity and novelty of these technologies. These gaps typically include:

- **Regulatory Compliance**: In general, there is often a lack of understanding of applicable regulatory frameworks (e.g., FDA, EMA, HIPAA and GDPR) and unclear pathways for approval or certification due to evolving regulations. For AI/ML models, the adaptive nature of these technologies creates additional challenges in meeting regulatory standards, particularly as regulations lag behind advancements.
- **Data Privacy**: General gaps include insufficient assessment of compliance with data protection laws (e.g., GDPR and CCPA) and inadequate measures for securing sensitive healthcare data. For AI/ML models, additional concerns arise regarding sourcing of training data, obtaining informed consent, data anonymisation and ensuring the prevention of algorithmic bias.
- **Clinical Validation**: Many digital health solutions lack rigorous evaluation of their efficacy, safety and real-world performance. For AI/ML models, limited validation of their robustness, generalisability across diverse population, and adaptability to new clinical scenarios is a common shortcoming.
- **Bias and Transparency**: General digital health solutions may overlook ethical considerations, such as equitable access and fairness in outcomes. For AI/ML models, there are additional risks of algorithmic biases and disparities, often due to underrepresentation in training datasets, which can lead to unequal outcomes.
- **Cybersecurity**: General gaps include weak evaluations of data security measures and resilience against breaches. For AI/ML solutions, these gaps extend to vulnerabilities in the handling of training data and protecting models from adversarial attacks.
- **IP**: General ambiguities arise regarding ownership of co-developed digital health solutions or datasets. For AI/ML models, unclear ownership of algorithms, training datasets and derivative insights can create legal and operational conflicts.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

It is worth noting that the PPA published in August 2022 a document detailing the challenges of privacy protection involved in the use of telemedicine services. The document maps the types of remote medical services currently provided in Israel, reviews the risks to patients' privacy when using telemedicine services, summarises legal provisions and relevant guidelines and presents clarifications and recommendations regarding the manner in which telemedicine services should be used in order to reduce the harm of patients' privacy (including collection, documentation, storage and processing). While the recommendations are not mandatory, companies interested in entering the digital healthcare market should be aware of these recommendations and ensure that they are applied by the telemedicine services suppliers.

Adv. Eran Bareket holds an LL.B. degree, 1990, from Tel-Aviv University and teaches in leading Israeli universities.
Eran's expertise is in litigation, in particular: IP rights; unjust enrichment; competition law and complex litigations, particularly those involving technology issues; and management of multi-jurisdiction IP litigations.
Eran has vast experience appearing before all Israeli courts, including the Patents, Designs and Trademarks Registrar. He is well versed in the fields of: IP; high technology; technology transfer and licensing; digital health; big data licensing; competition law; agency and distributorships; regulatory law (pharmaceuticals/medical devices); defence and homeland security; and governmental companies.
Eran is often involved in the Israeli Parliament (*Knesset*) legislative process, acting on behalf of various entities. He serves as a consultant for IP matters to the Accountant General's Division of the Ministry of Finance and represents the government regarding disputes surrounding inventions by state employees (service inventions).
Eran is continuously commended by leading international guides.

Gilat, Bareket & Co., Reinhold Cohn Group
26A Habarzel St.
Tel Aviv, 6971037
Israel

Tel: +972 3 567 2000
Email: eranb@gilatadv.co.il
LinkedIn: www.linkedin.com/in/eranbareket

Adv. Alexandra Cohen holds an LL.B. degree, 2016, from Tel Aviv University.
Alexandra handles various aspects of IP rights, including patents, trademarks and copyrights, and represents clients in litigation proceedings before Israeli courts and the Registrar of Patents, Designs and Trademarks. Alexandra's expertise extends to various patent litigations across different sectors, including the pharmaceutical industry, serving a diverse clientele both locally and internationally. She also provides services with respect to commercial law, licence agreements and privacy issues. Additionally, she has contributed to several guides, particularly in the areas of patents, trade secrets, digital health and privacy.

Gilat, Bareket & Co., Reinhold Cohn Group
26A Habarzel St.
Tel Aviv, 6971037
Israel

Tel: +972 3 567 2000
Email: alcohen@gilatadv.co.il
LinkedIn: www.linkedin.com/in/alexandra-cohen-502b192a7

Reinhold Cohn Group (RCG) is the leading IP consulting firm in Israel. RCG offers a full breadth of IP-related services and expertise including protection, asset management, due diligence, and litigation & legal services. The firm operates in all areas of IP such as patents, trademarks, designs, copyrights, open source, plant breeders' rights, etc.
The group includes the patent attorneys firm, Reinhold Cohn & Partners, and the law firm, Gilat, Bareket & Co.
The synergy of patent attorneys experienced in a diverse spectrum of technological and scientific disciplines working alongside legal professionals, creates a unique and effective platform for maximising the value of a client's IP assets by securing optimal protection.
RCG and its team of professionals are internationally renowned for excellence and continually ranked amongst the top tiers in leading international and local guides.

gilat-bareket.rcip.co.il

Gilat Bareket Attorneys at Law | Reinhold Cohn Group

Italy


Sonia Selletti


Claudia Pasturenzi

Astolfi e Associati, Studio Legale

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

A legal definition is not provided by Italian law; however, "digital health" can be defined as the use of information and communication technologies in the health sector for the purposes of prevention, diagnosis, treatment and monitoring of diseases (in compliance with the definition provided by the World Health Organization). The term also takes on a larger significance than that of the medical-therapeutic field, including the use of lifestyle and wellness technologies.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

In Italy, the practical applications implemented to date in part or in full as regards digital health are the online sale of (non-prescription) medicinal products, the health card, electronic medical prescriptions, reservations for online healthcare services (through the *Centro Unico Prenotazioni*), electronic health records (EHRs) (Ministerial Decree of 7 September 2023 introduced the "electronic health records 2.0", in order to ensure the spread of and the access to data and documents in the national territory by both patients and healthcare professionals (HCPs)), digitalised reports, telemedicine and teleconsultation.

For improving patient care and rendering healthcare services more efficient, the use of digital technologies should be implemented, such as medical apps, the Cloud, artificial intelligence ((AI) including chatbots), robotics in surgical interventions, virtual-reality systems for the simulation of complex surgical interventions and bionics.

In 2023, *Anitec-Assofarm* (the Italian Association for Information and Communication Technology) published the white paper "A vision of the future for digital healthcare", which analyses the market situation with particular attention to the issues that companies are facing in the sector of health technologies.

The white paper highlights that AI solutions are increasingly being used in the healthcare sector and the growth of AI and blockchain is higher than the growth of the Cloud; whereas digital twin and clinical decision support systems represent technological instruments of the future.

1.3 What is the digital health market size for your jurisdiction?

The continuing technological acceleration in the Italian healthcare system is part of a socio-economic context that had been moving along this path – albeit at a different speed – for years; a situation clearly reflected in the introduction of EHRs or the first regulations governing telemedicine.

In 2023, the digital health market in Italy exceeded 2.3 billion euros, with significant growth due to the spread of solutions such as telemedicine and electronic medical records. Telemedicine is one of the key areas, adopted by 72% of Italian healthcare facilities, while data integration and advanced digital strategies are the focus of about 80% of the regions, which are committed to improve access to and management of digital health information.

Growth projections for digital health in Italy remain positive, also due to the support of public–private partnerships aimed at adopting new technologies, such as AI and health data analytics.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

Among the digital health companies with a more relevant market, we could mention Philips Healthcare, Reply, Dedalus Italia S.p.A., Healthware Group, Artexe S.p.A., Afea S.r.l., AlmavivA S.p.A. and Maticmind S.p.A.

We should add that the digital health ecosystem is also populated by numerous start-ups with innovative, high-performance proposals, who successfully obtain the approval, economic and otherwise, of other more structured organisations, as well as of State/regional authorities to begin operating at territorial level.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

In Italy, digital healthcare is seeing significant growth in response to the need to innovate health services, and some companies are distinguishing themselves by expanding their activities, mainly thanks to funds from the National Recovery and Resilience Plan (PNRR).

We do not have direct information on the fastest growing digital health companies in our jurisdiction but, as far as we know from the public access sources, we can include: Dedalus Group; Telbios; Healthware Group; and Exprivia-Italtel.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The main healthcare regulatory authorities in Italy are: the Ministry of Health, as the promoter and implementing body and controller of initiatives aimed at the development of digital health both at an EU and national level, through coordination that serves to guide and optimise efforts and resources made available by all stakeholders; the Ministry of Economy and Finance, responsible for planning public expenditure and verifying its progress; the Ministry of the University and Research, promoting research; and the Privacy Authority, as the controller of the application of Regulation (EU) 2016/679 (GDPR) and the Privacy Code and guarantor that the processing of personal data is compliant with the fundamental rights and freedoms of individuals. Although this is not an authority with an assigned role in health IT issues, the Ethics Committee can play an important role with reference to projects (including clinical trials) using digital/new health technologies. In Italy, the Ethics Committee may serve as a consultation body for any ethical health-related issues as well as a guarantor of the rights, safety and well-being of the subjects involved.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

In Italy, the regulation of digital health is governed by different regulatory schemes.

In particular, the main regulatory schemes are Regulations (EU) 2017/745 (MDR) and 2017/746 (IVDR) and national decrees no. 137/2022 and 138/2022 on medical devices cover traditional devices and software such as medical devices (Software as a Medical Device (SaMD)), imposing strict requirements in terms of quality and safety.

The protection of personal data is regulated by the GDPR and the Italian Privacy Code (Legislative Decree 196/2003).

Anti-kickback rules govern the financial relationships between healthcare workers and medical device companies, with the National Anti-Corruption Authority tasked with preventing unethical practices and ensuring transparency.

In the area of national security, the National Cybersecurity Agency is responsible for protecting healthcare infrastructures from cyber-risks, particularly considering the ever-increasing value of health data, applying cybersecurity laws, including Legislative Decree no. 138/2024, which transposed the Directive 2022/2555 (so-called NIS2).

The EU Regulation on Artificial Intelligence (AI Act, Regulation (EU) no. 1689/20024) introduces specific requirements for AI systems used in healthcare, including SaMD. That said, the first essential step is to assess if and when software falls within the definition of a medical device.

To complement this regulatory framework is the bill "Provisions on digital therapies", currently under discussion, which aims to include digital therapies in the National Health System. If passed, this law will officially recognise digital therapies as therapeutic tools, improving the regulatory framework and facilitating access and patient safety in the context of digital care.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The factors that may slow down the "take-off" of digital health in Italy constitute the "mirror" of the areas for intervention and improvement. The intervention areas are:

- investment programmes to train dedicated HCPs – both the new generations and the already active health workers – an increasing number of universities offer courses on the subject and continuing medical education is an important way to spread knowledge and develop culture;
- management of the social and relationship-based aspects with patients and caregivers to reassure that the required assistance and care are ensured despite the use of new tools: this fosters efficiency and promotes quality; and
- development of culture, and education on the use of digital health technologies to patients, caregivers and patient associations; it is important to engage in information, keeping in mind that patients are increasingly "experts" and "demanding" interlocutors, while also being vulnerable subjects suffering from an illness, with a desire to recover.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

SaMD is governed by the MDR, IVDR and by the following local decrees that have been issued to complete the framework: no. 137/2022 (adaptation to the MDR); and no. 138/2022 (adaptation to the IVDR). Such rules, *inter alia*, recognise the possibility to sell medical devices online (within certain limits).

The competent authority in this sector is the Italian Ministry of Health.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

In addition to the laws and regulation already mentioned above, the only specific regulation on this matter is the AI Act. There are no specific local laws regarding AI/machine learning (ML)-powered digital health devices or software solutions and their approval for clinical use.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Regulatory authorities are adapting their traditional approval schemes to better address the dynamic nature of AI/ML-based digital health solutions. The Italian Medicines Agency (AIFA) and the Ministry of Health have begun exploring frameworks for more agile assessments, recognising the need to evaluate digital health tools as they evolve through continuous updates.

Key efforts include developing guidelines and best practices that consider real-world data and performance monitoring as part of post-market surveillance, acknowledging that AI/ML solutions often undergo changes that impact their functionality and efficacy.

Moreover, the Italian Data Protection Authority has been particularly active in addressing data privacy challenges related to AI, with a focus on ensuring compliance with GDPR principles. The authority has issued opinions and guidelines on the processing of health-related data through AI systems as well as through websites and apps aimed at putting into contact patients and HCPs.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation data plays a critical role in the regulatory considerations for AI/ML-based digital health solutions in Italy. This data is essential to demonstrate the safety, efficacy and performance of AI-driven technologies, which may adapt and evolve in real-time as they interact with data inputs. Italian regulatory authorities, aligning with European frameworks like the MDR and AI Act, require evidence of clinical validation to ensure that AI/ML algorithms consistently deliver accurate and reliable outcomes across diverse patient populations and in different healthcare settings.

Data-driven validation helps establish trust with healthcare providers and end-users by ensuring transparency and minimising risks associated with bias or inaccurate predictions.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Digital health products and solutions are primarily governed by national-level regulations that align with broader European directives and frameworks, such as the MDR and GDPR. These regulations are enforced and implemented by national bodies, such as the Italian Ministry of Health, AIFA and the Italian Data Protection Authority. However, certain aspects of healthcare services and the practical application of digital health initiatives may be subject to regional regulations and oversight.

Italian Regions have the authority to implement healthcare regulations, including digital health solutions, at a regional level, in order to address local needs, infrastructure capacities and healthcare priorities. For instance, Regions may establish specific protocols for telemedicine, EHRs and other digital services to reflect the unique demands and resources of their populations. While national regulations set the broad framework, regional healthcare bodies may influence how these standards are applied in practice, resulting in some variations in the accessibility, governance and operation of digital health solutions across different regions.

This dual regulatory approach ensures both consistency in meeting essential safety, efficacy and data protection standards, while allowing flexibility to cater to localised healthcare challenges. On the other side, it can also be difficult to meet all the different requirements provided for on a regional level, for example when cross-regional data sharing or interoperability of digital solutions is involved.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Regulatory enforcement actions for digital health products and solutions are evolving to keep pace with technological innovation and the increasing complexity of these tools. Enforcement is primarily guided by overarching European regulations, such as the MDR and GDPR, with Italian authorities like the Ministry of Health, AIFA and the Italian Data Protection Authority playing key roles in ensuring compliance. Tailored actions have focused on both pre-market approval and post-market surveillance to manage risks, promote patient safety and ensure adherence to data protection standards.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  The main legal issue is the need of a prior authorisation for the performance of healthcare activities. On this point, telemedicine initiatives have received support from case law, which has recognised that non-purely health activities that pertain to broader telemedicine projects (such as the collection of health data through patient/technology interaction with subsequent sending to a physician for reporting) are not subject to the prior authorisation required by Italian legislation for the performance of healthcare activities (Supreme Court, criminal section, decision no. 38485/2019).
- **Robotics**
  The use of robots in the healthcare sector (in the surgical and rehabilitation field, implantable robotic systems, robotic pharmaceutical cabinets and "social" robots, already used in some hospitals, etc.) requires:
  - continuous software updates and maintenance to remedy malfunctions that can lead to multiple issues related to liability; and
  - protection from risks related to hacking, deactivation or erasure of robotic memory.

  Openness to this technology requires the adequate training of health professionals as well as exhaustive information to patients, in order to comply with the rule of informed consent for the service, which is an expression of the principle of the inviolable freedom of choice of each individual.
  The main legal issue regarding the use of this healthcare technology is connected to the individuation of responsibilities in case of damages occurred to patients.
- **Wearables**
  The core legal issues related to the use of wearables in the healthcare sector are connected to the management of security and the protection of information collected in compliance with confidentiality and data protection laws and the qualification of certain instruments as medical devices to ensure the application of the relevant legislation.
  Additional knowledge is needed from the user and the physician, and a culture based on scientific evidence must be spread in order to gain awareness as regards actual use.

- **Virtual Assistants (e.g. Alexa)**
  The main issues connected to this technology consist of the management of the large amount of data and the liability of subjects involved in their creation and use.
  Often, this software will process users' data in order to divide them into groups according to their behaviour. This activity falls within the definition of profiling, hence it is necessary to take the precautions provided for by current legislation. This also helps to prevent a violation of the principle of non-algorithmic discrimination, which requires the data controller to use appropriate profiling procedures and adopt suitable technical and organisational measures to minimise the risk of error. In this regard, the Italian Privacy Authority has adopted the 2015 Guidelines (still applicable to the extent compatible with the GDPR).
  Privacy legislation applies also with reference to geolocation systems, which are often used by Virtual Assistants.
- **Mobile Apps**
  There are many apps used in the health sector, which offer a wide, constantly evolving range of updated content: wellness and fitness apps; apps for time management (e.g. reminder apps); management apps (e.g. geolocation apps for services and professionals); and apps for self-diagnosis and diagnosis assistance (e.g. apps for measuring eyesight, apps for interpreting laboratory test results), etc.
  The main issues concern the legal classification of the apps (notably, whether they fall within the definition of a medical device), as well as the processing of the enormous amount of data.
  With reference to apps for illness management or diagnosis support, it will also be essential to provide adequate information to the patient and physician.
  As regards data processing, the Italian Authority for the Protection of Personal Data expressed important indications for their correct management.
- **Software as a Medical Device**
  Software that falls within the definition of a medical device must comply with applicable legislation on the matter. While many different software currently fall into risk class I (affixing the CE marking without the intervention of the notified body), the MDR establishes stricter rules that may potentially lead to an increase in the risk class, with the consequent involvement of the notified body.
  The correct qualification of the software is the first step to properly approach the market: a mistake in its qualification can damage the idea. The regulatory process is equally important; it is recommended to have the support of experts and local advisors.
  Correct management of personal data and responsibilities of the manufacturer, distributors and users are remarkable issues.
- **Clinical Decision Support Software**
  Clinical decision support software uses technologies such as ML, Natural Language Processing (NLP) and Big Data analytics to assist physicians with clinical decision-making tasks, delivering actionable recommendations and providing complimentary materials such as data reports, guidelines, clinical document templates, etc. Consequently, the main issues are connected to liability profiles, should the clinical decision harm the patient, and the management and security of the personal data and information processed by the software.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  With reference to AI and ML solutions, regulatory assessment of the context and rules to be applied may be necessary, depending on the type of activity covered by the digital health solution.
  Relevant profiles include management and processing of personal data and correct identification of liability for damage arising from system errors or malfunctions. The outsourcing relationship requires a specific contract to govern these profiles.
- **IoT (Internet of Things) and Connected Devices**
  Internet of Things (IoT) should ensure the protection of privacy and the correct use of personal data collected. Risks related to the safety of devices should not be underestimated: if they are not adequately safeguarded, it can lead to multiple issues of liability in the event of malfunction.
- **3D Printing/Bioprinting**
  Among the main fields of application of 3D printing and bioprinting technology in healthcare there are: the production of medical devices; and the recreation of realistic models of organs to facilitate the understanding of complex surgical interventions in the surgical field.
  3D printing can also be used to reproduce biological material for the replacement of human organs and tissues (bioprinting).
- **Digital Therapeutics**
  Digital therapeutics (DTx) are hybrid solutions that present specific characteristics of medical devices but also affinities with pharmaceuticals. This also has implications as regards the national authorities responsible for the assessment of DTx. Other questions to be considered are personal data privacy and security, and, depending on the type of technology and functions applied, risks relating to the safety of devices. Another complex issue is certainly the liability of the parties involved in the production, marketing and use of these solutions.
  The "Digital Therapeutics working paper" adopted by Farmindustria (the Italian Association of Pharmaceutical Companies) in May 2023 has highlighted the need for a specific law governing the main aspects connected to DTx (a good starting point could be represented by the proposal of law on DTx presented to the Parliament on 7 June 2023).
- **Digital Diagnostics**
  The main legal issues are connected to the fact that the diagnosis is reserved only to the physician, who cannot be replaced by a machine in the performance of this activity.
  Particular attention should be paid to addressing ethical and legal issues in an appropriate manner by providing adequate information to HCPs and patients to support informed decisions and ensure data security and confidentiality.
- **Electronic Medical Record Management Solutions**
  Different subjects (HCPs, patients, etc.) can access electronic medical records; therefore, security measures should be adopted in order to ensure the correctness and accuracy of data and information and the confidentiality of personal data.
- **Big Data Analytics**
  Big Data analytics in the healthcare sector involves the processing of large volumes of data, often containing

personal or sensitive information, and for this reason it is regulated by the GDPR and the Guidelines of the Privacy Guarantor. These regulations state that health data, when used for the analysis of Big Data, must be managed in a secure manner and, where possible, anonymised to reduce the risk of violation of patients' privacy. Furthermore, the processing of health data requires a sound legal basis, such as informed consent or clearly defined legitimate interests. In the European context, the use of Big Data for health purposes must also comply with the ePrivacy Regulation, which provides guidelines on how to collect, store and share sensitive data in a safe and ethical way, avoiding improper or discriminatory uses.

- **Blockchain-based Healthcare Data Sharing Solutions**
  Blockchain technology is emerging as an innovative tool for the secure management and sharing of health data, but it is subject to specific regulatory requirements to ensure privacy and data protection. The GDPR requires that any processing of personal data, including its storage in a decentralised network, respects the principles of transparency, security and erasure possibilities, which can be complex to implement in a blockchain. In Italy and in the EU, there are no specific regulations for the use of blockchain in healthcare, but several guidelines are being studied to establish how this technology can comply with existing laws. It is essential for suppliers to ensure security measures to prevent unauthorised access and develop methods for anonymisation and selective access to data.
- **Natural Language Processing**
  The difficulty of an algorithm being able to understand human language is an issue.
  It is necessary to develop new solutions inspired by different disciplines (e.g. linguistics, computer science, neuroscience, etc.) to understand and generate text in a natural language that is more similar to human language, and have a large amount of data to validate and implement services.
  The use of NLP-based tools should be subject to prior information to educate the user on the decoding of information received and its application in everyday life.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

The main issue is the liability for illegal content uploaded to digital platforms.

As regards copyright, according to the Italian Supreme Court of Cassation (decision no. 7708/2019 and no. 39763/2021), the hosting service provider is jointly liable with the user who uploaded protected content, in the event that:

(i) it is aware of the offence committed by the recipient of the service;
(ii) the unlawfulness of the conduct of others is reasonably ascertainable; and
(iii) it has the opportunity to take action after being informed of the illegal content uploaded.

With regard to the second point, the Court referred to the degree of diligence, saying that it is reasonable to expect this from a professional network operator due to the "technological development existing at the time that the event took place", referring to AI as a tool to locate illegal content uploaded to the web.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The processing of personal data on a large scale thanks to the use of new technologies, the Internet and virtual servers represents the main issue. The huge flow of information that derives from the use of digital technologies in the health sector implies the need to solve a series of issues related to the process and protection of personal data (very often of a "sensitive" nature, as it is related to health), in compliance with the GDPR and Legislative Decree no. 196/2003 (the Privacy Code), which can impose compliance with more rigorous obligations and requirements than those of other sectors.

Other issues are related to the circulation of health data, the outsourcing and delocalisation of systems and services (considering that Cloud services and software on which digital health technologies are based are managed by service providers, hence the data is no longer stored on the user's physical servers, but is allocated on the systems of the supplier, which often keeps data of varying users with different or even conflicting interests and needs), as well as the storage of data in geographic locations often regulated by different legislation.

When processing personal health data, in addition to the GDPR and Italian Privacy Code, orders and guidelines issued by the Italian Data Protection Authority should also be considered, since they give useful indications on different questions, such as security measures to be implemented, the different roles in the processing, the legal basis, etc. With specific reference to personal data processing in the health sector, the Italian Data Protection Authority adopted opinions and guidelines on the processing of health-related data through AI systems, as well as through websites and apps aimed at putting into contact patients and HCPs (see question 2.6).

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In Italy, the use of personal health data is primarily regulated at the national level, with uniform application of the GDPR at the EU level and further detailed by the Italian Privacy Code.

According to our Constitution, Regions have the authority to adopt specific regulations in the health sector, always within the regulatory framework established on a national level. For example, Regions have a degree of autonomy regarding the operational aspects, including the processing of health data, of implementing and managing EHRs and telemedicine platforms, while still adhering to national requirements and ensuring that access and data sharing across healthcare facilities comply with national security and privacy standards.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

According to the Italian Privacy Code, processing by a public authority is always allowed if it is necessary for the

performance of a task conducted in the public interest or for the exercise of the authority's public powers and that if the purpose of processing is not expressly envisaged under a law or regulation, it shall be decided and indicated by the authority consistently with the task conducted or the power exercised.

Furthermore, the Italian law provides specific rules on the processing of health data by health professionals and health facilities (Privacy Code and Acts issued by the Italian Privacy Authority). The Privacy Code rules on information disclosed to patients by general practitioners and paediatricians (Art. 78), as well as public and private health facilities (Art. 79). Provision no. 55 of 7 March 2019 of the Italian Privacy Authority gives indications on the privacy information scheme, the legal basis of the processing activity, the appointment of the Data Protection Officer, and processing records specifically for the processing of health-related data carried out by HCPs, regardless of whether they operate as freelancers or within a public or private healthcare facility.

4.4 How do the regulations define the scope of personal health data use?

A definition exists at neither a national nor European level. The GDPR has established that the processing purposes must be specific, explicit and legitimate. It is up to the data controller to identify the processing purpose and specify it in the disclosure provided to the data subject (Art. 13 and Art. 14 of the GDPR).

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

Since there are no specific national provisions on this topic, GDPR rules shall apply.

Firstly, the data subject should be clearly informed of the specific purposes for which personal health data is collected and processed, in accordance with the principle of purpose limitation established by the GDPR. It is essential to outline the rights of data subjects, including access, rectification, erasure and the right to object, ensuring compliance with GDPR provisions. Additionally, the legal basis for processing health data should be specified and, if the explicit consent of the data subject represents the legal basis for a specific purpose of the processing, it shall be collected through a request that shall be presented in an intelligible and easily accessible form, using clear and plain language. Provisions on data minimisation and retention should ensure that only the necessary data is collected and retained for a limited time and the data subject should be informed on the specific retention period of his/her personal data. Appropriate technical and organisational measures should be implemented in order to safeguard the data security. If data processors are involved, the agreement should require adherence to data protection obligations provided for in Art. 28 of the GDPR.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The Italian Privacy Code provides for the possibility of submitting a complaint to the Italian Privacy Authority or, alternatively, of pleading the judicial authority, as long as a violation of rights under the GDPR occurs. The Italian Privacy Authority also has the power to issue the provisions pursuant to Art. 58 of the GDPR, including the application of administrative fines, pursuant to Art. 83 of the GDPR, both on reporting and *ex officio*.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

As already indicated above (see questions 4.1 and 4.3), in Italy there are specific rules set out in the Privacy Code and specific opinions and guidelines adopted by the Italian Data Protection Authority regarding the processing of personal health data, also through digital technologies (health apps, AI systems, etc.).

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The identification of subjects who have access to the personal data processed and their respective roles is the main focus; in complex supply chains, it could be difficult to identify who processes the personal data involved among the various managers of intermediate services. It is important to establish the capacity of each subject, identifying who acts as an independent data controller, who works as joint controller and who is designated as a data processor or sub-processor for the processing activity, stipulating specific agreements that govern relations among the various subjects.

In the Italian jurisdiction, these aspects are regulated by the same laws applying to the processing of personal data (i.e. the GDPR, Privacy Code, opinions and guidelines of the Italian Data Protection Authority).

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Personal data sharing is subject to the same laws and regulation generally applying to personal data processing. For this reason, the same analysis reported above (see question 4.2) may be considered here.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Data-sharing operations require more caution for health-related data processing as performed by HCPs. The processing of such data is carried out for purposes of care, and any sharing or transfer to other subjects would need to "match" the purposes (e.g. marketing purposes). It is therefore necessary to carefully evaluate the subjects with whom the data collected are shared, and verify the purposes for which they will be processed.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Ministerial Decree of 7 September 2023 (see question 1.2) ruled the "electronic health records 2.0", which includes more documents and information and a "personal section" of the record, in which personal documents related to health treatments could be inserted, together with the "patient summary", an informatic document written and updated by the physician, in order to ensure the continuity of care.

Additionally, the guidelines adopted by the Italian Data Protection Authority on websites and apps aimed at putting into contact patients and HCPs is an example of an initiative regarding standards for sharing health data (see question 2.6).

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

When sharing data and, in particular, healthcare data, it is necessary to implement adequate security measures in order to protect the accuracy and confidentiality of personal data from any unauthorised access. For this scope, the subjects entitled to collect and upload data, have access to and process them shall be identified. Furthermore, an appropriate retention period of data should be determined, taking into account the purpose of the processing, and data subjects' rights should be granted. The same rules governing data privacy already mentioned shall apply.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

In the Italian jurisdiction, patent laws impact the scope of patent protection for digital health technologies by setting specific criteria for patent eligibility under the Industrial Property Code (IPC, Legislative Decree no. 30/2005).

The Code outlines the scope of the patent by indicating patent requirements and the cases that remain excluded from the patentability. Patents shall be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible to industrial application. The following, in particular, shall not be regarded as inventions: (i) discoveries, scientific theories and mathematical methods; (ii) schemes, rules and methods for performing mental acts, playing games or carrying out business, and computer programs; and (iii) presentations of information. Methods for surgical or therapeutic treatment of the human or animal body and the diagnostic methods applied to the human or animal body cannot be patented.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

In the Italian jurisdiction, the Copyright Law (Law no. 633/1941) impacts the scope of copyright protection for digital health technologies by safeguarding the expression of ideas – such as the source code and graphical interfaces – rather than the underlying functionality or concepts.

In particular, the Copyright Law gives the creator the exclusive right to use his/her work, which lasts for the entire life of the creator, and up to 70 years after his/her death. Copyright ceases with its first sale, which means that once the creator puts a work on the market, he/she can no longer oppose the subsequent circulation of the work being sold or given to third parties, without prejudice to the prohibition on copying, duplicating or renting it (copyright fees must be paid for these activities). According to the law, computer programs (software) and databases that, due to the choice or arrangement of the material, constitute an intellectual creation of their creator, are protected by copyright (see question 6.5).

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

In the Italian jurisdiction, trade secret laws play a significant role in protecting digital health technologies by securing proprietary information that provides a competitive advantage, including, for example, algorithms, data analytics models and proprietary methodologies.

Legislative Decree no. 63/2018 enforced the EU Directive on the protection of confidential know-how and confidential business information, expanded the protection already present in the Italian legal system in the IPC and increased penalties for violations carried out through the use of IT tools.

What is protected are "trade secrets" (Art. 98 of the IPC), that is, company information and technical-industrial know-how, including commercial know-how, subject to the legitimate control of the holder. The qualification of secrecy depends on the following conditions, and namely that the information:

(a) is secret, in the sense that as a whole, or in the specific configuration and combination of its elements, it is generally unknown or not easily accessible to experts and operators in the sector;
(b) has economic value, given that it is secret; and
(c) is subject to measures deemed reasonably adequate to keep it secret by subjects who legitimately exercise control.

The protection is extended to data relating to tests or other secret data, the processing of which involves a considerable commitment, and whose presentation is subject to the authorisation of market placement of chemical, pharmaceutical or agricultural products involving the use of new chemical substances.

The legitimate holder of trade secrets has the right to prohibit third parties from acquiring, revealing to third parties or using these secrets in an abusive way without consent, unless they have been obtained independently. It is recommended to draft non-generic confidentiality agreements that explain which information must be considered secret and which is public, as well as the relative scope of dissemination. In addition to these agreements, it is advisable to think of specific organisational policies applicable to those who will access the data.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

The technology transfer includes all of the activities underlying the passage of a series of factors (knowledge, technology, skills, manufacturing methods and services) from the field of scientific research to that of the market. This is a process that results

from the collaboration between academia and industry, whose main objective is to make technology accessible to the public. As such is based on research and innovation, it is crucial to consider the protection of intellectual property, which renders the technology transfer safer and more efficient by promoting the use of the innovation by existing or newly-created companies (spin-offs and start-ups). This protection usually falls under the patent protection for inventions or copyright. For inventions created in universities (or public research institutes) the reference is Art. 65 of the IPC, a provision that is not entirely clear as regards its scope and interpretation. It outlines two "scenarios". The first is of "institutional research", in which the patentable inventions made by researchers will be owned by the researchers themselves, and not by the university or public research entity. The researcher is responsible for filing the patent application and informing the institution, and the latter is granted the right to receive at least 30% of the profit of the invention in the event that it is actually exploited economically, also through the grant of licences to third parties. It is then explicitly expected that the entities can establish different ways of distributing the profit by regulatory means, which cannot reduce the benefits of the researcher below the threshold of 50% of the total. The other "scenario" concerns the so-called "funded" research, i.e. that carried out within the framework of specific research projects financed by public or private third parties, for which the entity is entitled to ownership of the invention and can clearly negotiate the rules for the use of the results with the financing party.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

In principle, software is considered a literary work of art, and is protected by copyright. In this sense, Legislative Decree no. 518/92 (enforcing Directive no. 91/250/EU) expresses itself on the legal protection for computer programs, which integrated the law on copyright (Law no. 633/1941). Copyright does not protect the idea, but only its expression, and the expression of a software is in its code. Thus, copyright concerns the source code and the object code, but not their function. This means that anyone can create software with a function similar to that of the first author, as long as they do so without copying the source code and object code. The protection of copyright is automatic with the creation of the work. It is possible to register the program in the Public Software Register at the Italian Society of Authors and Publishers in order to obtain proof of authorship. Copyright must be governed in any software contract (development, licence and transfer).

However, it cannot be excluded that a software can have a technical function, thus be assimilated to an invention, and therefore be patentable; this is possible for SaMD. The Italian IPC (Art. 45) and the European Patent Convention (Art. 52) exclude the patentability of software "as such"; although, if it is possible to demonstrate the additional technical effect of a software, the protection deriving from the patent gains more significance because it allows the protection of the invention in any form it is reproduced, even if the patent has a shorter duration of protection (20 years) than that of copyright (70 years from the death of the creator), and requires registration in all of the areas in which protection is sought. As such, the costs are higher. Distinguishing between patentable and non-patentable software is often complicated and requires a case-by-case assessment by an expert. This is especially the case for SaMD, where the regulatory complexity of the qualification as a medical device is added to the complexity of the patent.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

The ownership of patents invented by AI devices is a topical issue and is still being debated in a number of jurisdictions.

To date, there are no Italian rulings on the matter, although different jurisdictions have refused to recognise AI as an inventor of a patent based on the fact that the inventor must be a natural person and that AI's inventions do not possess the characteristics of creativity and originality necessary for specific protection.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

The reference for government-funded inventions is Art. 65 of the IPC (see question 6.4), which applies to the inventions of researchers who work for a university or other public entity whose institutional purposes include research. Art. 65 of the IPC does not apply to research carried out within specific research projects funded by public entities other than the entity to which the researcher belongs.

According to Art. 65 of the IPC, when an invention is developed by researchers working for universities or research institutions, the rights to the invention typically belong to the institution, except for the right to be recognised as the author, which belongs to the researcher. However, the researcher may file the patent for the invention under his/her own name, if the institution does not do it within the term indicated by Art. 65 or if the institution declares that it has no interest in it.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

As far as we know, there are no specific decisions on this matter. However, with reference to intellectual property rights in the life sciences sector, we can recall the Italian Supreme Court decision no. 19335 dated 15 June 2022, which examined the case of a pharmaceutical company that commissioned a marketing agency to create graphic files. Upon termination of their contract, the pharmaceutical company sought not only the executable files but also the source files. The Supreme Court distinguished between executable files, source files and licensed software, ruling that the source files could not be claimed without explicit contractual clauses or sufficient evidence of authorship. This decision highlights the critical importance of clear contractual arrangements concerning intellectual property rights in the digital health sector.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

When dealing with collaborative improvements, the parties should consider that the link between the various subjects of the network is generally obtained with specific agreements that may have different legal nature, depending on the scope and purpose pursued, such as: consortia; contractual joint

ventures; and partnerships between public and private entities; as well as licensing relationships if intellectual property is involved. It is recommended that a customised contractual model be prepared that is adapted for the specific project and its potential outcomes. It is crucial that the role of each party be defined in all types of agreements, as well as the contribution, participation methods (governance), ownership, sharing of results and intellectual property and its economic exploitation.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

The healthcare sector in Italy (as well as in the EU) is subject to strict rules to both protect health and encourage business development. Healthcare companies are structured to operate in compliance with detailed regulatory schemes, and also take part in self-regulatory organisation that provides for the extension of rules and principles in relation to companies with less restricted activities in other sectors. It is therefore fundamental to capitalise on the experience of healthcare companies in the business and contractual model in order to encourage efficient integration and cooperation.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

The main aspects that parties should consider are the ones connected to security and confidentiality of data. The federated learning system should be protected by adequate security measures, since a possible attack to the system could jeopardise the data and information of all the participants.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Parties should consider aspects connected to data privacy, liabilities in case of damages occurred by patients and intellectual property rights. Furthermore, it should be considered that the only subject entitled to make a diagnosis is the physician, and so a generative AI (GAI) technology can be used only as a support to the activity of the physician and cannot provide a diagnosis on its own.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

In addition to the authorities already mentioned above with specific reference to the regulatory schemes related to digital health (see question 2.1), also the Ministry of University and Research and the Ministry of Economic Development play a role in enforcing regulatory schemes related to AI/ML.

In particular, each one in their respective area of competence, they rule innovation and economic aspects related to AI, supporting compliance with industry standards, and fostering AI research and development within ethical guidelines. It collaborates with other bodies also on an EU level in order to establish regulatory frameworks for AI's role in business and industrial innovation.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

There are no specific regulatory schemes related to AI/ML in our jurisdiction. For this reason, laws and regulations already mentioned on data protection, intellectual property rights and copyright and medical devices shall apply (see questions 2.1–2.9, 4.1–4.7, 5.1–5.5 and 6.1–6.8).

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Italian legislation poses some obstacles to the recognition of intellectual property rights for that created by ML software. The Italian Civil Code and Copyright Law (Law no. 633/1941) focus on the personal creation of the work and seem to exclude the ownership of copyright by subjects other than the creator and his/her successors. At present, it appears that AI-equipped software, despite having created the work, cannot hold the consequent rights. However, even the creator (natural person) of the software may not be the owner of the rights to work created by the software, due to the lack of the requirement of personal creativity. It is evident that using this thesis potentially has negative consequences for technological development and may de-incentivise investments. An alternative route currently being explored is aimed at pre-empting the investigation of the "creative act" when programming the software. Entries of software programming would thus become central and coincide with human creativity, which is an essential requirement for the attribution of an exclusive right.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

One of the main issues is the identification of the criteria for the adequate financial valorisation of intangible resources, such as ML data. There are several criteria for estimating the value of intangible resources (e.g. the determination of creation costs and discounting of income consequent to use of the resource, the discounting of presumed royalties that the company would pay if it did not own the resource, etc.). The choice depends on the type of intangible resource, the purposes and context of the assessment, and the ease with which reliable information is found on the resource and market on which it is placed.

Furthermore, it is essential to ensure compliance with data protection regulations, according to which personal data must be processed lawfully, transparently and for specific purposes. Licensing agreements must explicitly outline the scope of use, duration and rights related to the data, as well as the obligations of both parties regarding data protection and security

measures. Additionally, the terms of the agreement should address potential liabilities in the event of data breaches or misuse, along with indemnification clauses to protect the data provider from legal repercussions.

When it comes to licensing healthcare data, these considerations become even more complex due to the "sensitive" nature of medical information. According to data protection law, the licensing of healthcare data must prioritise patient confidentiality and, if necessary, informed consent, requiring explicit permission from individuals whose data is being processed. For this reason, licensing agreements, if possible, may provide for data aggregation, anonymisation processes and compliance with ethical standards. Companies may also consider incorporating clauses ruling secondary use of data, ensuring that it aligns with ethical guidelines and regulatory frameworks.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

As far as we know, in Italy, regulatory bodies overseeing AI/ML do not make a specific differentiation between standard AI and GAI.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Legal and regulatory issues surrounding GAI in digital health are shaped by concerns about data privacy, transparency and safety. GAI, particularly in healthcare, can process vast amounts of patient data, which raises privacy and security risks. The Italian Data Protection Authority temporarily banned ChatGPT in 2023, having detected data privacy issues under the GDPR. After this decision, the European Data Protection Board decided to launch a dedicated task force to foster cooperation and to exchange information at a European level on possible enforcement actions conducted by data protection authorities. The investigations are currently ongoing and a full description of the results is not available yet. Furthermore, in 2024, the Italian Data Protection Authority issued a guidance on how to protect personal data published online by public and private entities in their capacity as data controllers from web scraping (i.e. the indiscriminate collection of personal data on the Internet), carried out by third parties for the purpose of training GAI models.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

The Italian legal landscape does not currently have explicit rules specifically targeting AI/ML, but there is an increasing focus on developing frameworks to better manage and secure data used in AI. For this reason, the rules provided for by the laws on industrial property and copyright shall apply (see questions 6.1–6.8).

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

To date, the model of imputation of man's indirect responsibility for any adverse outcomes produced by the use of digital health technologies has been used without any particular problems. However, as complex as these technologies may be, the damage can always lead back to the person who planned, built or used this tool.

This "traditional" model of imputation of liability has been questioned following the advent of the latest generation of AI systems that operate on the basis of algorithms open to structural self-modification, determined by the experience of the system itself (ML), giving rise to completely unpredictable and inevitable behaviour on behalf of the programmer and/or user. Given this situation, a doctrine theorised the possibility of identifying the liability of the intelligent entity, whether cumulatively or independently of the liability of the programmer and/or user.

The Italian Council of State recognised the legitimacy of a decision by which the Public Administration ordered the transfer of civil servants on the basis of an algorithm, where there is:

- full knowledge upstream of the algorithm used and criteria applied; and
- the imputability of the decision to the entity holding power (which must verify the logic and legitimacy of the choice and results entrusted to the algorithm) (decision no. 2270/2019).

9.2 What cross-border considerations are there?

In case legal relationships may arise from the supply of the technological service such as to involve multiple subjects in different countries, thus involving multiple legal systems (such as a supplier in a country other than that of the user who uses the technological service, but everything could be further complicated by the competing liability of third parties), in order to avoid disputes upstream as regards interpretation issues on the competent jurisdiction and applicable law in the event of dispute between the user and supplier, it is wise to pay absolute attention and use maximum precision in the regulation of contractual relations between the parties.

According to the rules of international law (Law no. 218/1995), EU Regulations apply (applicable only to Member States), which give priority to the rights of parties to determine the jurisdiction and the law applicable to the relationship by consensus, introducing the so-called "connection criteria" to designate the applicable jurisdiction and law only in cases where nothing has been agreed upon otherwise between the parties.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Addressing liability risks related to AI and ML in digital health requires implementing best practices that integrate technical, ethical and regulatory approaches. To minimise legal risks, developers and providers must align with evolving standards,

especially given that AI/ML algorithms used in healthcare could directly impact patient outcomes. Here are some key practices Italian regulators and health organisations should focus on:

(1) **Data privacy and security**: the Italian Data Protection Authority issued opinions and guidelines on how to process personal health data, which directly applies to AI systems used in healthcare contexts.
(2) **Transparency**: AI systems should be transparent in their operations, especially regarding decision-making processes. In healthcare, this transparency is crucial for professionals who need to understand AI-generated insights for clinical decision-making.
(3) **Professional supervision**: Risks can be mitigated if the use of AI/ML systems is subject to supervision by an expert.
(4) **Product safety standards and risk assessment**: By identifying and mitigating with adequate security measures the possible risks early, developers can reduce the chance of liability issues arising later. Following MDR standards is especially critical for digital health products that impact patient diagnosis and treatment.
(5) **Post-market monitoring and continuous updates**: The monitoring of AI systems post-deployment can help to track performance, manage updates and respond to identified risks.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Liability for the misuse of healthcare data in AI/ML models in digital health solutions may imply liabilities related to data protection and data subjects' rights violation, professional and medical liability, and liability for defective products.

In Italy, the case law has in some decisions examined different liabilities that can be implied in the use of trained AI/ML models (e.g., Milan Court, decision no. 2059/2017 on the consequences of the use of a robot in surgery; Supreme Court, decision no. 2541/2016 on the liabilities of the medical staff related to the misuse of a device for monitoring vital parameters).

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based services are services offered on-demand by a supplier to an end-user through the Internet (e.g. data archiving, processing or transmission).

In healthcare, Cloud systems assist in innovating services provided to patients and healthcare facility management. In Italy, an example of an active Cloud-based service that is subject to specific legislation is the EHR, through which the HCPs and patient can update, view and share all of the health data of the latter.

The main key issues are: the outsourcing of data management, which requires appropriate rules for the control; and the need for full security guarantees of privacy.

The quality of network connectivity is essential to the efficacy of the performances and to guarantee the continuity of system accessibility. Therefore, it is essential to choose a service provider with high-quality standards in order to minimise the risks, and the Cloud computing contract must cover all aspects that could represent critical or unknown factors such as to generate liability (also taking the methods to manage information and data entered in the Cloud into account).

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Non-healthcare companies must carefully know and take into consideration the healthcare sector rules and regulatory frameworks, among which, for example, are as follows:

- about the authorisation for the healthcare activity;
- about the relationships with HCP public employees: in Italy, the performance of non-institutional assignments by public employees is subject to specific requirements (prior authorisation from the body to which it belongs is required); and
- about the marketing of compliant products: among these, not only the compliance requirements (for example, medical device standards if the medical app is qualified as such), but also the rules on information and advertising to consumers.

The evaluation of the legal environment is crucial in supporting the business model.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Once again, the knowledge of the legal framework is crucial for each choice functional to an investment, in order to identify the strengths and possible critical points of the project.

The evaluation requires an interdisciplinary approach, hence it is advisable to have a highly specialised and differentiated team that is constantly updated. On this point, given that the digital sector evolves on a continuous basis, we must consider the issue of obsolescence, which characterises the digital sector, which, in comparison to the others, is in constant evolution.

The market needs must then be analysed, while considering that the two main trends in the health sector consist of, on the one hand, unmet medical needs and, on the other hand, sustainability of the health system.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The main barriers are due to various factors, linked both to economic and organisational issues as well as the possibility of access to digital health solutions by HCPs and patients.

In particular, digital health solution technologies involve costs that require the use of funds that public health facilities may not always have at their disposal.

Another key barrier is purely organisational, and depends on the autonomy of each Region in its need to prepare resources and implementation tools. Organisational intermediation by the Region appears necessary in order to obtain the structured configuration of the service, to define the procedures, competencies and responsibilities of the structures and professionals involved, as well as the related costs. In Italy, this implies that the legislative-regulatory structure, organisational models and welfare strategies implemented for this

purpose by the Regions differ from one to another, with consequent non-standardisation and fragmentation of the development and diffusion of these systems on a national level.

In addition, access to digital health solutions requires the availability of infrastructures (e.g., Internet connection) and devices (e.g., tablets and/or smartphones), to which some portions of the population of patients and HCPs do not have easy access.

A further obstacle to the widespread clinical adoption of digital health solutions could be that regarding issues of health liability.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In Italy, there is no formal certification by medical associations in accordance with an objective protocol of criteria and without misleading claims.

At most, the endorsement of products by medical associations can take place. In order to be lawful, this endorsement must be accompanied by a certification of quality from passing a specific approval procedure, and not a mere commercial agreement, against payment, of product sponsorship by the association.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

In Italy, reimbursement models for digital health solutions, especially DTx, are evolving within a framework that prioritises clinical evidence and cost-effectiveness. Italian authorities have yet to fully formalise standardised reimbursement pathways.

In 2023, the update of the new Essential Levels of Assistance (LEA, i.e. the minimum health assistance services that are granted by the NHS) included, among others, some new technologies for the prosthetic assistance (e.g., eye communicators and keyboards adapted for people with very serious disabilities, digital technology hearing aids, home automation equipment and command and control sensors for environments, voice recognition and eye pointing systems).

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

In Italy, the healthcare ecosystem faces several due diligence gaps when analysing digital health solutions, particularly those that are data-driven or involve AI/ML technologies. One major gap is the lack of standardised frameworks for evaluating the clinical efficacy and safety of digital health products, which leads to inconsistent assessment criteria across healthcare providers and institutions. Many digital health solutions, especially those based on AI/ML, generate probabilistic rather than deterministic results, making it challenging for regulatory bodies to ensure these tools meet clinical reliability standards. Additionally, there is a limited capacity for conducting thorough audits on data privacy, security and algorithmic transparency, despite these being critical under the GDPR and Italian Data Protection Code.

Another gap lies in the technical expertise available to evaluate the algorithms and ML models that underpin these products. Few healthcare institutions have the in-house capacity to assess complex data-driven solutions fully, making them reliant on external certifications or reports that may not capture specific risks or biases in local clinical settings. Finally, a lack of interoperability standards in Italy complicates the integration of digital health solutions into existing health information systems, creating gaps in data sharing, continuity of care and system-wide risk assessments. The above-mentioned EU AI Act may help address some of these gaps by imposing stricter standards for high-risk AI applications in healthcare, yet without specific national guidance, these challenges persist at both regulatory and institutional levels.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

Worthy of note are digital therapies, that is, technologies controlled by a software, which provide real therapeutic interventions based on evidence of effectiveness (evidence-based) aimed at preventing, managing or treating a disease or a medical disorder.

This trend of the digital health ecosystem is demonstrating great potential for the treatment of various diseases, including addictions and chronic diseases.

The still unexplored potential of these digital therapies and the complexity of these new frontiers inevitably leads to various profiles of possible criticality, starting with the gaps in the regulatory landscape, which make it difficult to accurately frame these new tools.

Among the main issues, we mention the legal framework of digital therapies and the responsibility of digital technologies (the functioning of digital therapies is generally subordinated to the implementation of intelligent algorithms that allow interaction with the patient and, consequently, the clinical benefit). This feature opens up the previously discussed question of the responsibilities of digital technologies.

Furthermore, the specific elements of digital therapies would require *ad hoc* discipline to offer the regulatory clarity necessary for potential vulnerabilities also with reference to privacy and cybersecurity.

In this regard, the proposal of law on digital therapies (see question 2.1) does not seem, at the moment, to solve all the issues on this delicate topic.

Sonia Selletti graduated in law from the University of Pavia in 1991. She was admitted in Milan in 1994. She is a Supreme Court Barrister. After practising international law and after a period as Head of the internal legal office of an Italian pharmaceutical company, in 1995, Sonia joined Astolfi e Associati where she is a Partner and Head of the Life Sciences Group. She has 25 years of expertise in pharmaceutical and health legislation for medicinal products, cosmetics, medical devices and health supplements.
Sonia is a member of the Supervisory Bodies in sanitary and pharmaceutical companies pursuant to Legislative Decree no. 231/2001, aimed at preventing criminal liabilities of corporate entities.
She is the Director responsible for the specialist legal journal *Rassegna di diritto farmaceutico e della Salute*. She has authored various publications on legal topics concerning life sciences.
Sonia collaborates with the University of Pavia in administrative law courses on procedures for the access of medicines to the market. She also provides training courses in the healthcare and pharmaceutical field at CME events for health professionals.

Astolfi e Associati, Studio Legale
Via Larga, 8, 20122 Milan
Italy

Tel: +39 02 885 561
Email: sonia.selletti@studiolegaleastolfi.it
LinkedIn: www.linedin.com/in/sonia-selletti-b25953164

Claudia Pasturenzi graduated in law from the University of Pavia in 2010. She has been a member of the Pavia Bar Association since 2014. Claudia has been working with Astolfi e Associati since 2014 and mainly works in the field of pharmaceutical and healthcare law, in handling questions on the advertising of medicinal products and medical devices, also with regard to new communication channels (social media).
She is a member of the editorial board for the specialist legal journal *Rassegna di diritto farmaceutico e della salute*, as well as the author of several publications.

Astolfi e Associati, Studio Legale
Via Larga, 8, 20122 Milan
Italy

Tel: +39 02 885 561
Email: claudia.pasturenzi@studiolegaleastolfi.it
LinkedIn: www.linkedin.com/in/claudia-pasturenzi-687032167

Astolfi e Associati, Studio Legale was founded by Antonio Astolfi in 1955. Fostering his original interest in international trade law, he founded the law journal "*Diritto Comunitario e Degli Scambi Internazionali*" ("*EU Law and International Trade Law*"). Later, in the 1960s, he developed a strong interest in pharmaceutical and health law (life sciences) showing longsighted vision. In 1968, he founded the law journal "*Rassegna di Diritto Farmaceutico*" ("*Pharmaceutical Law*"), still edited today after more than 50 years, in its new version "*Rassegna di diritto farmaceutico e della salute*". This heritage is today the practice area of Astolfi e Associati, deployed from civil, labour, commercial and banking law to pharmaceutical, health and food law, proposing complementary and comprehensive services to clients to fully meet their needs for legal advice. Astolfi e Associati assists Italian and foreign clients in both extrajudicial and judicial matters.

www.studiolegaleastolfi.it

Japan

Masanori Tosu

Kenji Tosaki

Nagashima Ohno & Tsunematsu

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

In Japan, there is no clear legal definition of "digital health". It is generally used as a generic term for products and services related to medicine and healthcare that utilise digital technologies and data.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Regulatory approvals were granted with respect to various software as a medical device ("SaMD"), such as Artificial Intelligence ("AI") programs to assist in the diagnosis of diseases through images and smartphone applications to treat nicotine dependence and hypertension. Such software is being used in medical settings. Also, telemedicine is becoming popular due to deregulation and the difficulty of face-to-face medication during the COVID-19 pandemic. Various wearable devices and smartphone applications for general health promotion purposes outside of medical settings are also widely used.

1.3 What is the digital health market size for your jurisdiction?

We are not aware of any definitive data on the digital health market size in Japan.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

We are not aware of any definitive data on the comparative revenue of digital health companies in Japan.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

We are not aware of any definitive data on the comparative revenue of digital health companies in Japan.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The principal regulatory authorities for the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices ("PMD Act") are the Ministry of Health, Labour and Welfare ("MHLW"), the Pharmaceuticals and Medical Devices Agency ("PMDA") and local governments. The principal regulatory authorities for the Medical and Medical Practitioners Law are the MHLW and local governments. The principal regulatory authority for the Act on the Protection of Personal Information ("APPI") is the Personal Information Protection Commission ("PPC"). The principal regulatory authority for the Fair Competition Code is the Fair Trade Council. The principal regulatory authority for the Act Against Unjustifiable Premiums and Misleading Representations ("AUPMR") is the Consumer Affairs Agency.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

The PMD Act applies to digital health devices including programs that meet the following criteria for medical devices: (i) the device falls under the devices listed in the Cabinet Order; and (ii) the purpose of use of the device is the diagnosis, treatment or prevention of diseases or is to affect bodily structures or functions. Class I programs are excluded from the definition of medical device. A regulatory notice issued by the MHLW entitled "Guidelines concerning Applicability of Medical Devices for Programs" provides more detailed criteria including examples of programs not falling under medical devices. The PMD Act requires, among others, obtaining business licences and marketing authorisation for each product, complying with manufacture and quality control standards and conducting pharmacovigilance activities. In addition, false and exaggerated advertisements and advertisements of unapproved medical devices are prohibited. For the details of the regulations, please see the response to question 2.4.

Consumer healthcare devices or software that fall under the category of medical devices are subject to the regulations under the PMD Act. Consumer healthcare devices or software that do not fall under the category of medical devices shall not be advertised as if they are intended to diagnose, treat or prevent diseases. In addition, any other advertisements or representations that falsely claim that the products or services are better than they actually are will be in violation of the AUPMR.

Under the Medical Practitioners Act and the Medical Care Act, medical practices such as the diagnosis, treatment and prevention of diseases may only be provided by physicians and other qualified HCPs. In addition, previously, physicians and patients were required to meet face-to-face at medical institutions when providing medical treatment. However, the regulations have been gradually eased and currently, telemedicine services, in which patients are examined, diagnosed and provided with diagnostic results and prescriptions live through ICT devices, are increasingly permitted provided that the various requirements set forth in the "Guidelines for the Proper Implementation of Online Medical Treatment" published by the MHLW are met.

The application of the regulations under the APPI is a key issue with respect to data privacy and data compliance. For the details of the regulations, please see the responses to questions 4.1 through 5.5.

The prohibition of bribery under the Criminal Code is applicable when the physician is a (deemed) public official, and for certain manufacturers and distributors of medical devices, the regulations under the Fair Competition Code prohibit offering premiums (including money and other benefits) to doctors and medical institutions as a means of unfairly inducing them to trade in medical devices.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

As for the medical device regulations, the key enforcement areas are the determination of whether a program qualifies as a medical device and the regulation of device advertisements.

As for the data regulations, the key enforcement areas are the implementation of the necessary procedures for handling healthcare-related information and the implementation of the security control measures therefor, especially at medical institutions.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

In order to market SaMD in the Japanese market, it is necessary to obtain both business licences for the relevant entities/sites and a marketing authorisation for each product. As to the business licence, the company that markets the SaMD must obtain a marketing business licence. In addition, a manufacturing business licence must be obtained for each manufacturing facility and a sales business licence must be obtained for each sales office.

There are two pathways in respect of the marketing authorisation for SaMD products. Marketing Certification is the pathway for Class II or III medical devices for which the MHLW specified and published the evaluation and specification standards. Marketing Approval is the pathway for (a) Class II or III medical devices not subject to Marketing Certification, and (b) Class IV medical devices.

Clinical trials are usually required to be conducted for novel types of SaMD. When conducting clinical trials, medical device good clinical practice must be observed. Recently, the MHLW published evaluation indices for the safety and efficacy of SaMD that induces behavioural changes for disease treatment.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

The regulatory framework is essentially the same as that for SaMD. The MHLW published evaluation indices for the safety and efficacy of medical image diagnosis support systems using AI technology.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

An expert committee at the PMDA has discussed and published a part of recommended methods for the examination of adaptive AI devices that are intended to autonomously change their performance after being marketed. The relevant discussion will continue going forward.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation data such as clinical trial data will be a material part of regulatory review for marketing approval for AI/ML-based digital health solutions, the same as other types of medical devices. If a medical device subject to regulatory review is not a noble type of medical device, clinical trial data may not be required.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

There is currently no difference in regulations between the national and local levels.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

There is currently no noticeable difference in regulatory enforcement actions to digital health products and solutions.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Please see the response to question 2.1.
- **Robotics**
  If the product falls under medical device, the PMD Act shall apply.

- **Wearables**
  If the product falls under medical device, the PMD Act shall apply.
- **Virtual Assistants (e.g. Alexa)**
  If the product falls under medical device, the PMD Act shall apply.
- **Mobile Apps**
  If the product falls under medical device, the PMD Act shall apply.
- **Software as a Medical Device**
  Please see the responses to questions 2.1, 2.4 and 2.5.
- **Clinical Decision Support Software**
  Please see the responses to questions 2.1, 2.4 and 2.5.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  Please see the responses to questions 2.1, 2.4 and 2.5.
- **IoT (Internet of Things) and Connected Devices**
  If the product falls under medical device, the PMD Act shall apply.
- **3D Printing/Bioprinting**
  If the product falls under medical device, the PMD Act shall apply.
- **Digital Therapeutics**
  Please see the responses to questions 2.1, 2.4 and 2.5.
- **Digital Diagnostics**
  Please see the responses to questions 2.1, 2.4 and 2.5.
- **Electronic Medical Record Management Solutions**
  If the product falls under medical device, the PMD Act shall apply.
- **Big Data Analytics**
  If the product falls under medical device, the PMD Act shall apply.
- **Blockchain-based Healthcare Data Sharing Solutions**
  If the product falls under medical device, the PMD Act shall apply.
- **Natural Language Processing**
  If the product falls under medical device, the PMD Act shall apply.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

The "Safety Management Guidelines for Providers of Information Systems and Services that Handle Medical Information" issued by the Ministry of Economy, Trade and Industry ("METI") and the Ministry of Internal Affairs and Communications ("MIC") are applicable to providers of medical information systems and services. The guidelines contain stipulations such as the risk management process required upon the provision of medical information systems to medical institutions.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Under the APPI, personal information can only be used within the scope of the purpose specified in relation to the obtainment of personal information, and the principal's consent is required when such information is used for any other purpose. In addition, personal information related to medical or health matters falls within the category of sensitive personal information and the consent of the principal is required for the obtainment of such sensitive personal information.

"Anonymously Processed Information" is the information that is processed so that it cannot be restored to re-identify a specific individual, and it is treated as non-personal information to which the above-mentioned limitation on the purpose of use does not apply. "Pseudonymously Processed Information" is the information that is processed so that a specific individual cannot be identified without cross-checking with other information, and it can be used for purposes other than those specified in relation to an obtainment without the principal's consent, provided that the modified purpose is publicly announced. These types of information are expected to be utilised in the fields of medicine and healthcare.

In addition to the APPI, when personal information is obtained and used for life sciences and medicine-related research, regulations based on Ethical Guidelines issued by the Ministry of Education, Culture, Sports, Science and Technology, the MHLW and the METI, such as Institutional Review Boards approval and informed consent, would also apply.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

The amendment to the APPI, which integrates national and local government regulations on personal data, came into effect as of April 2023, and there is currently no difference in the regulation of health data use between the national and local levels.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The above-mentioned restrictions under the APPI do not apply to the use of personal information for academic research purposes by academic research institutions, such as universities (including university hospitals). For the difference of the regulation depending on the nature of data, please see the response to question 4.1.

4.4 How do the regulations define the scope of personal health data use?

Apart from certain exceptions stipulated in the APPI, the use of personal information including personal health data is limited to the specified purpose. Exceptions include cases where the use is particularly necessary for the improvement of public health and when it is difficult to obtain the consent of the principal. In a Q&A recently published by the PPC, it was indicated that the use by pharmaceutical companies for the purpose of research on rare diseases or the like may fall within this exception.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

In regard to the securing of comprehensive rights to use

personal information and data, the key point is to define the purpose as broadly as possible in the contract terms and privacy policy. Having said that, according to the guidelines published by the PPC, it is not sufficient to merely specify the purpose of use in an abstract or general manner, instead, it is desirable to specify the purpose in such a way that the principal can generally and reasonably assume the kind of business and the purpose the information will ultimately be used for.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The APPI stipulates that efforts must be made to keep personal data accurate and up to date. The APPI also prohibits the use of personal information in a manner that may encourage or induce illegal or unjustifiable acts, which include the use of personal information to illegally discriminate against a person.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

Please see the response to question 5.4.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Under the APPI, apart from certain exceptions, such as outsourcing or joint use, personal data may not be provided to third parties without the consent of the principal. In obtaining consent for international transfer, information must be provided to the principal in advance regarding the personal data protection system in the country where the third party is located and the measures to be taken by such third party to protect the personal data.

Exceptions include cases where the use is particularly necessary for the improvement of public health and when it is difficult to obtain the consent of the principal. In a Q&A recently published by the PPC, it was indicated that the provision to pharmaceutical companies for the purpose of research on rare diseases or the like may fall within this exception.

Anonymously Processed Information may be provided to third parties without the consent of the principal, whereas the provision of Pseudonymously Processed Information to third parties is prohibited.

When providing personal data to a third party outside Japan, apart from certain exceptions, it is necessary to obtain consent from the principal even in the case of outsourcing or joint use.

The regulations based on Ethical Guidelines may also apply in the domains of life sciences and medicine-related research.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

There is currently no difference in regulations between the national and local levels. Please see the response to question 4.2.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

The above-mentioned restrictions under the APPI do not apply to the provision of personal data to academic research institutions or provision by academic research institutions to a third party for academic research purposes. For the difference of the regulation depending on the nature of data, please see the response to question 5.1.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Under the APPI, the provision/sharing of medical information to a third party (such as provision by a medical institution to a pharmaceutical company) requires the opt-in consent of the principal. However, the Next Generation Medical Infrastructure Act ("NGMIA") allows an opt-out process instead of opt-in consent for the collection and provision by a medical institution of medical information to a certified entity performing anonymous processing of medical information to enhance the utilisation of Anonymously Processed Information in medical fields. Since the 2023 amendment to the NGMIA, a similar regime also applies to Pseudonymously Processed Information in medical fields. It is expected that, in some respects, Pseudonymously Processed Information, where the deletion of outlier information is not required upon processing, may be more useful than Anonymously Processed Information in medical fields.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

In principle, healthcare data itself constitutes personal information and when such data is to be shared, the consent of the principal is required under the APPI. Even in respect of federated learning, where only parameters and/or learned models excluding personal information are to be shared with third parties, it is necessary to confirm whether the use of healthcare data for federated learning will be within the purpose of use that was presented to the principal.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Under the Patent Act of Japan, inventions are classified into three categories: an "invention of a product"; an "invention of a method"; and an "invention of a method for producing a product". To obtain patent protection for digital health technologies, one can either seek patent protection for a system or program that utilises digital health technologies as an "invention of a product" or seek patent protection for information processing or services that utilise digital health technologies as an "invention of a method". In the case of an invention of a product, to act in such a way as to constitute direct patent infringement is to produce, to use, to "Assign, etc." (i.e. to assign or to lease, including, in the case where the product is a computer program, to provide through an electrical communication line), to export, to import or to offer to "Assign, etc." the product as part of one's business. For an invention of a method, on the

other hand, to act in such a way as to constitute direct patent infringement is to use the method as part of one's business. In the case of an invention of a method for producing a product, to act in such a way as to constitute direct patent infringement is to use the method as part of one's business or to use, to "Assign, etc.", to export, to import or to offer to "Assign, etc." the product produced by the method as part of one's business. When the allegedly infringing product or method meets all the elements of the patented invention, the above-mentioned acts constitute acts of literal patent infringement. Even when a part of a patent claim does not correspond to the allegedly infringing product and the product does not literally fall within a patent claim, the scope of protection of the patent claim extends to the product under the doctrine of equivalents if (i) the non-corresponding part is not the essential part of the patented invention, (ii) the purpose of the patented invention can be achieved by replacing this part with a part in the product and an identical function and effect can be obtained, (iii) a person skilled in the art could easily come up with the idea of such replacement at the time of the production of the product, (iv) the product is not identical to the technology in the public domain at the time of the patent application or could have been easily conceived at that time by a person skilled in the art, and (v) there were no special circumstances such as the fact that the product had been intentionally excluded from the scope of the patent claim in the course of the prosecution. A patent owner can seek injunctive relief and/or compensation against an infringer through court proceedings.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Software, screen displays and instruction manuals used in digital health technologies may be eligible for copyright protection. A copyright includes a right of reproduction, a right of stage performance, a right of musical performance, a right of on-screen presentation, a right of transmitting to the public, a right of recitation, a right of exhibition, a right of distribution, a right of transfer, a right to rent out and a right of adaptation. A copyright owner can seek injunctive relief and/or compensation against an infringer through court proceedings.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Information used or generated by businesses utilising digital health technologies may be protected as trade secrets. In general, the wrongful acquisition, use and disclosure of "Trade Secrets" are regarded as "Unfair Competition" under the Unfair Competition Prevention Act of Japan ("UCPA"). "Trade Secrets" are defined as "technical or business information useful for business activities, such as manufacturing or marketing methods, that are kept secret, and are not publicly known". A person who wrongfully acquired, used or disclosed "Trade Secrets" may be enjoined from using and/or disclosing the "Trade Secrets" and/or be held liable for damages by the court under the UCPA.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Technology licensing organisations ("TLOs") are organisations that transform the results of research by university researchers into patents and transfer the results to private companies. TLOs can submit plans for the implementation of their technology transfer businesses to the Ministry of Education, Culture, Sports, Science and Technology and the METI and seek their approval. Approved TLOs will be eligible for a discount of annual patent fees. Further, when approved TLOs take out a loan for their approved businesses, an Incorporated Administrative Agency will guarantee the debts incurred by these TLOs.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

An invention of software can be patented. If an invention of software to be used for a medical device is patented, the scope of patent protection is the same as that for other patents. Please see the response to question 6.1 on the general scope of patent protection. Further, software can be considered as works of computer programming under the Copyright Act of Japan. The scope of copyright protection for works of computer programming is the same as that for other works. Please see the response to question 6.2 on the general scope of copyright protection.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

No, an AI device cannot be considered an inventor of a patent under Japanese law. Under Japanese law, only a "person" can own a right and an AI device is not a "person". As an AI device cannot own a right to obtain a patent, an AI device cannot be named as an inventor. On May 16, 2023, in the litigation where the applicant of a patent application for an invention titled "Food Container and Devices and Methods for Attracting Enhanced Attention" allegedly autonomously generated by an AI device called "DABUS" sought the revocation of the dismissal of the patent application by the Commissioner of the Japan Patent Office, the Tokyo District Court dismissed the action, holding that an "inventor" is limited to natural persons.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

The scope of intellectual property ("IP") rights provided to the government for government-funded inventions is the same as that for other inventions. With respect to certain IP rights that are associated with the results of government-contracted research and development, or of government-contracted software development, the national government may decide not to acquire such rights in a situation where the contractor promises that (i) if such results have been obtained, the contractor will report them to the national government without delay, (ii) the contractor will grant the national government the right to use such rights free of charge if the national government requests the contractor to do so while making it clear that the reason for doing so is that it is particularly necessary for the sake of the public interest, (iii) the contractor will grant a third party the right to use such rights if the contractor has not used such rights for a considerable period of time and does not have a legitimate reason for not having used such rights for a considerable period of time, and if the national government requests

the contractor to do so while making it clear that the reason for doing so is that it is particularly necessary to facilitate the use of such rights, and (iv) when intending to transfer such rights, the contractor will obtain the approval of the national government in advance.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

In providing services utilising digital health technologies, servers located outside of Japan may be used. In such cases, the territoriality of IP rights can be an issue. With respect to the principle of territoriality, the Intellectual Property High Court ("IPHC") recently rendered two key judgments addressing this issue. In one case, the patentee of a patent covering an invention of a program titled "Display Device, Method of Displaying Comments, and Program" sued defendants who transmitted their program from a server located in the United States to users in Japan. Article 2(3)(i) of the Patent Act of Japan sets forth the definition of "working" of an "invention of a product" and pursuant to that definition, in the case of an invention of a program, "providing through a telecommunication line" is included in "working". On July 20, 2022, the IPHC held that in the case of an invention of a program that may be transmitted via a network, "an act of transmitting a program can be considered to constitute 'providing' under the Patent Act of Japan when such transmission can be evaluated as having been performed within the territory of Japan from a substantive and overall perspective". In the other case, the patentee of a patent covering an invention of a system titled "Comment Delivery System", which is the plaintiff in the first case, sued defendants who transmitted files used for the defendants' services from a server located in the United States to user terminals in Japan, which are the same defendants as in the first case. Pursuant to the definition of "working" set forth in Article 2(3)(i) of the Patent Act of Japan, "producing" is included in "working". On May 26, 2023, the IPHC held that even if a server, which is part of the components of a network-type system, is located outside Japan, newly producing that network-type system constitutes the act of "producing" under Article 2(3)(i) of the Patent Act of Japan when such production can be considered to have been performed within the territory of Japan. These two judgments were appealed to the Supreme Court, and it is expected that the decisions will be rendered by the Supreme Court in the first quarter of 2025. Once the Supreme Court renders its decisions, the opinions will include a new ruling on the circumstances under which the patentee of a Japanese patent could enforce the patent against acts across the border of Japan, and they will be very important.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

In general, when conducting collaborative development or improvements, it is important to stipulate in the contract, among others, the roles and cost allocation of each party, the rights and licence of the deliverables, and the confidentiality obligation. If the rights of one party are restricted during and after the collaboration (e.g., restriction on a similar development), antitrust issues may arise. When collaborating with academia, compensation for non-execution and publication procedure may also be negotiation points.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

Although there is nothing special to note, it would be helpful to note that healthcare companies are highly regulated and the contents of agreements may be affected by applicable regulations.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

The purpose of use of the AI models provided by AI developers to the data holders should be limited to the purpose of federated learning. In addition, it would be preferable for the AI developers not to limit the purpose of use of the learned AI models provided by such data holders to such AI developers to the extent possible in order to eliminate restrictions on business development. It would also be important to provide representations, warranties and covenants regarding compliance with data privacy regulations.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

It should be noted that, if the personal information to be used by a generative AI contains sensitive information such as medical data, the consent of the principal is required to obtain and provide such data to a third party under the APPI. In addition, since the output from the generative AI cannot be controlled in principle, it would be necessary to take care in respect of the risk of the output rising to a level where it would constitute a diagnosis, which could lead to issues regarding the generative AI unintentionally constituting a medical device and/or medical service.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

There is no regulatory authority that is comprehensively in charge of regulations related to AI/ML in Japan and the governmental agencies that oversee each industry are in the process of organising their respective policies and guidelines on AI/ML-related regulations.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

Please see the responses to questions 2.4 to 2.7.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

If there is no active human involvement in the software development at all, no IP rights will arise. However, if the development of the software falls under the act of "adaptation" of an original work, the copyright holder of the original work holds rights on the developed software including the right of reproduction, the right of transmitting to the public and the right of adaptation. This means that, for example, the developed software cannot be reproduced without obtaining a licence from the copyright holder of the original work.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

In transactions of licensing data, the following issues should be considered: (i) rights to deliverables; (ii) liability for defective data; (iii) losses derived from licensed data; and (iv) limitations on the purposes of use.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

There is currently no specific difference in regulations between standard AI and generative AI.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Among the various issues, the issues under the Copyright Act and the APPI are important. The issues under the Copyright Act include (i) whether a copyright infringement occurs when a generative AI uses a work for learning, (ii) the risk of an AI-generated product infringing on a third party's copyright, and (iii) whether the AI-generated product itself constitutes a copyrighted work. The various discussions related thereto are ongoing. With respect to the APPI, it is important to check whether the principal consented to certain uses of personal information by a generative AI for learning. It is also important to check whether the input of prompts containing personal information into a generative AI constitutes (a) a purpose other than those that were presented to the principal, or (b) the provision of such personal information to a third party (in both cases (a) and (b), the principal's additional consent is required). The PPC has issued a warning related thereto.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

While there is no clear precedent to date, such disgorgement by trained AI/ML models without appropriate data rights may constitute a violation of the APPI.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

In general, liability can arise in tort (either under the Civil Code or under its special law, the Product Liability Act ("PLA")) or under contract. Since "products" for which a claim under the PLA can be asserted are limited to movable property, a claim based on the PLA cannot be filed for an adverse outcome caused by programs unless there exists a device in which such program is incorporated and a defect in the program leads to a defect in the device itself.

An administrative notice recently issued by the MHLW provides that even when a patient is treated using a program that provides AI-based diagnosis and treatment support, the physician is responsible for the final decision for those acts.

9.2 What cross-border considerations are there?

Under the conflicts of laws principle in Japan, the governing law of a tort is the law of the place where the adverse consequence of the tortious act occurred. On the other hand, the parties' agreement takes precedence over the decision of the governing law of the contract.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

It would be advisable to include provisions regarding limitation of liability in the terms and conditions for the use of the generative AI. It would also be advisable to include appropriate disclaimers to avoid any misunderstanding about the nature of the subject device/service for digital health solutions using a generative AI.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Misuse of healthcare data may constitute a violation of the APPI and a civil tort that would result in damage compensation liability.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

The PMD Act regulations of SaMDs would apply to the medical programs provided in a form that allows only the right to use the program in the Cloud without transferring ownership of the program.

In addition, providers of Cloud-based services that handle medical information would be subject to the METI/MIC guidelines described in the response to question 3.2.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

When entering the digital health product market, whether the PMD Act is applicable or not is the key issue. When entering the digital health service market, it is necessary to keep in mind that private companies are not allowed to provide services that fall under medical practice.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

As the healthcare sector, including digital health, is highly regulated, it is advisable for venture capital and private equity firms to conduct due diligence carefully, especially on regulatory and compliance matters. In addition, as IP would be a key asset for digital health ventures, it is also advisable to carefully examine IP-related matters in due diligence.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The key barrier is the low predictability of applicable regulations regarding medical devices and medical practice. The MHLW is working to ensure the foreseeability of the applicability to medical device regulation to programs by establishing a consultation service and publicising consultation cases.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The clinician certification body in Japan is the MHLW. Having said that, the Japan Medical Association, a voluntary membership organisation for medical doctors, may have a certain influence on the policy making regarding the clinical adoption of digital health solutions.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

Digital health solutions may be reimbursed under the National Health Insurance ("NHI") system. To be eligible for reimbursement, a digital health solution provider needs to apply to the MHLW for inclusion on the NHI Price List and to undergo a review process by the MHLW.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

When conducting due diligence on the digital health solution, especially data-driven products such as AI/ML-based solutions, it is crucial to review the subject products not only from the pharmaceutical/medical regulation perspective but also from the data privacy/protection regulation perspective.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

As the next amendment to the APPI is currently being discussed, it is necessary to closely monitor how it will affect the digital health field.

Masanori Tosu is a partner at Nagashima Ohno & Tsunematsu. He provides services in a wide range of matters, including mergers and acquisitions, licensing, collaborative research and development, and various other transactions, as well as regulatory and governmental affairs, for clients both inside and outside Japan, with a focus on the life science, pharmaceutical and healthcare fields.
He also worked for the Ministry of Health, Labour and Welfare (MHLW) from 2019 to 2021. While at the MHLW, he was involved in various life science and healthcare-related policies and administrative actions and, among others, in various measures taken by the Japanese government to the COVID-19 pandemic.

Nagashima Ohno & Tsunematsu
JP Tower
2-7-2 Marunouchi, Chiyoda-ku
Tokyo 100-7036
Japan

Tel: +81 3 6889 7245
Email: masanori_tosu@noandt.com
URL: www.noandt.com/en/lawyers/masanori_tosu

Kenji Tosaki is a partner at Nagashima Ohno & Tsunematsu. His practice focuses on dispute resolution. He specialises in IP litigation and complex commercial litigation, and he also covers the area of TMT, including data protection matters.
In the area of IP litigation, he handles both IP infringement litigations and IP invalidation litigations before the IP High Court, the Supreme Court, District Courts and the Japan Patent Office. His IP expertise includes a wide variety of IP matters (patents, copyrights, trademarks, design rights, unfair competition and trade secrets) in many areas, such as telecommunications, electronics, social games and pharmaceuticals. He also provides pre-litigation counselling, including infringement/invalidity analysis.
In the area of complex commercial litigation, he gives advice on matters such as securities law and cross-border contracts.

Nagashima Ohno & Tsunematsu
JP Tower
2-7-2 Marunouchi, Chiyoda-ku
Tokyo 100-7036
Japan

Tel: +81 3 6889 7206
Email: kenji_tosaki@noandt.com
LinkedIn: www.linkedin.com/in/kenji-tosaki-8b084311

Nagashima Ohno & Tsunematsu, based in Tokyo, Japan, is widely recognised as a leading law firm and one of the foremost providers of international and commercial legal services. In representing our leading domestic and international clients, we have successfully structured and negotiated many of the largest and most significant corporate, finance and real estate transactions related to Japan. The firm has extensive corporate and litigation capabilities spanning key commercial areas such as antitrust, intellectual property, labour and taxation. We are known for path-breaking domestic and cross-border risk management/corporate governance cases, such as fraud investigations and white-collar criminal defence, and for handling insolvency and restructuring proceedings including large-scale corporate reorganisations. In order to deliver optimal service and value to our clients, the approximately 600 lawyers of the firm, including about 50 experienced lawyers from various jurisdictions outside Japan, work together in customised teams to provide the expertise and experience specifically required for each client matter.
The firm has a vast network of relationships with foreign companies and law firms that provide it with a unique perspective when representing clients in international deals. Our overseas network includes locations in New York, Singapore, Bangkok, Ho Chi Minh City, Hanoi, Jakarta* and Shanghai. The firm also maintains collaborative relationships with prominent local law firms across Asia and other regions. We regularly handle and coordinate matters involving complex legal issues in a number of Asian jurisdictions. As a pioneering Japanese law firm that has established its presence in New York, our activities in the United States and throughout the Americas and Europe are expanding rapidly. The firm strives to meet the needs of both its international clients operating in Japan and Asia and its domestic clients operating outside Japan or seeking to expand their operations overseas.
(*Associate office)

www.noandt.com

NAGASHIMA OHNO & TSUNEMATSU

Korea


Jin Hwan Chung


Eileen Jaiyoung Shin


Sungil Bang

Lee & Ko

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

No statutory definition has yet been established. However, "digital health" is generally understood as the combination of healthcare services and information and communication technology, which includes telemedicine, mobile health, health information technology and hospital digitalisation systems, such as electronic medical records (EMRs) and electronic health records (EHRs).

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Korea is one of the leading countries in the field of digital health. The picture-archiving and communication system was introduced in the mid-1990s, and EMRs and EHRs were introduced in the early 2000s. In recent years, software as a medical device (SaMD) products have become a key emerging part of the digital health industry, and in particular, disease diagnosis and treatment assistance technologies utilising artificial intelligence (AI) are experiencing rapid commercialisation.

1.3 What is the digital health market size for your jurisdiction?

No official data is available. However, the Korea Health Industry Development Institution, an organisation under the Ministry of Health and Welfare (MOHW), estimated the market size at approximately 1.57 billion USD in 2022 (1 USD = 1,300 KRW). Additionally, some international media outlets project that South Korea's market size will reach approximately 2.46 billion USD by 2024.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

No official data is available.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

No official data is available.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

When the Digital Medical Products Act, which was enacted on 23 January 2024, comes into effect on 24 January 2025, the Ministry of Food and Drug Safety (MFDS) will become the principal regulatory authority responsible for its enforcement. The MFDS will oversee all aspects of digital health, including product approvals, manufacturing and quality control of digital health products.

However, Korea implements a universal public health insurance system based on the National Health Insurance Act: every medical institution is required to provide medical services under the national health insurance system, and every citizen is required to contribute a health insurance premium based on his/her income or assets. As such, it is important for a digital health product or service to be eligible for reimbursement under the National Health Insurance Act for commercial success in the market. In this regard, the MOHW is the authority to determine whether digital health products/services can be covered by national health insurance.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

The MFDS has authority over regulatory approval of medical devices, AI, generative AI, SaaS, SaMD and combination products. However, obtaining regulatory approval from the MFDS does not necessarily mean that the digital health technology can immediately be used in medical settings. Certain new digital health technologies are required to undergo the new health technology assessment (nHTA) under the Medical Service Act (enforced by the MOHW) before being used at medical sites. Furthermore, as explained in question 2.1 above, approval from the MOHW is required for national medical insurance reimbursement eligibility.

The Personal Information Protection Act, which imposes strict data privacy protection obligations, plays an important role in the digital health field. In developing and providing digital health services to customers, it is necessary for a

manufacturer or service provider to have access to patients' health data without violating the data privacy regulations in Korea; however, these restrictions are not easy to fully comply with from the industry's perspective.

If a digital health product is classified as a medical device under the Medical Devices Act or a drug under the Pharmaceutical Affairs Act, anti-kickback restrictions, which prohibit a manufacturer, importer or distributor of medical devices or drugs from providing economic value to healthcare professionals for the purpose of promoting medical devices or drugs, will apply as well.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

With the enforcement of the Digital Medical Products Act on 24 January 2025, digital medical devices, digital convergence medicines and digital medical/health support products (formerly known as wellness devices), which were previously regulated separately under the Medical Devices Act and Pharmaceutical Affairs Act, will be primarily regulated under the Digital Medical Products Act as digital medical products. Depending on the characteristics of digital medical devices, additional regulations from the Medical Devices Act, Pharmaceutical Affairs Act and Medical Service Act may also apply.

Meanwhile, the Basic Act on the Development of Artificial Intelligence (AI Basic Act), passed the National Assembly's plenary session on 26 December 2024. Therefore, the AI Basic Act may also apply during the development or utilisation of digital medical products once this Act is enacted.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

Essentially, market authorisation must be obtained from the MFDS under the Digital Medical Products Act. Furthermore, even after obtaining market authorisation, to be used in medical settings, the product must undergo administrative procedures related to national health insurance reimbursement coverage.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Please refer to the response for question 2.4.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

The MFDS, which holds the authority for market authorisation, continues to update its regulations and guidelines related to approvals in order to reflect advancing technologies. Additionally, the Ministry of Science and ICT (MSIT), the Ministry of Trade, Industry and Energy, the MOHW and the MFDS have jointly established the Korea Medical Device Development Fund, a foundation aimed at supporting the development of medical devices based on digital technologies.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

The role of clinical validation data in the regulation of AI/Machine Learning (ML)-based digital health solutions is crucial, as it is considered a key element in ensuring the safety and efficacy of the technology. In Korea, such clinical validation data serves as an important criterion in the regulatory approval process.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In Korea, digital health products and solutions are regulated at the national government level.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Please refer to the response for question 2.6.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Under the Medical Service Act, telemedicine is permitted only between physicians: (a) physicians can receive support for patient treatment and diagnosis from other physicians via telecommunication devices; but (b) "physician-to-patient" telecommunication is not permitted.
  The government permitted "physician-to-patient" telemedicine on a temporary basis so as to cope with the COVID-19 pandemic by amending the Infectious Disease Control and Prevention Act in December 2020, which permission continued until the end of May 2023. Since June 2023, "physician-to-patient" telemedicine is permitted as a form of pilot programme implemented under the Framework Act on Health and Medical Services, and such temporary permission is expected to continue until the Medical Service Act is amended based on the consensus with the government and medical societies.
- **Robotics**
  Robotic surgery equipment is widely used in Korea; however, as far as digital health is concerned, no significant issues are being discussed.
- **Wearables**
  Many wearable devices are introduced in Korea as wellness products or medical device products, the latter of which will require MFDS's market approval. As medical services can be provided only by healthcare professionals under the Medical Service Act, wearable devices are not permitted to provide information or services that can be deemed medical services as defined by relevant Supreme Court precedents. In this regard, the MOHW provides guidelines on the health information that can be provided through wearable devices.

- **Virtual Assistants (e.g. Alexa)**
  Virtual assistants draw relatively less attention in Korea; however, similar issues as in the case of wearable devices can apply.
- **Mobile Apps**
  Mobile apps are one of the hottest areas in Korea, and the MFDS has established the Safety Management Guideline for Medical Mobile Apps in this regard.
- **Software as a Medical Device**
  This a rapidly growing field, and according to MFDS data, 376 products were approved between 2020 and 2023, with exports increasing by over 300% during the same period.
- **Clinical Decision Support Software**
  The majority of SaMD products approved by the MFDS may be classified as clinical decision support software. With the utilisation of AI technology, the development of products in this field is being accelerated, and interest from the medical field is also growing.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  AI/ML-powered digital health solutions can also require the MFDS's market approval if the product is deemed a medical device. According to the MFDS guideline, AI-based medical imaging software that can be deemed a medical device are as follows: (i) those that analyse medical data to diagnose, predict, monitor or treat diseases; and (ii) those that analyse medical data to provide clinical information necessary for the diagnosis or treatment of a patient.
- **IoT (Internet of Things) and Connected Devices**
  There are no specific guidelines regulating IoT and connected devices in the digital health field. However, given the nature of these technologies, more emphasis may be imposed on the protection of personal data.
- **3D Printing/Bioprinting**
  The government classifies 3D printing/bioprinting as one of the innovative medical devices under the Act on Nurturing the Medical Devices Industry and Supporting Innovative Medical Devices.
- **Digital Therapeutics**
  The Digital Medical Products Act systematically manages the safety and efficacy of digital therapeutics and outlines measures to support market entry and commercialisation.
- **Digital Diagnostics**
  In the field of digital diagnostics, such as radiology and electrocardiography, numerous products have been developed and received approval from the MFDS. However, these products are not intended to replace the judgment of a physician but have received approval as items that assist in the physician's judgment.
- **Electronic Medical Record Management Solutions**
  In Korea, the introduction of EMRs began in the early 1990s, and as of 2021, approximately 95% of all medical institutions, including solo practitioner's clinics, are utilising EMRs.
- **Big Data Analytics**
  In June 2023, the MFDS revised the "Regulation on Medical Device Review and Approval", recognising real-world evidence for medical devices incorporating digital technologies such as big data and AI as clinical trial data for safety and efficacy confirmation.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Blockchain technology is gaining attention in Korea for its potential to enhance interoperability of EMRs and the security capabilities of healthcare data. However, there are no specific regulations governing its use as of now.
- **Natural Language Processing**
  No particular development has been made from a regulatory or governmental policy perspective.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

In Korea, digital health platform providers must comply with key legal and regulatory issues, including data protection and privacy, medical device regulations, nHTAs, health insurance coverage and restrictions on telemedicine, as well as cybersecurity and liability requirements.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The main statutory regulations are as follows:

(1) Personal Information Protection Act

Personal health data is classified as sensitive information, requiring strict protection measures for its collection, processing, storage and provision.

Use of pseudonymised data: pseudonymised data differs from anonymised data, which completely removes all identifiable elements. Pseudonymised data involves deleting or replacing identifiable information while retaining the possibility of re-identification. As a result, pseudonymised data remains subject to the PIPA. Data pseudonymised for research or statistical purposes can be used without the consent of the data subject. However, since pseudonymised data can potentially be re-identified, additional security measures are required to prevent the risk of re-identification.

(2) Medical Service Act

Health information, such as medical records generated by medical institutions, is protected under the Medical Service Act, and its provision to or use by third parties is restricted. Patient consent is mandatory for providing medical information externally, and violations are subject to strict penalties.

(3) Bioethics Act

The use of sensitive data, such as genetic information, requires approval from an Institutional Review Board (IRB), and certain conditions must be met even when the data is anonymised.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

There is comprehensive regulation at the national government level.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The regulation of personal health data usage varies depending

on the nature of the data (e.g., sensitive information, pseudonymised information) and the entities handling it (e.g., medical institutions, corporations). Personal health data classified as sensitive information is strictly protected under the Personal Information Protection Act and the Medical Service Act, requiring patient consent for external provision by medical institutions. Pseudonymised information can be used for research or statistical purposes without consent, but security measures are required to prevent re-identification.

4.4 How do the regulations define the scope of personal health data use?

The scope of personal health data usage is defined through various laws and guidelines, such as the Personal Information Protection Act, the Medical Service Act and the Bioethics Act. Emphasis is placed on balancing secure data utilisation with the protection of data subjects. For detailed information, please refer to the response for question 4.1 above.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

It is necessary for a researcher or a company to collect patients' health/medical data to develop new digital health technology. In this regard, the condition and extent of the collection and use of pseudonymised or anonymised personal data has become one of the key issues.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The current Personal Information Protection Act and relevant laws do not stipulate explicit regulations with respect to data inaccuracy, bias and/or discrimination.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

Safe collection and use of personal health data are supported through laws such as the Personal Information Protection Act and the Medical Service Act, as well as the My Healthway platform (government-initiated health data platform) and healthcare data utilisation guidelines. Focus is put on striking a balance between data protection and promoting research.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The Personal Information Protection Act separately regulates (i) "third-party provision" of personal data where data is provided for the third party's own business objectives or own benefit, and (ii) "third-party outsourcing" where the personal data is transferred to the third party for the third party's processing of data for the purpose of the data processor.

Third-party provision of personal data requires the data processor to obtain consent from the data subject, outlining the following items: (i) the identity of the third-party recipient; (ii) the third party's purpose of using the personal data; (iii) the items of personal data to be provided; and (iv) the retention and use period of the personal data by the third party.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Personal health data sharing is regulated under unified laws and regulations at the national government level.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Regulations governing the sharing and utilisation of personal health data vary depending on the entities handling the data (e.g., medical institutions, corporations) and the nature of the data (e.g., patient data, pseudonymised data). Medical institutions, under the Medical Service Act, cannot provide data to third parties without patient consent, and the use of data for research purposes requires approval from an IRB. Companies may utilise pseudonymised data under the Personal Information Protection Act, but its use is often restricted to research and public interest purposes rather than commercial objectives.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Please refer to the responses for questions 4.1, 5.1 and 5.3 above.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

While patient medical and health data are strictly protected under the Medical Service Act and the Personal Information Protection Act, technological advancement and the shift in healthcare focus from treatment to health management and preventive care, along with the emphasis on precision medicine, have raised awareness of the need for healthcare data sharing. Accordingly, the MOHW and the Korea Health Information Service are developing a Korea-specific technical standard (KR Core) based on Fast Healthcare Interoperability Resources and promoting integration with EMR and personal health record systems to support domestic standardisation. In response to these societal changes, the government is formulating and implementing policies as explained above.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Under the current Korean Patent Act, in principle, medical practices cannot be patented due to their industrial use not being

recognised for public policy reasons. It is considered that medical practices should contribute to the sustention of life and well-being of humanity rather than being protected by patent rights for the promotion of property interests of specific persons.

For example, an invention that has the human body as a direct component, such as a surgical method, treatment method or diagnostic method is not recognised as an industrial use invention (provided, however, the mode of operation or method of measurement of a medical device, which does not use the interaction with the human body or a particular medical practice as its component, may be protected by patent rights as its industrial use will be recognised). As an exception, in the case of a medical practice in which the human body is an indirect component or a non-medical practice in which the human body is a direct component, then industrial applicability is recognised and a patent may be obtained.

In the case of software, patent protection is applicable only when the information processing carried out by the software is concretely realised using hardware. Patent protection in this case can cover the information processing system that operates with the software, the method of operation, a computer-readable medium containing the subject software, and the program stored on the medium.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

For digital health solutions, the software may be protected as copyright or the database itself may be protected under copyright if it meets the requirements for a database under the Copyright Act (a compilation that systematically arranges or organises materials so that the particular materials may be accessed or searched). Copyright under the Korean Copyright Act arises from the time its subject is created and does not require any separate procedures or formalities. However, copyright registration has its benefits as it is presumed that the work was created and made public at the time of copyright registration, the registered author is presumed to be the true author, and the person who infringes upon a registered copyright is presumed negligent in the act of infringement. Thus, copyright registration makes it easier to prove infringement in case of a dispute, and it is relatively easier to protect against infringement even after the author's death. The duration of a copyright continues through the life of the author and for a period of 70 years after the author's death.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

According to the Korean Unfair Competition Prevention and Trade Secret Protection Act, three conditions must be met in order to be protected as a trade secret: (i) non-disclosure; (ii) manageability of confidentiality; and (iii) usefulness. Non-disclosure means that the content of the information is not publicly known. Confidentiality means that such information must be managed and kept by the holder of said information in confidence. Usefulness means that the information must be useful and hold independent economic value. Meanwhile, even if a trade secret is protected, unlike with patents, there is no effect of excluding a third party from independently developing and using such trade secret.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

The Technology Transfer and Commercialisation Promotion Act applies to, or regulates the transfer of technology developed by academic institutions. According to Article 2(2) of the Act, technology transfer includes the transfer of technology from the technology holder to others through means of transfer, licensing, technical advice, joint research, joint venture, or merger and acquisition. Academic institutions often conduct research by receiving research and development funding from the government, and in such cases the state or public institution will make efforts to secure intellectual property rights for the results of such research. In such situations, the state or public institution may vest the results to the joint research institution, and may even grant permission for its use to a third party for a royalty.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Medical device software in itself cannot be protected by a patent, but information processing devices (e.g., medical devices) that operate in conjunction with medical device software, the method of operation, and medical device software saved onto storage devices can be protected by a patent. In addition, medical device software may also be protected as a copyright.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

According to Article 33(1) of the Patent Act, those eligible to receive a patent are limited to "natural persons" who have made the invention or their successors. Since AI does not belong to the category of natural persons, the general principle, which is recognised by the court as well, is that AI cannot be recognised as the inventor for the purpose of obtaining a patent.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

In Korea, the National Research and Development Innovation Act regulates inventions and results of research conducted through government funding. This statute and its subordinate regulations regulate the ownership, management and utilisation of inventions and other output (including software, products and publications, as well as intellectual property rights such as patents) developed with support from the government. A research and development institution that generates profits from the outcome of such research and development must pay a certain percentage of the amount of profits to the state.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

Key examples include the precedent described in question

6.6 above, where AI was not recognised as an inventor, and cases where the Patent Office and related industries established patent examination guidelines to keep pace with the rapid growth of digital healthcare technologies. These include efforts to prepare and discuss specific guidelines for drafting specifications and defining the scope of rights.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

Two things may be taken into consideration with priority: (1) to whom an intellectual property belongs; and (2) the method of profit sharing.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

There is no general rule; however, it would be helpful to consider the following: (1) non-healthcare companies may not have an understanding of the applicable regulatory scheme (e.g., the requirements under the Medical Service Act); and (2) medical institutions are not permitted to conduct for-profit activities in principle under the Medical Service Act.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

As explained above, under the current Personal Information Protection Act, data sharing is permissible only for the purposes of statistical compilation, scientific research and public interest record preservation. Furthermore, to engage in data sharing, one must go through the procedures set forth by the Personal Information Protection Act, such as internal review processes within the institution that holds the information.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

As explained in question 2.3, the AI Basic Act passed the National Assembly plenary session on 26 December 2024. Korea is the second country in the world to establish a basic law on AI.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

The main regulatory authorities enforcing AI/ML-related regulations and their scope of enforcement are as follows, and these organisations collaborate to establish a balanced regulatory system that ensures the safety and ethical use of AI technologies while also supporting industry growth.

The MSIT:

- Leads the advancement of AI technology through the AI Basic Act (scheduled for implementation in 2026).
- Defines high-impact AI and generative AI as regulatory targets, establishes obligations for transparency and safety, and outlines the responsibilities of operators.
- Supports AI safety and reliability verification and certification.
- Formulates a National AI Master Plan every three years and promotes the AI ecosystem, including the development of AI data centres and clusters.

The MFDS:

- Pursuant to the Digital Health Products Act (scheduled for implementation in 2025), is responsible for the approval, review, quality management and clinical trial approval of AI-based medical devices.
- Supports ongoing updates through AI medical device change management plans and evaluates the safety and effectiveness of medical devices.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

As described in question 8.1 above, the AI/ML-related regulatory framework in Korea is built around the AI Basic Act and the Digital Health Products Act.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Under the current Korean Patent Act, the inventor is limited to natural persons. Under the current Korean Copyright Act, in principle, authors are limited to natural persons, but corporations and organisations can also become authors as exceptions.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Various commercial considerations should be taken into account when licensing data for ML. In such cases, ML is not to produce output by using the data itself, but to produce an algorithm or model that is output through training by using the data, thus the fact that this is different from conventional methods of data usage should also be considered.

For example, the method of using the data, the scope of the data provided, the type of data and its content, the form of data, and the extent to which the data is used (including temporal, regional and human scope), the right to products of ML using the data, and the right to sublicense should all be considered.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Regulatory authorities differentiate between standard AI

and generative AI through the AI Basic Act. The Act classifies standard AI as a relatively low-risk application technology, such as general data analysis, prediction and decision support. Generative AI, which generates new content such as text, images and speech, is classified as high-risk (high-impact) AI.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

The AI Basic Act requires that when an AI business operator provides products or services based on generative AI, they must notify users in advance that the product or service is operated using generative AI. Additionally, the AI business operator must indicate that the outcome of the product or service was generated by generative AI. In particular, when providing results such as virtual sounds, images or videos that are difficult to distinguish from reality, the operator must notify or indicate in a way that ensures users can clearly recognise that the result was generated by an AI system.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

Laws such as the Personal Information Protection Act and the Copyright Act are used to regulate the improper use of data. However, Korea does not have a particular disgorgement law like the one in the U.S.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

General tort liability and contractual liability doctrines established under the Civil Code will apply in principle. In addition, the Product Liability Act may also apply. However, if the damage occurs within the scope of adverse events or warnings disclosed or stipulated in the package insert prepared pursuant to the Medical Devices Act with the review of the MFDS, the aforementioned liability of the manufacturer or supplier of the subject medical device may be exempted.

9.2 What cross-border considerations are there?

The international cross-certification system has not been introduced in Korea.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Currently, most terms of service for generative AI include disclaimers regarding intellectual property infringement, specifying that users of the AI are responsible for any liability arising from intellectual property infringement. Therefore, to minimise infringement liability, it seems necessary to review potential intellectual property infringement risks associated with the particular results generated by the generative AI.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

In cases where AI/ML models misuse medical data, various legal responsibilities may apply, including those pursuant to the Personal Information Protection Act, the Medical Service Act, Civil Law (tort liability) and the Product Liability Act. Companies and healthcare institutions need to strengthen data protection measures and ensure strict compliance with ethical and legal standards in the design and operation of AI/ML solutions.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

The following issues are discussed in connection with the protection of personal data: (i) whether the consent of the data subject is required; (ii) cross-border transfer of personal data; and (iii) data security.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

As to the provision of medical services to patients, two requirements are satisfied under the Medical Service Act: (i) only licensed healthcare professionals are allowed to provide medical services; and (ii) medical services should be provided at medical institutions through *vis-à-vis* diagnosis or treatment, in principle. That said, non-healthcare professionals may provide general health information (not replacing physician's diagnosis or treatment of patients) to customers without violating the Medical Service Act. Further, the developer of digital health technologies should take into consideration reimbursement eligibility under the National Insurance Act as well as the MFDS's market approval.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Digital health is one of the fastest growing markets and the government also has a strong desire to nurture the digital health industry. However, easy access to healthcare services with a low-cost burden under the national health insurance system may be a challenge to the commercial success of a digital health product or service in the market.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

It is difficult for a digital health solution to replace traditional medical services under the Medical Service Act, which requires that the medical service be provided by a licensed

healthcare professional at a medial institution. Further, given the universal national insurance system in Korea, it would be necessary for a digital health solution to be eligible for the national health insurance reimbursement so as to be widely used by medical service providers.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

No significant guidelines have been provided by major clinician certification bodies.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

With regard to private insurance, it depends on each insurance company's policies, and no significant general policy consensus has yet been established in the industry. However, as far as the national health insurance is concerned, the following processes are required: (i) the MFDS's product approval or certification under the Medical Devices Act; (ii) nHTA under the Medical Service Act if a new health technology is to be adopted; and (iii) review and determination of reimbursement eligibility under the National Health Insurance Act.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Korea's digital health ecosystem has several gaps, including issues related to data quality and standardisation, algorithmic bias and regulatory uncertainty.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

The government has a firm view that the digital health sector is one of the key industries that will lead national growth in coming decades.

Jin Hwan Chung is a partner in the Corporate Practice Group at Lee & Ko, and the co-head of the Healthcare/Life Sciences Team of Lee & Ko. For many years, Jin Hwan has provided legal representation and counsel to numerous leading pharmaceutical and medical devices companies, as well as medical institutions including Archigen Biotech, AstraZeneca, Baxter, BMS, Bayer, Berna Biotech (Crucell), CSL Behring, CSL Seqirus, Daiichi Sankyo, Eisai, Johnson & Johnson, Janssen, Merck & Co., Mundipharma, Novartis, Novo Nordisk, Takeda, UCB, Boston Scientific, Fresenius Medical Care, GE Healthcare, Hologic, Intuitive Surgical, Johnson & Johnson Medical, Medtronic, MerzAesthetics, Samsung Medical Center, Seoul National University Medical Center and Yonsei Medical Center in connection with various transactions and compliance issues. As a corporate lawyer, Jin Hwan has been involved in many mergers and acquisitions, and has advised his domestic and foreign clients on anti-trust and anti-corruption issues as well. Jin Hwan is one of the highest regarded experts in the area of healthcare compliance and is also a popular lecturer on this area of law.

Lee & Ko
63 Namdaemun-ro, Jung-gu
Seoul 04532
Korea

Tel: +82 2 772 4711
Email: jinhwan.chung@leeko.com
LinkedIn: www.linkedin.com/in/jin-hwan-chung-9a533719

Eileen Jaiyoung Shin is a partner in the Corporate Practice Group and the Healthcare/Life Sciences Team of Lee & Ko. Her practice focuses primarily on the health industry, including the pharmaceutical and biotechnology products, medical devices, food, nutritional supplements, cosmetics, tobacco and public healthcare sectors. Eileen has advised many multinational companies in the healthcare industry on a broad range of regulatory, corporate and competition law issues. In addition, with respect to the pharmaceutical industry in particular, Eileen regularly advises multinational clients on new drug pricing and after-launch life-cycle management with the firm's active market-access practice.

Lee & Ko
63 Namdaemun-ro, Jung-gu
Seoul 04532
Korea

Tel: +82 2 772 4831
Email: eileen.shin@leeko.com
LinkedIn: www.linkedin.com/in/eileen-shin-7294b026

Sungil Bang is a partner in the IP Practice Group and the Healthcare/Life Sciences Team of Lee & Ko. His practice at Lee & Ko focuses on legal issues in the areas of healthcare and intellectual property, with a special emphasis on medical device, pharmaceuticals, food and cosmetics. In addition to his legal credentials, Sungil has an extensive background in pharmaceutical and medical sciences, including earning both a B.S. in pharmacology and an M.S. in medical science at Kyunghee University. As a result, Sungil has a particularly excellent contextualised understanding of pharmaceutical and medical technology and intellectual property, as well as the full range of legal and regulatory concerns in the pharmaceutical and medical business sectors in Korea.

Lee & Ko
63 Namdaemun-ro, Jung-gu
Seoul 04532
Korea

Tel: +82 2 6386 6685
Email: sungil.bang@leeko.com
LinkedIn: www.linkedin.com/in/sungil-bang-973356240

Mexico


Carla Calderón


Marina Hurtado Cruz


Daniel Villanueva


Carlos Vela Treviño

Baker McKenzie

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

While there is no legal definition for digital health under Mexican law, the term digital health is traditionally associated with any application of information technologies to the provision of health services and products.

In the last couple of years, there have been some law initiatives, including proposals to amend the General Health Law ("GHL") and specific Technical Standards (Mexican Official Standards – "NOMs") to expressly regulate some applications of digital health. However, none of these have been successfully passed.

The most ambitious initiative to date has been the standalone "General Digital Health Law". This initiative, for example, includes the following definition of digital health: "*[A]ctivities related to health, services, and methods, which are performed at distance with help of ITs and other technologies. It includes telemedicine, tele-education in health, and encompasses diverse technologies such as IOT, AI, machine learning, macro data, robotics and other technological developments that may exist.*"

Digital health has also been defined in the Global Strategy for Digital Health 2020–2025 by the World Health Organization ("WHO") as "*the field of knowledge and practice associated with the development and use of digital technologies to improve health*". According to the WHO's Global Strategy, digital health can be further conceptualised as either eHealth or mHealth.

On the one hand, eHealth encompasses the use of ICT by healthcare providers and patients to aid in prevention, diagnosis and treatment.

On the other hand, mHealth: "*[E]xpands the concept of eHealth to include digital consumers, with a wider range of smart and connected devices. It also encompasses other uses of digital technologies for health such as the Internet of Things, advanced computing, big data analytics, artificial intelligence including machine learning, and robotics.*"

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Insurtech, virtual healthcare services, electronic prescription, medical apps, portable medical devices (med tech), online platforms for e-commerce, different digital platforms for health services, electronic health records and online pharmacies.

1.3 What is the digital health market size for your jurisdiction?

According to Statista, Mexico's Digital Health market has grown for the last five consecutive years and is projected to reach US$2,412m in 2024. Revenue is expected to show an annual growth rate of 8.86%, resulting in a projected market volume of US$3,688m by 2029. Mexico's largest market will be Digital Treatment & Care with a total revenue value of US$1,258m in 2024.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

According to a Capital IQ Company Screening Report, the five largest by revenue digital health companies in Mexico are ASISTIA (online platform for nursing services), BIOANA (medtech), SOFIA (insurtech), YANA (artificial intelligence ("AI")-based wellness platform to provide mental health solutions) and Prix (e-pharmacy).

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

FemTech, Clivi (virtual healthcare services for diabetes and weight loss), Sofía (insurtech), Prix (e-pharmacy) and Prena.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The Federal Commission for the Protection against Sanitary Risks ("COFEPRIS") is the federal authority in charge of health regulation, which includes drugs, medical devices ("MDs") and healthcare services. COFEPRIS issues market authorisations for MDs and manages notices of operation for healthcare services. It also performs health inspections to the regulated actors to verify compliance with applicable regulations. COFEPRIS recently published an Advertising Guide for Influencers in connection with healthcare services, drugs, MDs and dietary supplements to capture these actors' activities that are currently not regulated.

The National Institute of Transparency, Access to Information and Protection of Personal Data ("INAI") is the data protection regulator in Mexico. The INAI has the purpose of disseminating knowledge for the right to the protection of personal data, promote its exercise and oversee the due observance of the provisions of the corresponding laws and regulations. In this capacity, the INAI can perform audits, request documentation and information, as well as enforce the rights of access, correction, cancellation, opposition, and revocation on public and private entities. However, in November 2024, a Constitutional amendment ordered the disappearance of seven autonomous entities tasked with overseeing government compliance in diverse areas, including the INAI. The disappearance of the INAI has created uncertainty about who will assume its functions. According to available information, the responsibilities for personal data protection that previously belonged to the INAI will be taken over by the new Secretariat of Public Function, which will become the Secretariat of Anti-Corruption and Good Governance. This new entity will be responsible for managing archives, the National Transparency Platform and sanctions related to personal data protection. Nonetheless, we are still waiting for the secondary regulations to confirm the attributions with respect to data protection. The Congress has 90 days to implement legal changes required for the disappearance of the INAI, after which the INAI will be considered legally dissolved. We are yet to see the scope of the legal adequations to implement the disappearance of the INAI and how these will work in practice.

The Federal Consumer Protection Authority ("PROFECO") is responsible for promoting and protecting the rights and interests of consumers and for ensuring fairness and legal certainty in relations between suppliers and consumers. Such mandate includes, the oversight of marketing and misleading advertising, e-commerce regulations and product/services warranties. In 2023, the PROFECO issued *The Advertising Guide for Influencers* to emphasise that influencers' activities on social media are considered advertising. The PROFECO is particularly active in sectors where there may be substantial risk for individuals or vulnerable groups, which includes health services and products.

Meanwhile, the Mexican Institute of Intellectual Property ("IMPI") is the competent authority for the protection and enforcement of IP rights.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

Mexico does not have a comprehensive and dedicated regulation for digital health. However, the health regulatory framework applies to many product and services categories, which can capture digital health applications.

The framework law is the GHL, from which stem several Secondary Regulations that set forth rules for: (i) products, including drugs and MDs; (ii) establishments, including manufacturing plants, warehouses, pharmacies, hospitals and doctor offices; and (iii) activities, such as research and advertisement. More detailed subjects are regulated in the Technical Standards (NOMs for its acronym in Spanish), including labelling, techno vigilance and good manufacture practices.

Noteworthy, the product category of MD is very relevant for digital health applications. MDs include the sub-categories of medical equipment, prostheses, diagnostic tools, dental products, surgical and healing products, and hygienic products.

On December 21, 2021, NOM-241-SSA1-2021 on Good Manufacturing Practices for Medical Devices ("NOM-241") introduced the concept of Software as a Medical Device ("SaMD"). On July 26, 2024, a draft amendment for NOM-241 was published, which, among other modifications, expands the definition of SaMD and delegates regulation of the manufacturing of SaMD to the Mexican Pharmacopeia.

The Mexican Pharmacopeia also contains technical requirements that are relevant for digital health. On the one hand, its *Supplement on Establishments* contains key requirements for accepting e-prescriptions in pharmacies. On the other hand, the recently amended *Supplement on MDs* introduced a full Appendix on SaMD which contains detailed rules for the definition of SaMD, classification of the risk level, quality system, clinical evaluation and mobile apps. To date, this is the most detailed legal instrument for the regulation of digital health applications. The General Constitution (the "Constitution") sets forth the basic privacy rules and rights. From there, the Federal Law on the Protection of Personal Data held by Private Parties ("FDPL" or the "Law") and the General Law on the Protection of Personal Data held by Government Agencies ("GLPPD" or the "Law"), provide detailed rules for private and government entities in connection with the basic privacy rules considered by the Constitution. The INAI or the entity that assumes its responsibilities due to the INAI's recent disappearance, is permitted to issue secondary regulation and is entitled to enforce the Law. However, other agencies, such as the Ministry of Economy, may also issue privacy-related rules under the umbrella of the FDPL. Such laws regulate the processing of personal and sensitive data, which includes the complete cycle of such data, from its collection, storage, transfer and deletion. Different from other jurisdictions, in general, privacy laws in Mexico are Omni-sectorial; therefore, there are no particular regulations for health data. Instead, data protection is regulated by the laws mentioned herein, across all sectors and industries. Other laws, such as the Federal Law for Consumer Protection, provide guidance for e-commerce, which has been complemented by a NOM and a Code of Ethics on e-commerce, a NOM for e-signatures, as well as regulations for financial institutions and payments processors. An imminent amendment to the Secondary Regulations of Medical Products has been in the works since 2023. It is expected that it will include regulations on the e-commerce of medical products, which may include SaMD.

While Mexico has two different regulations for data protection, one for the private sector and one for public entities, both supply protection for the processing of personal data and sensitive personal data which includes past, present and future health data. Further to the principal requirements for the processing of personal data, which require the delivery of a privacy notice to the data subjects, the law considers monetary fines for the misuse of personal data, which are double the regular amount, when sensitive personal data is involved. Such regulatory compliance and the risk of misuse of sensitive personal data, which may result in fines, impose a big legal issue for the development of digital health in Mexico. In addition, because of the nature of digital health services, it is important for companies involved in the sector to consider having privacy by design in their concepts, as well as to conduct privacy impact assessments prior to their implementation. While it may be debatable that privacy impact assessments are mandatory, the INAI had publicly recommended their implementation, a trend that is likely to continue even

with the INAI's recent disappearance as it will likely be embraced by the entity that ultimately assumes the INAI's data protection authority. Also, the latent risks of being involved in a data breach or being subject to cybercrime activities increase the possible legal and reputational issues in Mexico.

Depending on the technology used in digital health services, there may be other regulatory issues, such as compliance with technical standards, considered by the NOMs or other laws and regulations such as the Federal Law of Telecommunications, particularly for the use of radio spectrum and the provision of telecommunication services.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

In the context of digital health, the most relevant regulatory category would be that of MDs, which includes the sub-categories of medical equipment, prostheses, diagnostic tools, dental products, surgical and healing products, and hygienic products. Furthermore, by recent addition, it also includes the sub-category of SaMD.

From a health regulatory perspective, digital health applications may constitute a product, a service or both. Once a regulatory category is triggered, a significant number of different obligations and requirements become binding.

On the one hand, if a digital health product is found to constitute a MD, for example, not only would the obligation to obtain a prior marketing authorisation be triggered, but also other regulatory requirements, including (i) product-related requirements, such as advertising rules, (ii) establishment-related requirements, such as rules for good distribution practices, or (iii) company-wide requirements, such as operating a techno-vigilance system.

On the other hand, if a digital health application is found to constitute a healthcare service, a variety of requirements are triggered, including (i) filing a notice of operation for at least a consulting room (or clinic or hospital), (ii) having a licence to practise for the physician, and (iii) operating the consulting room in full compliance with other technical requirements.

From a data protection perspective, this can be addressed by looking at sanctions and fines. The health sector and related industries have been one of the most fined. Regardless of the industry, the list of activities that are grounds for most sanctions has stayed the same as previous years, including: (1) processing personal information against the principles of the law; (2) collecting or transferring personal information without the consent of the data subject; and (3) omitting any of the minimum mandatory informational elements in the privacy notice. The INAI was a highly active regulator as is shown in its latest report for the first semester in 2023, with 91 recorded proceedings and having concluded 74 of them, which derived in total MX$46m in fines (approx. US$2.3m). The INAI also began 293 Right Requests to confirm compliance with the law, from which 155 relate to the access right, five to rectification, 122 to cancellation and 79 to opposition. In addition, the INAI encouraged companies with respect to the processing of biometric data and had lately taken the position in different scenarios that biometric data must be considered sensitive personal data; therefore, it should be processed as such, including a heightened level of diligence and security, since the fines derived from the misuse of sensitive personal data are double of the amount considered for misuse of non-sensitive personal data. Such position will likely continue.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

NOM-241 incorporated as a sub-category the notion of SaMD and the Supplement on Medical Devices of the Pharmacopeia, which was amended in 2023 to introduce a full Appendix X on SaMD, are the applicable regulations to SaMD and its approval for clinical use.

This Appendix establishes six objectives: (i) establishing harmonised definitions (including input data, output data, algorithm, definition statement and real-world performance data); (ii) establishing key considerations of the life cycle process (including requirements, design, development, testing, maintenance and use); (iii) providing guidance on the application of quality management system practices; (iv) standardising the terminology used for the software industry and integrating regulatory concepts to software engineering activities; (v) establishing a common understanding of clinical evaluation to demonstrate the safety, effectiveness and performance; and (vi) providing guidance on mobile applications.

This regulatory instrument is based heavily on the regulations developed by the International Medical Device Regulators Forum, which created the term SaMD, and the last section on Mobile Apps is heavily based on regulatory concepts adopted by the US Food and Drug Administration ("FDA"), such as listing certain apps in relation to which the FDA would reserve its discretion to exercise regulatory powers.

Apart from those category-specific provisions, the whole regulatory framework for MDs would be applicable to SaMD, including the GHL, the Secondary regulations for Medical Products, NOM-137-SSA1-2008 on the labelling of MDs and NOM-240-SSA1-2012 on techno vigilance.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

In 2018, Mexico issued an AI Strategy to create a framework for the development of an AI, becoming the 10th country to formalise an approach to AI. However, the former Administration of President Andrés Manuel López Obrador decided not to carry on with this strategy. It is very early in the new administration of President Claudia Sheinbaum and we are yet to see if developing regulations for AI/machine learning ("ML") is generally on the agenda. Therefore, it is unlikely we will see any policy development on AI soon. Nevertheless, since 2023, there are two draft bills that aim to regulate AI healthcare applications being discussed in the lower chamber (*Cámara de Diputados*).

Since Mexico does not have a particular regulation addressing AI or ML, their healthcare applications are regulated only by the health regulatory framework mentioned above.

Depending on the application and business model of certain AI or ML, one or more regulatory schemes would be triggered, including the regulation for the processing of personal data through automated decision-making technologies.

The INAI had published its Recommendations For The Processing Of Personal Data Arising From The Use Of Artificial Intelligence, which aim to disseminate knowledge and the relationship of AI/ML with the fundamental right to the protection of personal data, to promote the appropriate and

ethical use of personal data through the different technologies that use AI/ML for their operation and compliance with the obligations of the duty of security of personal data, for those responsible for the private and public sector that develop or use AI products or services.

The foregoing should not undermine the importance that those responsible for the processing of personal data must also comply with the other principles and duties established in the applicable legal frameworks. Similarly, this approach will likely continue with the new entity that will assume the INAI's authority.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

See question 2.4 above.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

See question 2.4 above.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Regulation of medical products, which encompasses the regulatory category of MDs, are regulated at a federal level. As mentioned above, NOM-241 and Appendix X of the Mexican Pharmacopeia are the only specific provisions for digital health products and solutions, which are applied together with the general regulatory framework of MDs.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

See question 2.4 above.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  From a health regulatory perspective, the absence of specific rules for telemedicine means that this is regulated through the existing general rules applicable to medical consulting rooms, which presuppose a brick-and-mortar establishment. This can be difficult to understand by new players proposing digital platforms.
  From an information technology regulatory perspective, the core issues include the processing of personal and sensitive personal data and the challenge of having to comply with the mandatory regulations, including having to obtain express consents, such as those necessary for: (i) the processing of sensitive personal data, including health data; and (ii) transferring the personal data to a third party (with some exceptions).
- **Robotics**
  From a health regulatory perspective, there are no major issues, as robotics could constitute medical equipment, a sub-category of MDs.
  Rather, challenges may exist in relation to IP protection. Further to the protection granted for the mechanical parts and configuration, there may be challenges regarding patenting software. While software can be protected as a copyright, the rapid change in its code sometimes makes it not worth having copyright registrations for the same and rely on the automatic protection for copyrights. Nonetheless, there are situations where registration is required for other situations, such as government grants, and it is always a good practice where possible. When developing robotics in Mexico, companies must make sure to secure ownership of the developments by having the correct contractual frameworks with their employees and/or contractors.
- **Wearables**
  Wearables may be considered MDs, depending on whether they serve a medical purpose. Many of them often act as diagnostic tools.
  With respect to privacy, it is important to consider privacy by design and privacy impact assessments, as well as to always consider that data subjects in Mexico are entitled to a reasonable expectation of privacy. In addition, it must be considered that when data controllers desire to use Cloud services for the processing of personal data, and the data controller simply adheres to the Cloud services terms and conditions, the Cloud services provider must comply with certain minimum mandatory requirements. Otherwise, in theory, the data controller would be prevented from contracting with such Cloud services provider.
- **Virtual Assistants (e.g. Alexa)**
  The main challenges relate to privacy, in the same terms described above.
- **Mobile Apps**
  Mobile apps would fall within the same regulatory category of SaMD, thus sharing the same challenges and regulation. It is often the case that there is a blurred frontier between wellness apps and medical apps. Regulatory definitions are key to draw distinctions (e.g., definition of mental health) and the new Supplement on Medical Devices of the Mexican Pharmacopeia has certainly shed light in this regard, but we are yet to see COFEPRIS's interpretation of these definitions.
- **Software as a Medical Device**
  A full set of provisions for SaMD have been recently introduced, as mentioned in questions 2.2 and 2.4. The main challenges are the same described above.
- **Clinical Decision Support Software**
  On the one hand, the provision of healthcare services, including mental healthcare, is legally conceived as being provided by licensed healthcare professionals, not machines or software. Therefore, clinical decision support software may be used as an auxiliary to the decision-making process of the healthcare professional. At the same time, under the new product sub-category of SaMD, a clinical decision support software could constitute a MD, requiring a prior marketing authorisation.
  On the other hand, professional liability for medical negligence can only arise from acts or omissions committed by a healthcare professional, assessed against *lex artis*; in contrast, product liability would arise where a product did not perform according to its announced, intended or approved function.

- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  The most relevant regulatory category would be regarding MDs, thus the same challenges described above for other digital health applications would apply. At the same time, under the new product sub-category of SaMD, this would constitute a MD, requiring a prior marketing authorisation.
  At the same time, there are issues related to the collection of real-world data from patients. This kind of data is not yet fully incorporated in the Mexican regulatory framework. For instance, it is not clear whether it can be used to support approval decisions.
  On the other hand, there is significant uncertainty in relation to the learning aspect, which requires the constant use of performance data from the user. If this is considered clinical research, it would be subject to an ethics and regulatory approval of the research protocol.
  The same challenges with respect to IP, data protection and privacy, as mentioned above, also apply.
- **IoT (Internet of Things) and Connected Devices**
  The same challenges with respect to IP, data protection and privacy, as mentioned above, also apply. Currently, there are no regulatory guidelines, although this may change at any time.
- **3D Printing/Bioprinting**
  Mexico has not yet issued regulations on 3D printing or in relation to bioprinting, although this may change at any time. Due to the absence of rules, product classification issues may arise regarding the bioprinting of tissues or organs. Noteworthy, ultimately, the place where the printing takes place will be considered the manufacturing site and would have to comply with applicable establishment requirements.
- **Digital Therapeutics**
  Mexico has not yet issued regulations on digital therapeutics. Although in some jurisdictions the relevant product categories for digital therapeutics would include both MDs and medicines, it is likely that in Mexico, they would be framed as a MD.
- **Digital Diagnostics**
  As with all digital health applications, there are no specific regulations for digital diagnostics, hence providers are bound to comply with regulation applicable to a physical version of the model. This includes the same challenges as telemedicine, and further adds that healthcare professionals engaged in the diagnostic must be licensed by competent Mexican authorities.
  Nonetheless, the same challenges would apply with respect to data protection and privacy, including the regulation for the processing of personal data through automated decision-making technologies.
- **Electronic Medical Record Management Solutions**
  The same challenges with respect to data protection and privacy, as mentioned above, also apply. Currently, there are certain regulatory guidelines, although this may change at any time. The Mexican Official standard NOM-004-SSA3-2012 establishes the mandatory scientific, ethical, technological and administrative criteria for the preparation, integration, use, management, filing, preservation, ownership, title and confidentiality of a clinical record.
- **Big Data Analytics**
  The same challenges with respect to data protection and privacy, as mentioned above, also apply. Currently, there are no regulatory guidelines, although this may change at any time. Nonetheless, companies must consider the regulation for the processing of personal data through automated decision-making technologies, which may be applicable to some extent.
- **Blockchain-based Healthcare Data Sharing Solutions**
  The same challenges with respect to intellectual property, data protection and privacy, as mentioned above, also apply. Currently, there are no regulatory guidelines, although this may change at any time.
- **Natural Language Processing**
  Natural language processing has not yet been discussed by the health regulator in Mexico. However, the same challenges, described above, for other digital health applications would apply.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

As mentioned in question 3.1, due to the absence of specific rules for digital platform providers in the digital health space, these providers are regulated through the existing general rules applicable to digital health applications (i.e. products, services or establishments), which presuppose in-person interactions and/or a brick-and-mortar establishment. This can be difficult to understand by new players proposing digital platforms.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

In accordance with the information published by the INAI for 2023, the key issues to consider for use of personal data are: (1) the processing of personal information in accordance with the principles of the Law; (2) collecting or transferring personal information only with the consent of the data subject; and (3) delivering and complying with the minimum mandatory informational elements in the privacy notice. However, there are others that should also be considered, such as considering the nature of the data (whether it is personal data or sensitive personal data), the reasonable expectation of privacy, implementing privacy by design, conducting privacy impact assessments, and having a privacy officer or similar function within the company that may address any data subject request. These issues are expected to continue having a substantial impact, regardless of whether the INAI remains the data protection authority.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

As mentioned above, privacy laws in Mexico are omnisectorial; therefore, there are no regulations for health data.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

While both the public sector and private sector laws are omni-sectorial, their application depends on whether the entity is public or private. Other than such distinction, the considerations do not change depending on the nature of the entities involved.

4.4 How do the regulations define the scope of personal health data use?

"Processing" is defined as the collection, use, disclosure or storage of personal data, by any means. Use encompasses any action of access, handling, use, exploitation, transfer or disposal of personal data.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

Contractual obligations may vary depending on the agreement's nature. For data transfers to a data processor, the agreement must show the existence, scope and content of the processing activities. In particular, it should also address the principal obligations for data processors: (i) to process personal data only in accordance with the instructions of the data controller; (ii) to refrain from processing the personal data for purposes other than those instructed by the data controller; (iii) to implement security measures in accordance with the Law; (iv) to maintain confidentiality with respect to the personal data processed; (v) to delete the personal data processed once the legal relationship with the data controller has been fulfilled or upon instructions from the data controller, provided that there is no legal provision requiring a retention period for personal data; and (vi) to refrain from transferring the personal data except where the controller so determines, the communication derives from subcontracting, or when so required by the competent authority.

For transfers to a third party as a new data controller, the agreement between the transferor and recipient must show that the transferor communicated to the recipient the conditions under which the data subject consented to the processing of the personal data. International transfers must consider at least the same obligations to which the controller transferring the personal data is subject, as well as the conditions under which the data subject consented to the processing of his or her personal data. There is a special regime for transfers between entities that belong to the same corporate group, where the transfers do not require consent to the extent that such entities run under the same data protection policies, where such policies are aligned with the principles of the Law.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

From a data protection perspective, personal data must always be complete and correct, imposing an obligation for data controllers to comply with such requirements. While bias and/or discrimination have not been formally addressed in connection with information technology, the Mexican government has provided, particularly for AI, that:

> *"AI actors must respect the rule of law, human rights, and democratic values throughout the lifecycle of data within the AI system. These include freedom, dignity and autonomy, privacy and personal data protection, non-discrimination and equality, diversity, equity, social justice, and internationally recognized labour rights."*

This has also been quoted by the INAI in its Recommendations for the Processing of Personal Data Arising from the Use of Artificial Intelligence.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The law applies to entities located in Mexico and to entities located abroad; specifically, under the implementing regulations of the Law, the regulation applies to entities located abroad: (i) if the data is processed in the place of business of the data controller located in Mexico; (ii) if the data is processed by a data processor (regardless of location) who is acting on behalf of a data controller located in Mexico; or (iii) if the data controller is not located in Mexico, but uses means located in Mexico to process personal data, unless such means are used only for transit purposes. While no definition of "means" is provided by the Law, this provision is likely to be interpreted broadly. In that regard, entities that are subject to the application of the law must primarily: (i) deliver a privacy notice that complies with the minimum mandatory information under the Law, the implementing regulations and the privacy notice guidelines; and (ii) obtain consent which must be express for the processing of sensitive personal data and financial data but may be tacit where no such special categories are processed.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Please see question 4.5.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

As mentioned above, privacy laws in Mexico are omni-sectorial; therefore, there are no regulations for health data.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Other than the considerations in question 4.5, because of the omni-sectorial nature of the law, these are not altered depending on the nature of the entities involved.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

The most like a governmental initiative to establish a standard regarding the sharing of health information is NOM-024-SSA3-2012. This NOM regulates Information Systems of the Digital Health Record and establishes the mechanism for healthcare providers to record, exchange and consolidate information. However, even though NOM-024-SSA3-2012 entered into force in 2012, we are still waiting to see implementation on a large scale.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Companies that share any personal data, including health data, must either: (i) have the data subjects' express consent for the transfer, having informed the data subjects in the corresponding privacy notice about the identity of the recipient and the purpose of the transfer, if the transfer is made on a controller-to-controller basis; or (ii) execute an agreement with the recipient, as described in question 4.5, if the transfer is made on a controller-to-processor basis, where the recipient only processes the personal data on behalf of the controller and once the relationship is over, the recipient deletes the data.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Patents protect inventions, including those related to digital health technologies. The Mexican Federal Law for the Protection of Industrial Property ("FLPIP") states that an invention is any human creation that allows the transformation of matter or energy that exists in nature, for its use by humans to cover their specific needs. Inventions can be products or processes.

Not all human creations can be considered inventions. The FLPIP establishes some exceptions (Art. 47), such as the following: discoveries, scientific theories or their principles; mathematical methods; literary, artistic works or any other aesthetic creation; the schemes, plans, rules and methods for the exercise of intellectual activities, for games or for economic-commercial activities or to conduct business; computer programs as such; the ways of presenting information; the biological material as found in nature; and the combination of known products or inventions unless their combination cannot function separately or that the characteristics of the same are modified to obtain an industrial result or use not obvious for a person skilled in the art.

Furthermore, the FLPIP states that inventions in all fields of technology, including digital health technologies, that are (i) new (i.e. are not in the state of the art), (ii) the result of an inventive activity (i.e. results are not deduced from the state of the art in an obvious way for a person skilled in the art), and (iii) capable of industrial application (i.e. the invention can be produced or used in any branch of economic activity) shall be patentable (Art. 48).

The initial term of protection of a patent is 20 years. Supplementary Certificates are available for patents filed in Mexico from July 1, 2020, when there are unreasonable delays in the prosecution of the patent attributable to the IMPI, that are translated in a period of more than five years, between the filing date in Mexico and the granting date. Regarding computer programs as such, these are excluded from patent protection; however, computer-implemented inventions related to digital technologies, that involve the use of a computer, computer network or other programmable apparatus, can be patented if they meet the patentability requirements and contain technical features.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Copyrights cover literary and artistic works. Computer programs as such, including those related to digital health technologies, are protected as Copyrights.

The Mexican Federal Copyright Act ("FCA") establishes that the works protected are those of original creation capable of being disclosed or reproduced in any form or medium (Art. 3 FCA).

Protection is granted to works from the moment they have been fixed on material support, regardless of merit, destination or mode of expression. Fixation is the incorporation of letters, numbers, signs, sounds, images and other elements in which the work has been expressed, or of the digital representations of those, that in any form or material medium, including electronic ones, allow their reproduction (Arts 5 and 6 FCA).

The recognition of copyright and related rights does not require registration or documents of any kind, nor will it be subject to the fulfilment of any formality (Art. 5 FCA). However, it is recommended to voluntarily register the art works with the Copyright Institute as a preventive action to have a precedent of the existence of this right.

In accordance with Art. 14 of the FCA, the following are not subject to copyright protection: the ideas themselves, formulas, solutions, concepts, methods, systems, principles, discoveries, processes and inventions of any kind; the industrial or commercial use of the ideas contained in the works; the schemes, plans or rules to carry out mental acts, games or businesses; the letters, digits or isolated colours, unless their stylisation is such that it is converted into original drawings; among others.

Copyrights grant their holders moral rights and economic rights. The first are inalienable, imprescriptible and unseizable. The second are valid during the life of the author and up to 100 years after his/her death.

Unlike patents, copyrights protect the expression, not the ideas or the technical features. Therefore, referring to computer programs of digital health technologies, copyrights protect the software whether in source or object code.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

The FLPIP defines trade secret as any information of industrial or commercial application, including information related to digital health technologies, that keeps the person who legally controls its confidentiality. This information represents for its owner the obtaining or maintenance of a competitive or economic advantage over third parties in carrying out economic activities and in respect of which it has adopted sufficient means or systems to preserve its confidentiality and restricted access to it.

Information regarding a trade secret may be contained in documents, electronic means or magnetic, optical discs, microfilms, films or in any other medium known. A trade secret owner shall adopt sufficient means to keep the confidentiality of the information and restrict access to it.

It shall not be considered a trade secret if the information is in the public domain, the information turns out to be known or is easily accessible to persons within the circles in which that information is used, or if it must be disclosed by legal provision or by court order.

The FLPIP entered into force in 2020, strengthening the protection of trade secrets and providing more legal certainty on this area. The FLPIP states a new definition of trade secret, indicated in the paragraphs above, as well as a definition for misappropriation and misappropriation infringement and offences. Similarly, it includes additional defences excluding certain information from being considered a trade secret.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

There is no general IP framework for academic technology transfer; general IP and contractual laws apply. Additionally, each Higher Education Institution has its own regulation that shall be considered, including specific restrictions on IP ownership and royalties. When collaborating with a university or institution, it is highly recommended to previously review any restrictions and agree the conditions in which intellectual property will be developed and protected to avoid future conflicts.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

There is no specific regulation for the IP protection of SaMD, so the general rules apply. In this way, the software, whether in source or object code, can be protected as copyright. If the software is related to a computer-implemented invention that meets the patentability requirements established by the FLPIP and that has technical features, it could be subject to patent protection.

In addition to the above, it is important to mention that, for example, the animated sequences and graphical interfaces of a MD application can be protected as industrial drawings.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

No. Under the FCA, only individuals can be considered authors. Similarly, under the FLPIP, only individuals can be considered inventors. Therefore, currently under Mexican laws, only individuals can be considered creators.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

There is no general regulation related to government-funded inventions in Mexico. However, public health institutions are subject to a different set of administrative law rules, which may contain IP-relevant provisions, which need to be studied on a case-by-case basis. Similarly, the rules regarding issues of ownership or licensing of government-funded inventions may vary depending on the specific programme, so terms and conditions should also be reviewed on a case-by-case basis. For general patent protection issues, the general rules under the FLPIP would be applicable.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

We are yet to see IP issues related to AI/ML applied to digital health litigated in the Courts. However, a recent resolution in Mexico has confirmed that copyrights created by an AI are not protectable under Mexican copyright law. This decision is based on the principle that only human creators can be considered authors under current legislation. The ruling emphasised that intellectual creations require a human element of creativity and originality, which an AI, as a non-human entity, cannot provide. This resolution underscores the need for clear legal frameworks to address the growing presence of AI in creative fields.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

There must be a written agreement describing the scope of the collaboration and the obligations for each party. It must be agreed beforehand whether the resulting intellectual property can be used by each participant independently or if there should be a collective agreement from all or part of the same. Similar rules must be agreed for the transfer (licensing or assignment) of any resulting intellectual property. In addition, it must be considered that neither the FDPL nor GLPPD consider the existence of a co-controller status. Therefore, only the entity that decides on how the processing takes place would be considered as the data controller. Further to this, the transfer of personal data to a third party that is not another entity part of the same corporate group of the data controller or a data processor would require the data controller to obtain express consent from the data subject prior to the transfer. Lastly, certain collaborative improvements may constitute technical modifications to MDs that warrant either a modification to an existing Market Authorisation or a new Market Authorisation. The agreement shall also consider who will be the Market Authorisation holder, and in the event of termination of the agreement, who will maintain the Market Authorisation.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

General considerations regarding confidentiality, data privacy, intellectual property, damages, liability and warranties would apply to agreements between healthcare and non-healthcare companies. On the other hand, business models in healthcare typically require addressing technical issues such as quality control and post-commercialisation

vigilance obligations, which may require supplementary agreements. At the same time, it must be considered that regulatory approvals constitute intangible assets, the ownership of which needs to be defined in the related contracts. Also, it is important to remember that certain regulatory categories carry certain restrictions to the business model. For instance, the regulatory approval for a MD cannot be held by a foreign company, as it occurs with medicines, thus a local legal entity, most likely a distributor, would have to be the owner and responsible for the product approvals.

Considerations more specific to digital healthcare developments include considering the background of the two industries that converge in this sector. Healthcare companies come from a highly regulated industry and are therefore used to the burden of obtaining health authorisations from innovation to post-marketing. Moreover, they expect their return on investment in a much longer time frame, where the trial-and-error process from molecule to medicine takes several years.

In contrast, digital companies have emerged in a context of the absence of regulation, where innovations can be introduced to the market with little or no regulatory barriers and return on investment can be made much faster.

Therefore, it is important to manage the expectations of digital health companies regarding the time frames for introduction to the market of digital health developments and the time frame for obtaining a return on investment.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

When collecting health data for ML purposes, caution must be had since this may likely constitute health-related research and require health authorisations from an Ethics Committee and the approval of a research protocol from the COFEPRIS. Likewise, if the application is considered an experimental product, concerning which data is collected to prepare a dossier for obtaining a Market Authorisation in Mexico, then it would certainly require a Market Authorisation for its commercialisation. The agreement should therefore consider the obtention of the required health authorisations and allocate the responsibility in relation thereto.

Companies that share any personal data, including health data, must comply with the requirements described in question 4.5.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

As mentioned above, digital health solutions may require health authorisation. Before entering the Mexico market, it is highly recommended to consult with a local legal expert regarding whether a specific digital health solution triggers a regulatory framework.

In Mexico, only licensed health professionals may provide healthcare services. Thus, a limitation of a digital health solution could be that it may claim to assist licensed health professionals in providing healthcare services but may not claim or pretend to perform or render these services in and of itself.

In relation to intellectual property, it is important to review the terms and conditions of the tool used to obtain generative AI to determine the ownership and licensing rules for IP rights. Likewise, it is important to consider that there is a risk of invading the IP rights of third parties.

From a data protection perspective, companies using generative AI in the provisioning of digital health solutions must consider the rules for processing personal data with Cloud service providers, as described in question 10.1. In addition, companies must consider that the data controller remains the sole party responsible for compliance with Mexican data protection laws, even in the case that the misuse of personal data may come from the service provider.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

Please see questions 2.1, 2.2 and 2.5.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

Please see questions 2.1, 2.2 and 2.5.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Under Mexican copyright law, only individuals can be considered authors. Similarly, under the FLPIP, only individuals can be considered inventors. Therefore, currently under Mexican laws, only individuals can be considered creators.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

The commercial considerations are whether the data includes personal data and having to comply with the data transfer requirements set forth herein. However, from an IP perspective, to the extent that the data is embedded on a database, it would be necessary to address the requirements of the Copyright law and regulate ownership of any derivative works.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Please see questions 2.1, 2.2 and 2.5.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Please see questions 2.1, 2.2 and 2.5.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

In Mexico, the legal landscape surrounding trained AI/ML models that may include data for which the developer lacks appropriate data rights is evolving. Currently, there are no specific data disgorgement laws directly addressing this issue. However, general principles of data protection and IP law apply.

Mexican copyright law stipulates that only individuals can be considered authors and inventors. Thus, individuals are the only recognised creators under the law. This principle extends to the development and improvement of AI/ML algorithms.

When it comes to using data for AI/ML, commercial, contractual and strategic considerations are paramount, particularly when licensing data. For healthcare data, these considerations are even more stringent due to the sensitive nature of the information and compliance with data transfer requirements as per the Mexican data protection regulations.

From an IP perspective, if the data is embedded in a database, it is subject to the requirements of the Copyright law, and ownership of any derivative works must be clearly regulated in licensing agreements.

As for regulatory oversight, there is no clear differentiation between standard AI and generative AI technologies by the regulatory bodies in Mexico. However, ongoing initiatives aim to develop and refine regulations specific to generative AI, ensuring that the unique challenges and legal issues posed by these technologies are addressed appropriately.

In summary, while Mexico does not have explicit data disgorgement laws for AI/ML models, the existing framework of data protection and IP laws provide a basis for addressing unauthorised use of data. Continued development and refinement of regulations will be crucial as the use of AI/ML technologies expands.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

From a health regulatory perspective, health-related "product liability" is not well developed in Mexico. The most explicit rules relate to liability from clinical trials, where the only clear provision creates an obligation for the sponsor to cover for the medical treatment required to address medical complications directly related to the clinical research, although it is not as clear in relation to a wider notion of damage.

In turn, in relation to health-related "services", the notion of liability falls squarely in the field of medical negligence, where it is physicians (physical individuals) who may be subject to professional liability for acts or omissions assessed against the *lex artis*.

In terms of general rules of damages, in Mexico there is contractual and non-contractual liability. Within non-contractual liability, there are different scenarios:

(a) Objective liability for inherently risky goods – This takes place: (i) under the consumer protection regime, when the supplier fails to deliver the Instructions of Use; and (ii) under the civil code regime, unless it is demonstrated that the damage occurred due to fault or inexcusable negligence of the victim.

(b) Subjective liability – This requires an illegal conduct and takes place unless it is demonstrated that the damage occurred due to fault or inexcusable negligence of the victim.

At the same time, under the regime that controls technical standards, manufacturers must comply with quality control systems, which will be crucial when assessing the standard of care under the subjective liability system.

Finally, Class Actions were introduced in Mexico in 2011; and although healthcare was not explicitly included, the private healthcare market falls within the scope of the consumer protection law, which applies to the relationship between suppliers and consumers. However, in 14 years there has not been any Class Action in the healthcare sector.

9.2 What cross-border considerations are there?

Digital health has a cross-border nature, materialising the possibility of supplying healthcare services not only at a distance, but from another country. This at once begs the question of where the digital healthcare provider should be licensed in his/her place of residence or in the patient's place of residence? Would health import permits be required for digital health applications such as SaMD? Likewise, the absence of international harmonisation in the regulation of digital health means that digital health companies must follow different sets of regulations for the same product or service, in the different countries where they may have presence.

Cross-border data sharing is another relevant consideration (see question 4.5), as well as the possibility to file for patents or register trademarks in other countries, under the Patent Cooperation Treaty or the Madrid System.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

To minimise liability risks in the use of generative AI in the provisioning of digital health solutions, before entering the Mexico market it is recommended to consult with a local legal expert to establish whether a certain solution triggers a regulatory framework and which, if any, health authorisations are required. Likewise, care must be taken with the claims of the digital health solution since it may exclusively assist healthcare professionals in their role but is precluded from providing healthcare services. From a data protection perspective, companies using generative AI must assess and confirm that the terms and conditions of the AI provider complies with the rules for processing personal data with Cloud service providers.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Under Mexican law, the misuse of healthcare data in AI/ML models can invoke several liability theories, including breaches of the FDPL due to improper consent or protection and civil liability for damages resulting from unauthorised use or disclosure of health information. Companies must comply with regulations set by health authorities like COFEPRIS, and non-compliance can lead to fines and mandatory corrective actions. To minimise liability, companies should implement robust data protection measures, obtain explicit consent for

data use, regularly update data protection policies and ensure AI/ML models comply with ethical guidelines even if there are no particular AI laws that provide a mandatory application.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

If the data processor is a Cloud-based services provider, and the data controller merely adheres to a contract, certain minimum requirements must be included in the standard-terms contract. Otherwise, Mexican companies are prevented by law from contracting such providers. The INAI published minimum guidelines regarding contracting Cloud service providers.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Key issues that non-healthcare companies should consider before entering the digital healthcare market are that healthcare products with medical purposes typically require a longer process to market, since they need to generate clinical information, especially compared to tech companies' disruptive product cycle.

There is no specific regulation related to government-funded inventions in Mexico. The rules regarding issues of ownership or licensing of government-funded inventions may vary depending on the specific programme, so terms and conditions should be reviewed on a case-by-case basis. For general patent protection issues, the general rules under the FLPIP would be applicable.

Regulatory schemes of healthcare products with medical purposes require specific authorisations and not following the healthcare regulations can bring forth fines, as well as the application of safety measures such as temporary closure of the establishment.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

For the reasons mentioned in question 10.2, the commitment to invest of venture capital and private equity firms may require a longer period to generate return on investment.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

From a regulatory perspective, key barriers holding back widespread clinical adoption of digital health solutions in Mexico are the absence of updated and clear regulations, leading to the application of traditional rules to digital health solutions that do not respond to emerging business models. Also, a regulatory backlog from the healthcare regulator, COFEPRIS, is another barrier across healthcare products. At the same time, there is a risk of over-regulating digital health. Some of the law initiatives being discussed right now at the Federal Congress are proposing to create new authorisations for the digital version of certain activities, whereas the risks involved between the digital and physical versions of the activities may be the same. This may create market barriers or create unintended monopolies.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

Healthcare providers (physicians) must be licensed by a Medical School jointly with Mexico's Ministry of Education. Currently, there are no specific certification bodies for digital health applications in Mexico.

The National Centre for Health Technology Excellence has been proposed in draft law initiatives as a certifying body for digital healthcare providers, but it is not within its current scope.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

The provision of public healthcare services in Mexico are not provided through a reimbursement scheme. Rather, there is a system of public procurement of goods and services.

Only around 10% or so of the Mexican population has access to private medical insurance where a reimbursement scheme would apply in combination with a direct pay scheme. There is no straight answer for whether patients who use digital health solutions are reimbursed, since this depends on each insurer's policies and level of insurance protection. Noteworthy, most insurers will not cover medical experimental treatments in clinical phases. For instance, some specific insurance policies consider robotic surgery as experimental treatment and thus it would not be covered, unless it is for brain surgery.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

The main gap in the healthcare ecosystem for analysing digital health solutions is that current provisions for the regulation of digital health are generally fragmented and there is no comprehensive or dedicated legal framework for these applications.

For data-driven products, including AI/ML solutions, the same challenges would apply.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

The latest development regarding the regulation of SaMD was the publication on December 2023 of the Application Guide for Medical Devices Market Authorization issued by COFEPRIS. This Guide contains a detailed section on Market Authorisation applications for MDs, as well as detailed instructions regarding digital health applications (i) that contain a sensor or transductor to measure physiological parameters, and (ii) for digital health apps installed in a smartwatch. This is consistent with the trend of regulation of digital health applications with a bottom-top approach,

which hastens the regulation process as it is done at an administrative, rather than at a parliamentary level.

There have been several draft law initiatives submitted in the Federal Congress in the last three years, which focus on different aspects of digital health, mainly telemedicine and health applications of AI. The themes included have been telemedicine, electronic health records, e-prescription, medical apps, AI and neurorights. The last draft initiative on the regulation of health applications of AI dated December 15, 2023, obtained a favourable vote from the Chambers of Commons. However, 2025 is the first year of the administration of Mexico's new President, and at the time of writing, the focus is on consolidating the approval of a whole set of Constitutional amendments and issue the secondary regulations required for their implementation; therefore, it is unlikely any key regulations regarding digital health will pass in 2025.

Carla Calderón is Head of the Healthcare & Life Sciences Practice of Baker Mckenzie Mexico, a leading global law firm. She specialises in the life sciences and healthcare industries, helping clients navigate the complex and evolving legal framework that governs market access, commercial transactions, transfer and modification of marketing authorisations, digital health, consumer protection, advertising, medical incentives, patient support programmes, clinical trials, due diligence, compliance, litigation and contracts. She leverages her extensive experience in administrative law, commercial law and her knowledge of international private law and environmental, social and governance issues to deliver innovative and effective solutions that balance business objectives and social responsibility.

Baker McKenzie
Edificio Virreyes, Pedregal 24, 12th Floor
Lomas Virreyes/Col. Molino del Rey
Mexico City, 11040
Mexico

Tel: +52 55 5351 4105
Email: carla.calderon@bakermckenzie.com
LinkedIn: www.linkedin.com/in/carla-calderon

Marina Hurtado Cruz leads Baker McKenzie's Patent Practice in Mexico. With more than a decade of experience handling sophisticated IP matters, she advises on a broad range of areas, including prosecution, licensing and litigation of patents, utility models, industrial designs and trademarks. In addition to this, Marina has extensive experience in the areas of Health, Advertising and Consumer laws. In October 2019, Marina was appointed by the Secretary of the Mexican Ministry of Foreign Affairs, as *ad honorem* external advisor on IP issues to collaborate in the development of IP public policies in Mexico.

Baker McKenzie
Edificio Virreyes, Pedregal 24, 12th Floor
Lomas Virreyes/Col. Molino del Rey
Mexico City, 11040
Mexico

Tel: +52 55 5279 2900
Email: marina.hurtado@bakermckenzie.com
LinkedIn: www.linkedin.com/in/marina-hurtado-544863104

Daniel Villanueva collaborates with clients across various industries, focusing on the intersection of intellectual property and technology. He assists technology companies in cross-border transactions, drafting and negotiating commercial agreements, including software and technology licences. Daniel's expertise extends to advising software developers, AI developers, hardware manufacturers, video game creators, social networks, e-commerce platforms and internet companies globally.
His advisory services cover a wide range of areas, including regulatory restrictions, intellectual property, data privacy and security. Daniel provides guidance on global data privacy, data protection, cybersecurity, digital media, and other legal and regulatory issues.

Baker McKenzie
Av. Paseo Royal Country 4596, Torre Cube 2, 16th Floor
Fracc. Puerta de Hierro, Zapopan, Jalisco 45116
Mexico

Tel: +52 33 3848 5387
Email: daniel.villanueva-plasencia@bakermckenzie.com
LinkedIn: www.linkedin.com/in/daniel-villanueva-plasencia-655bbab

Carlos Vela Treviño is the Lead Partner of the Telecommunications, Media and Information Technology Practice at Baker McKenzie. Carlos's practice operates at the intersection of the digital economy, regulation, information technology and human rights. Carlos advises highly disruptive companies in all sectors of the digital economy on a daily basis; his practice involves regulatory and contractual aspects of communications, digital media, copyright, software and cloud transactions, technology disputes, relations with regulators, privacy and cybersecurity.

Baker McKenzie
Edificio Virreyes, Pedregal 24, 12th Floor
Lomas Virreyes/Col. Molino del Rey
Mexico City, 11040
Mexico

Tel: +52 55 5279 2911
Email: carlos.vela-trevino@bakermckenzie.com
LinkedIn: www.linkedin.com/in/carlos-vela-trevi%C3%B1o-96290b2

Baker McKenzie is a top-tier full-service firm with a front-running position in the life sciences market in Mexico and the United Kingdom. The healthcare and life sciences industry group are active on matters throughout the whole life cycle of products, from research and development to manufacturing and commercialisation. The team is noted for advising clients on regulatory matters, particularly medical devices, digital health and pharmaceuticals. The team is also actively involved in legal and trade associations that have life sciences focus or working groups. The strong regulatory practices of health law, information technologies and intellectual property provide the solid bases for an experienced and highly recognised practice on digital health.

Additionally, as a full-service law firm, we have integrated advice in the fields of consumer law, transactional, M&A, foreign trade, antitrust, compliance, employment, tax and litigation.

www.bakermckenzie.com

Poland


Michał Czarnuch


Dr. Paweł Kaźmierczyk


Julia Nowosielska-Łaskawiec

Rymarz Zdort Maruta

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

In Poland, there is no specific legal definition for "digital health". However, Polish law acknowledges the provision of healthcare services through information and communication technologies. The Act on Medical Activity allows for medical services to be conducted via IT and communication systems, encompassing activities such as healthcare provision.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

1) Telemedicine – the adoption of telemedicine has surged, especially following the COVID-19 pandemic.
2) Artificial Intelligence (AI) in healthcare – AI applications are becoming increasingly prevalent in Polish healthcare.
3) Digital treatment and care – digital tools for treatment and care management are gaining traction.
4) Health data digitisation – efforts to digitise health data are underway, with initiatives like the establishment of Regional Centres for Digital Medicine.

1.3 What is the digital health market size for your jurisdiction?

Revenue in the digital health market is projected to reach US$2.779 billion in 2025.[1]

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

Identifying the top digital health companies in Poland by revenue can be challenging due to the dynamic nature of the industry and the limited availability of specific financial data. However, based on available information, here are some notable companies in Poland's digital health sector:

1) Asseco Poland S.A. – Asseco Poland is one of the largest IT companies in Poland, with significant involvement in the healthcare sector. Asseco is recognised as the largest provider of IT solutions and services for the healthcare sector in Poland.
2) DocPlanner – DocPlanner is an online medical appointment booking platform that connects patients with healthcare professionals. Operating in multiple countries, it has a significant presence in Poland and has been expanding its services globally.
3) Infermedica – Infermedica specialises in AI-driven pre-diagnosis and triage solutions, assisting healthcare providers in patient assessment and care recommendations. The company has been growing its client base internationally and continues to innovate in the digital health space.
4) MedApp S.A. – MedApp is a Polish company that develops innovative medical technologies, including CarnaLife, a telemedicine platform that enables remote monitoring of patients' health parameters. The company has been expanding its offerings and presence in the digital health market.
5) Synerise – Synerise is a Polish technology company specialising in AI and big data solutions. While not exclusively focused on healthcare, its AI-driven platforms have applications in the health sector. As of 2023, Synerise has been recognised as one of the fastest-growing companies in Poland.

Please note that the digital health sector is rapidly evolving, and company standings can change quickly. For the most current information, it is advisable to consult recent industry reports or financial disclosures.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Identifying the top five fastest-growing digital health companies in Poland by revenue is challenging due to the dynamic nature of the industry and limited publicly available financial data. However, based on available information, here are some notable companies experiencing significant growth:

1) eGabinet – founded in 2020, eGabinet offers a cloud-based platform that enables medical facilities to manage patient appointments and documentation efficiently. The company has seen significant growth, doubling its customer base in the past year and raising €548,000 in a recent funding round to expand its platform's functionality.
2) DocPlanner – DocPlanner is an online medical appointment booking platform that connects patients with healthcare professionals. Operating in multiple countries, it has a significant presence in Poland and has been expanding its services globally.
3) Infermedica – Infermedica specialises in AI-driven pre-diagnosis and triage solutions, assisting healthcare

providers in patient assessment and care recommendations. The company has been growing its client base internationally and continues to innovate in the digital health space.

4) Applover – Applover, a Wrocław-based full-stack digital agency specialising in IT solutions for healthcare, has demonstrated remarkable growth. In 2022, the company generated zł25 million in sales revenue and was recognised in the 'FT 1000: Europe's Fastest Growing Companies' list, ranking 13th among Polish companies.
5) Synerise – Synerise, a Polish technology company specialising in AI and big data solutions, has been recognised as one of the fastest-growing companies in Poland. As of 2023, the company has achieved a valuation of approximately US$85 million.

Please note that the digital health sector is rapidly evolving, and company standings can change quickly. For the most current information, it is advisable to consult recent industry reports or financial disclosures.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

1) Ministry of Health (*Ministerstwo Zdrowia*) – the Ministry of Health is the primary governmental body responsible for public health policy, including the integration and regulation of digital health solutions within the healthcare system. It oversees the implementation of e-health initiatives, such as electronic medical records (EDM) and telemedicine services.
2) Centre for e-Health (*Centrum e-Zdrowia* – CeZ) – CeZ is a key governmental institution responsible for implementing digital health solutions in Poland. It manages national e-health systems, including the Internet Patient Account (IKP), e-prescriptions, e-referrals and EDM. CeZ also supports the digital transformation of the healthcare sector and ensures compliance with national and EU regulations on digital health.
3) Agency for Health Technology Assessment and Tariff System (*Agencja Oceny Technologii Medycznych i Taryfikacji* – AOTMiT) – AOTMiT conducts health technology assessments to inform decisions on the financing of healthcare services, including digital health technologies. Its evaluations ensure that new technologies are both effective and cost-efficient before being adopted into the healthcare system.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

1) Medical devices and Software as a Medical Device (SaMD) – the Office for Registration of Medicinal Products, Medical Devices, and Biocidal Products (URPL) is responsible for the registration, supervision and control of medical devices in Poland. This includes evaluating and authorising medical devices and SaMD before they can be marketed. Manufacturers must submit a marketing authorisation application, a product identity declaration and documentation confirming the company's legal status.
2) Data privacy and compliance – the Office for Personal Data Protection (UODO) enforces data protection regulations, ensuring that personal health data is processed in compliance with the General Data Protection Regulation (GDPR). This includes overseeing the implementation of codes of conduct for data processing in the healthcare sector.
3) AI in healthcare – while Poland does not yet have specific laws relating to AI, big data or machine learning (ML), the Polish authorities have expressed the need to have state regulations governing this topic and define their goals in terms of both the implementation of EU regulations and the preparation of their own legislative projects.
4) Health technology assessment and reimbursement – the AOTMiT conducts health technology assessments to inform decisions on the financing of healthcare services, including digital health technologies. Its evaluations ensure that new technologies are both effective and cost-efficient before being adopted into the healthcare system.
5) E-health infrastructure – CeZ is responsible for implementing digital health solutions in Poland. It manages national e-health systems, including the IKP, e-prescriptions, e-referrals and EDM. CeZ also supports the digital transformation of the healthcare sector and ensures compliance with national and EU regulations on digital health.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The key areas of enforcement are as follows:

a) Data protection and privacy – digital health solutions must adhere to GDPR, ensuring the secure handling of personal health data. Compliance with the Act of 6 November 2008 on Patients' Rights and on the Patient Ombudsman (*Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta*) is also essential, as it outlines rules for outsourcing and data processing in healthcare settings.
b) Medical device regulation – software classified as a medical device must comply with the EU Medical Device Regulation (MDR) 2017/745. This involves rigorous conformity assessments, proper classification and obtaining CE marking before market entry. The URPL oversees these processes in Poland.
c) Cybersecurity compliance – healthcare entities are subject to the Act on the National Cybersecurity System of 5 July 2018, which mandates the implementation of appropriate security and organisational measures to manage cybersecurity risks and incidents. This indirectly affects digital health software providers, requiring them to ensure their solutions support the cybersecurity obligations of healthcare providers.

The emerging areas of enforcement are as follows:

1) AI integration – as AI becomes more prevalent in digital health solutions, regulatory scrutiny is increasing. Ensuring transparency, accountability and ethical use of AI in healthcare applications is becoming a focal point for regulators. Compliance with forthcoming EU AI regulations will be crucial for developers.
2) Interoperability standards – with the advancement of the European Health Data Space (EHDS), there is a growing

emphasis on the interoperability of digital health solutions. Enforcement efforts are focusing on ensuring that health data can be seamlessly and securely exchanged across systems and borders, adhering to standardised formats and protocols.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

In Poland, the regulation of SaMD aligns with the EU's framework, primarily governed by Regulation (EU) 2017/745, known as the MDR. This regulation, which became fully applicable on 26 May 2021, establishes the requirements for the safety, performance and conformity assessment of medical devices, including software intended for medical purposes.

In addition to the MDR, Poland has enacted the Act of 7 April 2022 on Medical Devices (referred to as the "MD Act"), which supplements EU regulations by addressing specific national requirements. The final provisions of this Act came into effect on 1 July 2023, introducing additional obligations for manufacturers, importers and distributors operating within Poland.

At the national level, the URPL is the competent authority overseeing medical devices in Poland. The URPL's responsibilities encompass approving medical devices for market placement, supervising clinical trials, monitoring safety and ensuring compliance with both EU regulations and national laws.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

In Poland, the regulation of AI- and ML-powered digital health devices and software solutions is primarily governed by EU legislation, complemented by national frameworks.

1) MDR – AI/ML-powered digital health solutions that qualify as medical devices fall under the MDR. This regulation establishes comprehensive requirements for the safety, performance and conformity assessment of medical devices within the EU. Manufacturers must conduct a conformity assessment, which may involve a Notified Body depending on the device's risk classification, to obtain CE marking before marketing the device in Poland. The MDR is enforced in Poland by the URPL.
2) Artificial Intelligence Act (AI Act) – the proposed AI Act is set to be the EU's first comprehensive legal framework specifically addressing AI. It adopts a risk-based approach, categorising AI applications into different risk levels and imposing corresponding obligations. High-risk AI systems, which include certain medical devices, will be subject to stringent requirements concerning data quality, transparency, human oversight and accountability. Once enacted, the AI Act will work in conjunction with the MDR to regulate AI/ML-powered medical devices.
3) Data protection regulations – compliance with data protection laws is crucial for AI/ML-powered digital health solutions, especially given the sensitive nature of health data. GDPR applies across the EU, including Poland, setting strict standards for data processing, patient consent and data security. In Poland, the UODO oversees the enforcement of GDPR provisions.
4) National regulations – at the national level, Poland has enacted the MD Act, which supplements EU regulations by addressing specific national requirements. This Act introduces additional obligations for manufacturers, importers and distributors operating within Poland, including those related to AI/ML-powered medical devices.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Regulatory authorities in Poland, in line with broader EU initiatives, are in the process of planning and developing changes to better handle the dynamic nature of AI/ML-based digital health solutions. These changes are still in the planning phase and are expected to evolve as new technologies emerge.

Key initiatives that will shape the regulatory landscape include Poland's Digital Strategy (*Strategia Cyfryzacji Polski do 2035 roku*).[2] The strategy aims to support the adoption of emerging technologies, including AI and ML, in the healthcare sector. This strategy also emphasises the need for a flexible regulatory framework that will accommodate the dynamic nature of AI-powered solutions, while ensuring the safety, security and effectiveness of healthcare applications. Regulatory changes are expected as the strategy develops, with a focus on integrating AI/ML technologies into healthcare systems and ensuring that they meet both national and EU standards.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

In Poland, there is an ongoing discussion regarding the role of clinical validation data for AI/ML-based digital health solutions. Currently, there are no concrete regulatory solutions in this area, but the topic is gaining significance as digital technologies in healthcare continue to develop.

One of the important steps toward regulating clinical validation was the attempt to create the Health Applications Portfolio (*Portfel Aplikacji Zdrowotnych*), which aimed to define the principles for assessing and approving digital health solutions. However, despite this ongoing project, it does not yet provide clear solutions regarding clinical validation in the context of AI/ML.[3]

According to the Poland Digital Strategy 2035, more detailed solutions regarding clinical validation in the context of AI/ML are planned for the coming years. These solutions aim to ensure the safe and effective introduction of new technologies into Poland's healthcare system. These discussions also include integrating European regulations, such as the AI Act, which will influence the legal framework for AI/ML in healthcare.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Poland, as an EU Member State, is also subject to EU-level regulations that govern digital health products and services, particularly for those with cross-border implications. For example, the MDR, *In-vitro* Diagnostic Regulation, AI Act and GDPR are all consistent with EU regulations, and Poland adheres to these rules.

What distinguishes Poland is the different process for reimbursement of solutions by the public payer, the National Health Fund (NFZ). The reimbursement process in Poland may vary from other EU countries, as the NFZ has its own specific procedures for evaluating and reimbursing digital health solutions and medical devices. This process involves assessing the effectiveness and cost-efficiency of the solution, in addition to its regulatory compliance, to determine whether it will be covered by public healthcare funding.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

The e-health regulatory package is expected to be adopted in Q1 2026 as part of Poland's ongoing digital health transformation efforts. However, the specific details of the package are not yet known, as discussions and preparations are still underway. This package is anticipated to address various aspects of digital health, including standardisation, interoperability and the regulation of health applications and telemedicine services.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  a) Telemedicine is legally permissible. It is crucial to maintain the general requirements related to due diligence in the provision of health services and the protection of privacy.
  b) Reimbursement by the NFZ – telemedicine services can be reimbursed by the NFZ under specific conditions, with varying reimbursement policies for different telehealth services.
  c) Key limitations concern the ability to issue prescriptions for certain medications (e.g. narcotics) during teleconsultations.
- **Robotics**
  a) Robots used in healthcare (e.g., for surgery or rehabilitation) must comply with the EU MDR.
  b) Liability issues – questions of liability in the event of malfunctions or errors involving medical robots are addressed under product liability laws and healthcare professional liability.
- **Wearables**
  a) Wearables that collect health data must comply with GDPR, ensuring that personal health information is handled securely.
  b) If the wearable device is used for medical purposes (e.g., monitoring vital signs), it may fall under the EU MDR, requiring appropriate certification and compliance.
- **Virtual Assistants (e.g. Alexa)**
  a) Virtual assistants processing personal health data must comply with GDPR to ensure data protection and secure storage of sensitive health information.
  b) If the virtual assistant is intended for medical purposes (e.g., patient monitoring or diagnosis), it may fall under the MDR and must be appropriately classified as a medical device.
- **Mobile Apps**
  a) Mobile apps that provide diagnostic, therapeutic or clinical monitoring services may be classified as medical devices under the MDR and must comply with relevant medical device regulations.
  b) Apps handling personal health data must comply with GDPR to ensure secure processing, storage and sharing of user data.
- **Software as a Medical Device**
  a) Software that is intended to be used for medical purposes must comply with the MDR, requiring CE marking and clinical evidence to demonstrate safety and efficacy.
  b) SaMD must meet high standards of cybersecurity to ensure the protection of patient data and the integrity of the software.
- **Clinical Decision Support Software**
  a) If the software assists in clinical decision-making, it may be classified as a medical device under the MDR, requiring regulatory approval and clinical validation.
  b) Clinical decision support software that handles patient data must comply with GDPR, ensuring secure processing and storage of sensitive health information.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  a) AI-based solutions are subject to the EU AI Act, which will create guidelines for the development, deployment and monitoring of AI in healthcare.
  b) AI-driven medical devices must comply with the MDR, requiring clinical validation and continuous monitoring to ensure safety.
  c) AI solutions processing personal health data must adhere to GDPR, ensuring data privacy and security.
- **IoT (Internet of Things) and Connected Devices**
  a) IoT devices used in healthcare must comply with GDPR and relevant cybersecurity regulations to protect patient data and prevent unauthorised access.
  b) Connected medical devices must meet the MDR and ensure safe and effective use, with CE marking and post-market surveillance required.
  c) Devices must comply with national standards for interoperability, ensuring that they can safely communicate with other healthcare systems.
- **3D Printing/Bioprinting**
  a) 3D-printed medical devices or implants may comply with the MDR to ensure that they meet safety and efficacy standards.
  b) Bioprinted tissues or organs are subject to rigorous clinical validation and regulatory approval and may need to be classified as medical devices under the MDR.
- **Digital Therapeutics**
  a) Digital therapeutics may be classified as medical devices under the MDR, requiring clinical evidence of safety and effectiveness before they can be marketed.
  b) If used in the Polish healthcare system, digital therapeutics may be eligible for reimbursement through the NFZ, provided they meet cost-effectiveness and clinical-effectiveness criteria.
- **Digital Diagnostics**
  a) Digital diagnostic tools (e.g., apps or software used for diagnostics) must comply with the MDR, requiring appropriate certification and clinical validation.

b) Digital diagnostics platforms must ensure compliance with GDPR to protect patient health data and ensure privacy.

- **Electronic Medical Record Management Solutions**
  a) Electronic health record (EHR) systems must comply with GDPR, ensuring the secure processing, storage and sharing of patient records.
  b) EHR systems must meet national interoperability standards, ensuring they can integrate with other healthcare systems.
  c) The software must be designed to ensure the integrity and accuracy of medical records, with regulatory oversight ensuring compliance with healthcare data standards.
- **Big Data Analytics**
  a) Big data solutions in healthcare must comply with GDPR, ensuring that patient data is anonymised, secure and processed with consent.
  b) Big data analytics solutions that influence clinical decisions may need to demonstrate their efficacy and safety to comply with medical device regulations.
- **Blockchain-based Healthcare Data Sharing Solutions**
  a) Blockchain-based systems must comply with GDPR, especially regarding the ability to update and delete data, which may be complicated by the immutable nature of blockchain.
  b) Blockchain solutions must meet cybersecurity standards and ensure interoperability with other healthcare systems.
  c) The use of blockchain for healthcare data sharing must comply with regulations governing consent, patient rights and the ethical use of data.
- **Natural Language Processing**
  a) Natural language processing (NLP) solutions must comply with GDPR, ensuring the protection of personal health information when processing patient data.
  b) If used in a clinical context (e.g., for speech-to-text in patient records), NLP solutions may be regulated as medical devices under the MDR.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

a) Digital platform providers in digital health must comply with GDPR, ensuring that personal health data is processed securely and with patient consent.
b) If a platform or software is used for medical purposes (e.g., diagnostics, monitoring or treatment support), it may be classified as a medical device under the EU MDR.
c) Platform providers must be aware of product liability issues, including claims for damages due to faulty software or data inaccuracies that lead to adverse health outcomes. Clear terms of use, disclaimers and indemnity clauses can help manage liability.
d) Digital health platforms that offer services directly to consumers must ensure that the terms and conditions are transparent, clear and in line with Polish consumer protection laws. This includes ensuring that users are aware of their rights and can easily access information about the service.
e) Providers must comply with cybersecurity regulations to ensure the protection of sensitive health data from hacking, unauthorised access or cyberattacks.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Under GDPR, health data is classified as sensitive personal data (also known as special categories of personal data). Processing such data requires meeting specific legal requirements and having a valid legal basis for processing. The key legal bases for processing health data under GDPR include:

a) Healthcare and medical purposes – health data can be processed without explicit consent for healthcare-related activities, such as medical diagnosis, provision of healthcare or management of healthcare systems, as long as it is carried out by health professionals or under their authority.
b) Public health and scientific research – under certain circumstances, health data can be processed for reasons related to public health, scientific research or statistical purposes, provided there are adequate safeguards in place.
c) Explicit consent – the most common legal basis is obtaining explicit consent from the individual whose data is being processed.

GDPR applies to all organisations processing personal data in the EU.

Under the Polish Act on Patient Rights and the Patient Ombudsman, patient data must be treated confidentially, and healthcare providers must ensure that patients' health information is protected. There are strict guidelines regarding the sharing of health data between healthcare providers, ensuring that only authorised individuals have access to sensitive patient information.

The Health Information System Act (*Ustawa o systemie informacji w ochronie zdrowia*) governs the management of health data and systems for EHRs in Poland.

Healthcare data stored or transmitted digitally must also be protected from cyber threats. This includes implementing encryption and secure access controls. The Cybersecurity Act (*Ustawa o Krajowym Systemie Cyberbezpieczeństwa*) governs cybersecurity measures and protocols in Poland.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In Poland, personal health data use is particularly regulated by two key pieces of legislation: the Act on Patient Rights and the Patient Ombudsman; and the Health Information System Act. These laws provide specific frameworks for the management, protection and use of personal health data within the healthcare system.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

In Poland, the legal and regulatory considerations for the use of personal health data vary significantly depending on the nature of the entities involved (e.g., healthcare providers

vs. non-healthcare entities) and the nature of the data (e.g., personal health data *vs.* anonymous data). These differences affect how data is processed, stored and shared, as well as the level of protection required under the law.

4.4 How do the regulations define the scope of personal health data use?

In Poland, the use of personal health data is primarily governed by GDPR at the European level, along with local legislation-related healthcare regulations. The use of health data may be generally divided into three main areas:

a) Patient treatment – health data is used primarily within the framework of medical law for purposes such as diagnosis, treatment and ensuring proper healthcare. This includes the provision of medical services and the management of healthcare systems.
b) Scientific and research activities – health data is used in scientific research and clinical studies, including clinical trials. In this context, data may be processed for purposes such as medical advancements, drug development and other research-related activities.
c) Other applications – for uses outside of direct healthcare and research, the processing of health data typically requires the explicit consent of the patient, unless the data is anonymised. This category includes uses for marketing or other non-medical purposes, where the consent of the individual is a key requirement unless the data is no longer personally identifiable.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

In Poland, when dealing with personal health data use and data collection, particularly in healthcare or research contexts, there are several key contractual terms that need to be carefully considered to ensure compliance with the relevant laws and regulations, such as GDPR and Polish health data protection laws. These terms help protect both the data subjects' rights and the entities processing the data:

a) purpose and scope of data use;
b) data subject consent;
c) data retention period;
d) data security and confidentiality;
e) data subject rights;
f) sub-processors and third parties;
g) legal and regulatory compliance; and
h) data transfer and cross-border transfers.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

In Poland, the issue of accuracy of health data is addressed through guarantees of diligence on the part of medical personnel who are responsible for entering and updating patient data. Medical professionals are required to ensure the accuracy and completeness of the data they record, and they must act with the appropriate professional care when handling health information. If inaccuracies are found, they must be corrected to ensure high-quality care and compliance with medical standards.

Regarding bias and discrimination, there are no specific regulations directly targeting these issues in the context of health data. However, general principles of professional diligence and anti-discrimination laws apply. The principle of professional care mandates that healthcare providers must not let bias affect their treatment or data handling practices. Additionally, anti-discrimination provisions in Polish law prohibit discrimination based on health status in areas like employment and access to services. These broader legal frameworks help mitigate any potential issues of discrimination or bias in healthcare and data use.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

In Poland, the standards for using and collecting personal health data are governed by both EU regulations and Polish national medical law.

GDPR is the central piece of legislation for personal data protection across the EU, including Poland. It establishes general principles for processing personal data, including sensitive health data, which is classified as a special category of personal data.

In addition to GDPR, Poland has specific national medical laws that govern the use and collection of health data, particularly in the context of healthcare provision.

What distinguishes Poland from other jurisdictions is the existence of two codes of conduct approved by the UODO, which provide detailed, practical guidelines for the processing of health data in the country.[4] These codes of conduct help organisations better understand the expectations around personal health data processing, ensuring compliance with both GDPR and Polish-specific legal requirements. The approval of these codes by the UODO serves to standardise practices and reduce legal uncertainties for entities processing health data in Poland.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

In Poland, the sharing of personal health data is subject to a combination of data protection laws and medical regulations. Below are the key legal and regulatory issues to consider when sharing personal health data, including those not necessarily specific to healthcare technologies:

a) Basis for data sharing – the most common basis for sharing personal health data is the explicit consent of the patient. Health data can typically only be shared with third parties or entities if the patient provides their consent, except in cases where other legal grounds apply (e.g., medical treatment, public health). The relevant regulations for this are:
   - GDPR (Article 9): under GDPR, processing and sharing health data require explicit consent from the data subject, unless specific exceptions are met, such as for medical treatment or legal obligations.
   - Polish medical law: national medical regulations also support the requirement of explicit consent for data

sharing, particularly outside the context of healthcare treatment or related services.

b) Lack of standard for anonymisation and pseudonymisation – the absence of a standardised approach to anonymisation and pseudonymisation of health data in Poland makes it challenging to enhance data accessibility while ensuring privacy protection. Without standard techniques, data sharing and re-use for research or healthcare purposes may face barriers related to privacy risks. GDPR is the relevant regulation for this issue.

c) Reform of the EHDS – the EHDS reform aims to create a unified framework for access to and sharing of health data across EU Member States, including Poland. The EHDS seeks to enhance interoperability and secure data sharing for better healthcare services, research and policy-making while ensuring strong privacy protections.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Key to the regulation of health data sharing in Poland are the provisions of national medical law, which outline the rules for disclosing patient data, including the requirements for patient consent and exceptions to this rule.

Article 26 of the Act on Patient Rights and the Patient Ombudsman is a key provision in Poland governing the sharing of personal health data. It sets out the rules for disclosure of health information and specifies the circumstances under which healthcare providers are allowed to share or disclose patient data.

Article 35 of the Health Information System Act regulates the use and management of health data in Poland, with a particular focus on EHRs and the interoperability of healthcare information systems. This law is crucial in establishing the framework for digital health data management and the sharing of personal health data within Poland's healthcare system.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

When health data is shared between healthcare providers (e.g., doctors, hospitals, clinics), the primary consideration is typically to ensure continuity of care and facilitate medical treatment. Healthcare providers must also adhere to strict confidentiality and data protection requirements under both GDPR and national medical law.

When non-medical entities are involved, such as technology companies, insurance companies or research organisations, the regulations become stricter. These entities typically need to obtain explicit patient consent before accessing or processing personal health data.

Public health authorities, such as the Ministry of Health, and other governmental entities may have broader access to personal health data, often related to public health purposes (e.g., disease monitoring, vaccination programmes). They are allowed to access data without patient consent in cases where public health needs justify the data sharing.

Data that is anonymised or pseudonymised is subject to less stringent regulations, making it easier to share.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

In Poland, the standards for sharing health data are governed by both EU regulations and Polish national medical law.

Please see the response to question 4.7.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Platform P1 is a central element of the Medical Information System (SIM), aimed at integrating medical data in Poland and enabling its secure sharing across healthcare institutions. The platform enables healthcare providers to access and share patient data, ensuring interoperability between different healthcare systems, while maintaining strict data protection standards.

In Poland, data on medical events (healthcare services provided to patients, such as treatments, procedures or consultations) are transmitted by healthcare facilities (at the local level) to a central system as part of the SIM. This system is designed to aggregate and manage healthcare data, improving the overall efficiency and coordination of healthcare services while ensuring that relevant information is available to authorised professionals across different institutions. The transmission of medical event data is governed by the Health Information System Act.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Polish patent regulations set out specific criteria for patent protection (the inventions must meet the criteria of novelty, inventive step and industrial applicability) and exclusions from patent protection (for example, computer programs are not regarded as patentable inventions). In addition, the legislation regulates the specific steps required in the notification procedure.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Polish copyright law regulates the protection of copyrights, including those related to computer software in digital health technologies. Developers of digital health technologies may license and transfer copyright in such software under the terms of these laws. There are no dedicated copyright regulations specifically for medical law, but general intellectual property (IP) rules apply.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Polish trade secret laws establish a broad catalogue of obligations and rules for trade secret protection, including on the grounds of combatting unfair competition. The Act on Combatting Unfair Competition defines trade secrets broadly

and offers legal remedies against unauthorised disclosure or misappropriation. Infringement of a trade secret can raise legal measures and remedies such as injunctions, damages or the cessation of unfair competitive practices. There are no dedicated regulations specifically for medical law, but general rules apply.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

In accordance with the Act of 30 April 2010 on the National Centre for Research and Development (NCBR), as a rule, the copyright belongs to the entity to which the support funds have been granted. However, in the case of work carried out for the defence and security of the state and financed by the NCBR, the State Treasury is the owner of the results (see question 6.7 below).

In accordance with the Act of 20 July 2018 – Law on Higher Education and Science and Act of 30 April 2010 on the Polish Academy of Sciences (i.e., Journal of Laws of 2020, item 1796, as amended), higher education institutions and the National Academy of Sciences shall adopt rules and regulations for the management of copyright, setting out the rights and obligations of the institution, employees, doctoral students and students, as well as rules and procedures for commercialisation.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Polish IP laws do not contain specific regulations on the protection of SaMD, so the general rules apply accordingly.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

No, in the Polish legal system, the right to obtain a patent is vested in the creator (in the sense of an individual) or other persons holding rights to the invention, including legal persons. AI does not have the above-mentioned subjective qualities. No specific changes in this regard have been adopted yet.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

In Poland, IP rights for government-funded inventions are primarily governed by the Industrial Property Law and regulations related to public research funding. The key principles include:

1) Ownership by research institutions – if an invention is created within a government-funded project (e.g., through the NCBR), the rights typically belong to the institution conducting the research, not the government directly.
2) Government usage rights – public funding agreements may grant the government certain rights, such as a non-exclusive, royalty-free licence to use the invention for public purposes, particularly in sectors like healthcare or national security.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

At the time of writing, there are no precedential legal cases or decisions affecting IP rights protection of digital health innovation in Poland.

It is worth recalling the judgment of the Supreme Administrative Court (NSA) of 11 September 2020 (*II GSK* 923/18) – the court ruled that a lecture presenting previously collected clinical data does not have a creative character but rather a reproductive nature. This decision impacts copyright protection in digital health by limiting the scope of protection for scientific presentations based on pre-existing data.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

It is crucial for parties to consider several contractual and strategic factors, especially: (i) clear definition of roles and responsibilities of each party; (ii) IP rights, including ownership of jointly developed IP and licensing arrangements; (iii) confidentiality; (iv) a dispute resolution mechanism such as mediation or arbitration; (v) performance metrics and milestones to track progress of collaboration; (vi) a governance structure, especially in the scope of the decision-making process; and (vii) personal data management and processing.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

In addition to the elements indicated in question 7.1, it is important to consider: (i) rules and deadlines for payment, taking into account the status of the trader in light of the provisions on combatting excessive delays in payment transactions; (ii) data-sharing principles, with particular regard to the security of medical data; (iii) ethical and professional obligations of healthcare professionals employed by healthcare companies; and (iv) the scope of the consents required for the conclusion of contracts (in particular where the contract is concluded with hospitals that are public entities).

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

In addition to the elements outlined in question 7.1, it is crucial to manage the security of the personal and medical data exchanged, including: (i) the data access rules; (ii) the technological solutions used to acquire and store the data; (iii) the extent of potential data processing; (iv) managing the risk of loss or unauthorised access to the data; (v) the scope of the entities authorised to access the data; and (vi) the need for potential consents or licences to obtain and exchange data.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

When deploying generative AI in digital health solutions in Poland, parties should first establish clear ownership and licensing terms for the AI model and its outputs, addressing issues such as IP rights, data rights, and whether any third-party content or training data is involved. Second, contractual agreements must clearly define liability and risk allocation related to the accuracy, reliability and safety of the AI's recommendations, including compliance with applicable data protection regulations (such as GDPR) and healthcare standards. Finally, strategic considerations should include planning for ongoing model updates, ensuring transparency and auditability of AI processes, and addressing ethical concerns related to data privacy and informed consent, all of which are crucial for both regulatory compliance and public trust in digital health innovations.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

Currently, there are no dedicated regulatory authorities specifically focused on the oversight and enforcement of AI/ML technologies in Poland. Instead, various existing regulatory bodies oversee related areas such as data protection, consumer protection and cybersecurity, which may also encompass AI technologies, depending on the sector.

However, draft legal provisions related to AI are in development, which may establish more specific frameworks and authorities for regulating AI in the future. These provisions aim to address the unique challenges and risks posed by AI technologies, including issues related to ethics, transparency, safety and accountability. At this stage, AI regulation in Poland is still evolving, with efforts underway to create laws and regulatory structures tailored to the growing role of AI in various industries.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

Poland does not yet have a dedicated AI regulatory framework, but AI/ML systems are currently governed by existing laws and regulations that apply to data protection, consumer rights, cybersecurity and medical devices. Poland is also preparing for the upcoming EU AI Act, which will introduce specific legal requirements for AI/ML across different risk levels.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

The ownership of IP rights for algorithms improved by AI/ML without active human involvement is a complex issue, as existing laws in Poland and the EU do not explicitly address AI-generated innovations. The current copyright, patent and contract laws provide a framework for determining ownership.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

When licensing data for AI/ML, companies must consider a range of legal, commercial and strategic factors, including ownership rights, compliance obligations, liability risks and competitive advantages. These considerations become more complex when dealing with healthcare data, where privacy, security and ethical concerns play a crucial role.

When licensing data for AI/ML development, agreements typically cover ownership and usage rights, scope of use and restrictions, liability and indemnification, data retention and deletion, and compliance with data protection laws. Key strategic considerations include ensuring data accuracy, diversity and bias mitigation, assessing its competitive advantage, determining an appropriate pricing model and evaluating its impact on AI fairness, accountability and transparency.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Currently, Poland does not have specific regulations differentiating standard AI from generative AI. However, upcoming EU regulations, particularly the AI Act, introduce distinctions based on risk levels and functionalities rather than specific AI types.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Generative AI poses unique legal and regulatory challenges due to its ability to generate text, images, audio and code, raising concerns about data privacy, IP, misinformation and accountability. While Poland does not yet have dedicated generative AI regulations, it follows the EU regulatory framework, particularly the upcoming EU AI Act and existing GDPR provisions.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

Poland does not have dedicated laws on AI/ML models trained with improperly obtained data. However, GDPR and EU copyright laws provide strong enforcement mechanisms, including potential data disgorgement (forced deletion) when AI developers lack appropriate data rights. The upcoming EU AI Act will further regulate AI training datasets.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Product liability – manufacturers and developers of digital health solutions can be found liable on general rules for product defects or if any harm is caused (including software errors, hardware malfunctions or even inadequate instructions or labelling).

Medical negligence – healthcare providers using digital health solutions in day-to-day work can also be liable for failing to implement standards of care or for medical errors causing potential threat to a patient's health and life. This liability is based on the principle of fault and may relate to errors in diagnosis, treatment or the improper use of digital solutions themselves.

Professional liability – misuse of digital health solutions can also result in professional liability for those who introduce or use them.

Data protection violations – non-compliance with data protection laws, such as GDPR, can result in liability if healthcare data is mishandled or breached. This includes inadequate data security measures and unauthorised data sharing.

9.2 What cross-border considerations are there?

When digital health solutions cross national borders, cross-border considerations become critical. Providers must navigate differing regulatory frameworks, including variations in product liability, professional negligence and data protection laws (e.g., GDPR in the EU), and must clearly define the applicable law and jurisdiction in contractual agreements. Moreover, ensuring interoperability with local healthcare standards and meeting the legal requirements in multiple jurisdictions can complicate risk allocation and enforcement of liability, requiring careful strategic planning and local legal counsel.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

1) Compliance with regulations – ensure strict adherence to relevant regulations and regular review of them. It is also worth paying attention to emerging positions and practice guides developed by EU and national authorities.
2) Data management – implement data management practices, including data anonymisation, encryption and secure storage.
3) Transparency – preparing one-pagers or FAQs about used AI/ML algorithms can help healthcare providers, patients and authorities understand how they work and that the compliance standards are ensured. In addition, it is worth providing comprehensive training for healthcare providers that can show the proper and safe use of AI/ML technologies and will clarify the role of healthcare providers in the use of AI/ML.
4) Regular audits and monitoring – conducting regular audits and continuous monitoring of AI/ML systems on the basis of control plans/standard operating procedures can help identify and address potential issues early. On this basis, it is worth creating contingency plans for potential AI/ML failures or adverse outcomes that can help assess and mitigate potential risks.
5) Clear contractual agreements – establish clear contractual agreements that define the responsibilities and liabilities of each party involved in the development and deployment of AI/ML solutions.
6) Consents – preparation of consent forms for the use of the digital health solution in the course of diagnosis or treatment may prove to be an additional safeguard in the event of data breaches.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

When healthcare data is misused in trained AI/ML models within digital health solutions, several liability theories may apply:

1) GDPR violations – GDPR imposes strict standards for data processing, patient consent and data security. Misuse or unauthorised processing of healthcare data can result in significant fines, administrative sanctions and even criminal penalties under national laws implementing GDPR provisions in Poland.
2) Civil liability – beyond GDPR sanctions, parties may face civil liability claims for damages resulting from data misuse. Such claims could include compensation for violations of personal rights, such as breaches of privacy and data protection, which are recognised under Polish law.
3) Violation of patients' rights and medical law – misuse of healthcare data may also constitute a violation of patients' rights, leading to liability under medical law. This could involve claims related to negligence or malpractice if the data misuse adversely affects patient care or leads to erroneous clinical decisions. Healthcare providers and digital health solution developers might, therefore, be subject to legal action for failing to uphold the standards of care and patient confidentiality mandated by medical regulations.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based services in digital health must comply with GDPR, which classifies health data as sensitive personal data (Article 9), requiring strict security measures such as encryption and access controls. Importantly, under the Act on Patient Rights and Patient Ombudsman, any contract for medical data processing must be structured in such a way that it does not disrupt or impede the provision of healthcare services.

Data localisation and cross-border transfers pose challenges – the transfer of health data outside the EU is forbidden unless adequate safeguards are in place.

Security risks are also a major concern, with the NIS2 Directive mandating stricter cybersecurity standards for healthcare IT, including cloud providers.

Additionally, liability remains with healthcare providers, even when outsourcing to cloud vendors, making contractual compliance essential.

Another key issue is interoperability, as fragmented healthcare systems struggle with standardised data exchange. The

upcoming EHDS aims to address this by creating common data-sharing frameworks across the EU.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Entering the digital healthcare market presents non-healthcare companies with significant challenges, primarily related to regulatory compliance, particularly with GDPR and medical device regulations. Companies must ensure they meet strict privacy requirements, especially when handling sensitive health data, and be prepared for the complexities of data integration and interoperability with existing healthcare systems. Liability and risk management are also critical, as healthcare technologies must comply with strict quality and safety standards. Ethical concerns, such as addressing bias in AI and ensuring transparency in decision-making, must be prioritised. Additionally, companies must invest in cybersecurity to protect sensitive patient information, comply with NIS2 cybersecurity regulations, and build trust with both healthcare providers and patients. Finally, partnerships with healthcare organisations and understanding the competitive landscape are key to successful market entry.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Venture capital and private equity firms looking to invest in digital healthcare ventures must carefully evaluate regulatory compliance, especially with GDPR and medical device laws, as these can significantly impact the scalability and operational costs of the venture.

They should also consider the complexity of data integration and interoperability within existing healthcare systems, as well as cybersecurity risks given the sensitivity of health data.

Additionally, firms need to assess the market potential and competitive landscape, ensuring the product has unique value or differentiation.

Another key challenge is the difficulty of obtaining funding from public sources, such as the NFZ, which can be restrictive and competitive, further emphasising the need for strong private backing and strategic partnerships.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

The key barrier holding back widespread clinical adoption of digital health solutions in Poland is regulatory complexity and compliance with both EU and national health regulations, such as GDPR and medical device laws. These regulations create hurdles for developers, especially around data privacy, security and ensuring interoperability with existing healthcare systems.

Additionally, fragmented healthcare infrastructure and a lack of standardised data-sharing protocols make it difficult to integrate digital health tools across different clinical environments.

There is also resistance to change within healthcare institutions, with many providers reluctant to adopt new technologies without clear, demonstrated benefits in patient outcomes and workflow efficiency.

Finally, the limited access to public funding for innovation, especially from institutions like the NFZ, slows down the pace of adoption.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

AOTMiT plays a significant role in the clinical adoption of digital health solutions in Poland. AOTMiT evaluates the clinical efficacy and cost-effectiveness of medical technologies, including digital health tools, and provides recommendations on their inclusion in public healthcare systems. This can influence the adoption of digital health solutions by healthcare providers, particularly in terms of reimbursement policies and accessibility.

The URPL plays a crucial role by ensuring that digital health solutions, particularly those that qualify as medical devices, meet safety and efficacy standards before they enter the market.

Additionally, various scientific societies – such as the Polish Society of Radiology, the Polish Cardiac Society, and other specialty associations – issue clinical guidelines that help shape best practices and support clinician certification, further driving the integration of digital health innovations into routine care.

The Polish Chamber of Physicians and Dentists (*Naczelna Izba Lekarska*) is responsible for overseeing medical practice in Poland and ensures that healthcare professionals adhere to the highest standards of practice. It plays a role in ensuring that clinicians are qualified to use new digital health technologies.

The Ministry of Health, while not a certification body *per se*, establishes the regulatory framework.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

The NFZ provides reimbursement for digital health solutions, particularly for telemedicine services and certain health IT tools that are part of public healthcare programmes. However, reimbursement is usually limited to specific services that meet regulatory and clinical efficacy standards.

To be eligible for reimbursement, digital health solutions must be assessed by AOTMiT for their clinical effectiveness and cost-effectiveness. This involves a formal evaluation process for new technologies that are intended for integration into public healthcare programmes.

Medical device registration is required if the digital health solution qualifies as a medical device under Polish law or EU regulations. In such cases, the product must be CE-marked and undergo a conformity assessment before it can be reimbursed by the NFZ.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Key due diligence gaps in analysing digital health solutions, particularly AI/ML-based products, include inadequate

regulatory compliance with medical device and privacy laws, as well as insufficient clinical validation and evidence of efficacy. Many AI/ML tools lack data quality assurance, transparency and bias mitigation, which can impact their effectiveness and fairness. Additionally, interoperability with existing healthcare systems and cybersecurity risks are often overlooked. Ethical concerns, such as ensuring algorithm fairness and accountability, as well as the long-term viability of business models, also remain significant gaps in due diligence processes.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

The National Reconstruction Plan (KPO) for Poland outlines key milestones related to digital health transformation, focusing on the modernisation of the healthcare sector. These milestones are designed to enhance the accessibility, quality and security of healthcare services through digital solutions. Key milestones include:

a) 60% of medical records digitised by Q1 2026;
b) 30% of medical facilities connected to the central repository of health data by Q1 2026; and
c) 30% of hospitals using AI for medical purposes by Q1 2026.

Endnotes

1 https://www.statista.com/outlook/hmo/digital-health/poland?currency=USD

2 https://www.gov.pl/web/cyfryzacja/strategia-cyfryzacji-polski-do-2035-roku

3 https://www.gov.pl/web/zdrowie/aplikacje-certyfikowane-mz-w-portfelu-aplikacji-zdrowotnych-paz

4 https://uodo.gov.pl/pl/426/1110

Michał Czarnuch is an advocate admitted to practise in Poland, a partner in the corporate department of Rymarz Zdort Maruta and the head of the Life Sciences practice. He is one of Poland's most prominent lawyers practising in the broadly defined area of healthcare law. He specialises in administrative law, in particular pharmaceutical law, laws governing medical devices, medicine and advertising, as well as European and competition law, and compliance in cases involving allegations of corruption. He advises clients from the pharmaceutical and FMCG industries (including with respect to alcohol and tobacco products) on advertising and promotional activities, reimbursement, distribution, labelling and manufacturing, and quality control. He provides advice on the establishment of distribution and marketing systems for medicinal products in matters related to healthcare systems, including the financing of healthcare services, the establishment and restructuring of healthcare providers, telemedicine and health insurance.

He has been involved in a number of legislative processes, including participation in the development of healthcare laws and the creation of opinions and reports on the functioning of these laws. He is one of the originators of the Telemedicine Working Group and a member of the management board of the Telemedicine Working Group Foundation. He advises on projects related to outsourcing and access to medical data in cooperation with the Ministry of Health and the Centre for Health Information Systems (CSIOZ), where he is a member of the Interoperability Council. He also serves as a member of the Advisory Team to the Senate Committee on Health.

Rymarz Zdort Maruta
ul. Prosta 18, 00-850 Warsaw
Poland

Tel: +48 22 520 4428
Email: michal.czarnuch@rzmlaw.com
LinkedIn: www.linkedin.com/in/micha%C5%82-czarnuch

Dr. Paweł Kaźmierczyk is an attorney-at-law, a senior associate in the corporate department of Rymarz Zdort Maruta and a member of the Life Sciences practice. He specialises in medical law, including the principles of conducting medical activities, practising medical professions, patient rights and clinical trials, as well as legal issues related to telemedicine and e-health, AI and innovations in healthcare. He advises, among others: entities performing medical activities; pharmaceutical companies; IT service providers for the healthcare sector; medical startups; as well as local government units and public institutions operating in healthcare. He has extensive and practical experience in the area of providing ongoing advisory services to entities operating in the healthcare market, especially in the field of regulatory aspects related to medical activities, the drafting of contracts and documentation, and the ongoing operation of medical facilities.

Paweł has been involved in projects implemented in cooperation with industry organisations, including: the Telemedicine Working Group foundation (of which he is also a board member); the AI in Health Coalition; and the NIL IN network of physician innovators. He also coordinates substantive work on the code of conduct for the healthcare sector approved by UODO in 2023.

Paweł is a member of the Committee of Experts on Health at the Ombudsman's Office. He is a lecturer at postgraduate studies in medical law and the legal aspects of the use of new technologies in medicine, and is a co-author of commentaries on acts in the field of medical law.

Rymarz Zdort Maruta
ul. Prosta 18, 00-850 Warsaw
Poland

Tel: +48 22 520 4118
Email pawel.kazmierczyk@rzmlaw.com
LinkedIn: www.linkedin.com/in/pawe%C5%82ka%C5%BAmierczyk

Julia Nowosielska-Łaskawiec is a trainee advocate and an associate in the corporate department of Rymarz Zdort Maruta and a member of the Life Sciences practice.

Julia specialises in issues relating to regulated pharmaceutical market activities. She advises entities at each stage of the marketing of medicinal products, medical devices and cosmetics. She has considerable experience in the areas of regulated market transactions and the licensing of open-access pharmacies and pharmaceutical wholesalers. She supports her pharmaceutical sector clients with their day-to-day operations, in particular with regard to distribution, marketing and contracting matters, as well as in connection with administrative proceedings before Polish supervisory authorities.

Rymarz Zdort Maruta
ul. Prosta 18, 00-850 Warsaw
Poland

Tel: +48 22 520 4395
Email: julia.nowosielska-laskawiec@rzmlaw.com
LinkedIn: www.linkedin.com/in/julia-nowosielska-%C5%82askawiec-1627991a7

Singapore


Gloria Goh


Koh En Ying


Tham Hsu Hsien


Alexander Yap

Allen & Gledhill LLP

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

Whilst there is no formal definition of "digital health" under Singapore law, the Health Sciences Authority ("**HSA**") has referred to digital health as "the usage of connected devices, wearables, software including mobile applications and artificial intelligence to address various health needs via information and communications technologies".

1.2 What are the key emerging digital health subsectors in your jurisdiction?

The key emerging digital health subsectors in Singapore are presently in the areas of artificial intelligence ("**AI**"), data analytics/predictive preventative care, and digitised and integrated healthcare systems.

The Ministry of Health ("**MOH**") is responding to increasing pressure on Singapore's healthcare system from Singapore's ageing population and a rise in chronic illnesses associated with a modern lifestyle by leveraging technological developments to transform the healthcare sector. The MOH has identified certain key digital health technologies for study and funding, and such efforts can be expected to spur the growth of these subsectors.

AI is expected to play a pivotal role in the transformation of Singapore healthcare systems, driven by initiatives being taken in public healthcare institutions. Efforts are underway to identify proven and impactful AI use cases, with a view towards eventually scaling them into system-wide, national initiatives. Current plans include implementing the use of various generative AI tools to automate routine tasks such as updating/summarising of patient records to free up healthcare workers' time and provide better service to patients, as well as implementing AI in diagnosing and treating patients in multiple fields, including radiology, ophthalmology and oncology.

As regards data analytics/predictive preventative care, it is recognised that AI can also be used to deliver predictive preventative care through the implementation of disease prediction models based on parameters such as health status, lifestyle, socio-economic status, and that access to genomic data will further strengthen this. In line with this, the government has announced plans to invest S$200 million over the next five years to fund support for public healthcare institutions to ramp up preventive care through the use of AI tools and genomic data. An example of such an initiative is a national genetic testing program for familial hypercholesterolemia, which will identify patients with abnormally high cholesterol levels for genetic testing, and encourage immediate family members of such patients to be tested as well, thereby enabling at-risk persons to be counselled to adopt healthier lifestyles and be started on cholesterol-lowering therapies with a view to reducing/avoiding future heart disease and cardiovascular complications. Success in this program is likely to encourage the expansion of a similar approach for the management of other major severe diseases such as cancer, kidney failure, stroke and heart attack. Additionally, the National Precision Medicine program collects genomic data with a view to promoting health outcomes through precision medicine (i.e. rather than treating all patients with a particular condition in the same way, individual variations in genetics, environmental and lifestyle factors are taken into account to allow greater precision in predicting the efficacy of treatment and prevention strategies for particular groups of patients). The program is particularly valuable for its ability to collect data from the Asian population, which is presently underrepresented in global genomic research. Ultimately, the program seeks to facilitate the implementation of precision medicine in Singapore on a large scale by 2030.

Concurrently, platforms for digitised and integrated health systems (such as the National Electronic Health Record ("**NEHR**") and the Health Hub mobile application) continue to be progressively implemented to facilitate the consolidation, digital management and sharing of patients' information and records across both the public and private sectors. The NEHR has been fully adopted by all public healthcare institutions, and all nine private hospitals in Singapore have committed to contributing health information of their patients to the NEHR. An upcoming Health Information Bill ("**HIB**") is anticipated to further mandate the contribution of selected key health information by the private sector (licensed healthcare providers and MOH-approved care providers).

1.3 What is the digital health market size for your jurisdiction?

We are not aware of definitive data on the digital health market size in Singapore. However, as an indication, Statista reports that the revenue generated by the digital health market in Singapore (including the digital fitness and well-being, online doctor consultations, and digital treatment and care markets) is projected to reach US$893 million in 2025.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

We are not aware of definitive data on the comparative revenue of digital health companies in Singapore.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Please see the response to question 1.4 above.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The key healthcare regulatory schemes related to digital health in Singapore involve the regulation of healthcare service providers and healthcare professionals, digital health devices, and cybersecurity and data protection.

The regulation of healthcare services is overseen by the MOH, which is the government ministry responsible for monitoring the accessibility and quality of healthcare services provided in Singapore. Healthcare services are regulated under the Healthcare Services Act 2020 ("**HCSA**") and its subsidiary legislation. Under the HCSA regime, providers of licensable healthcare services are required to obtain a licence, and may provide the licensable healthcare service through at least one of four Modes of Service Delivery ("**MOSD**"). One such MOSD available to certain licensable healthcare services (such as outpatient medical services) is remote provision; this entails the provision of care to a patient who is not physically present in the same place as the healthcare service provider through the Internet or any other kind of technology for facilitating communication (commonly referred to as "**telemedicine**").

Specific healthcare professionals involved in the supply of digital healthcare are each regulated by their respective professional bodies. For example, doctors are regulated by the Singapore Medical Council ("**SMC**") under the Medical Registration Act 1997; nurses are regulated by the Singapore Nursing Board under the Nurses and Midwives Act 1999. Each professional body also typically promulgates its own code of ethics and/or ethical guidelines.

As regards devices used in the delivery of digital health solutions, health products (which include medical devices) are principally regulated by the HSA, a statutory board under the MOH, whose remit includes regulating the import, manufacture, export and supply of medical devices in Singapore, and ensuring that drugs, therapeutics, medical devices and health-related products are regulated and meet safety, quality and efficacy standards. The HSA administers and enforces the Health Products Act ("**HPA**") and its subsidiary legislation, and also promulgates related guidelines. Telehealth products, such as wellness devices that do not fall within the definition of medical devices, are also subject to scrutiny by the HSA (see the Regulatory Guideline for Telehealth Products (April 2019)), although they do not generally require registration and licensing.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

The increased usage of digital health records by healthcare institutions and the advent of mandatory contribution of patient data to digitised integrated healthcare systems like the NEHR make having a robust cybersecurity and data protection regime imperative. In this regard, the Personal Data Protection Commission ("**PDPC**") and the Cyber Security Agency of Singapore ("**CSA**") serve as the key authorities with oversight over the personal data protection regime under the Personal Data Protection Act 2012 ("**PDPA**") and its subsidiary legislation and guidelines (including the PDPC's Advisory Guidelines for the Healthcare Sector), and the cybersecurity regulatory framework under the Cybersecurity Act 2018 and its subsidiary legislation and guidelines respectively. Finally, the MOH also promulgates its own guidelines in consultation with the aforementioned regulators (for example, the Cyber & Data Security Guidelines for Healthcare Providers, issued in December 2023). The proposed HIB (see the response to question 1.2) is also expected to require healthcare providers to meet cyber and data security requirements. In anticipation of this, the MOH has developed the Cyber and Data Security Guidelines for Healthcare Providers, in consultation with the CSA, the Infocomm Media Development Authority ("**IMDA**") and the PDPC, to provide guidance on the measures to be put in place for the proper storage, access, use and sharing of health information, in the lead-up to the implementation of the HIB.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The key areas of enforcement would generally mirror the areas of regulation in respect of medical devices, healthcare services and healthcare professionals, including registration, dealer's licensing, quality control, advertising, post-market obligations of record keeping and reporting, and the security of patients' medical and health information (see the response to questions 2.1 and 2.2 above). As new subsectors of digital health emerge (see the response to question 1.2), regulations and enforcement relating to these areas will need to be updated to keep pace with new technologies.

The development of regulations regarding the remote provision of healthcare services has long been closely watched by the MOH, and the recent months have seen robust enforcement action taken as regards telemedicine practices. The National Telemedicine Guidelines have provided guidance to telemedicine providers since 2015, and following a "regulatory sandbox" for telemedicine and mobile medicine providers in which the MOH sought to better understand the risks of these service delivery models, remote provision of outpatient medical services has (since 2023) been formally regulated under the HCSA. Further, doctors who practice telemedicine are subject to the SMC's Ethical Code and Ethical Guidelines (2016) ("**ECEG**"). At the end of 2024, a recent investigation by the MOH into the teleconsultation practices of a local clinic concluded with revocation of the clinic's licence to provide outpatient medical services, and the regulatory obligations imposed on providers of telemedicine services have been re-emphasised in a joint MOH-HSA-SMC circular on regulations and professional standards for telemedicine services and advertisements.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

Where software falls within the definition of a medical device, this is regulated under the HPA regime (see the response to question 2.1). Such software includes software embedded in medical devices, standalone software (also known as "software as a medical device" or "**SaMD**"), standalone mobile applications and web-based software. The HPA and its subsidiary legislation, such as the Health Products (Medical Devices) Regulations 2010, set out the requirements for (amongst other things) registration, manufacturing and supply of SaMD. Unless exceptions (such as a special access route) apply, registration is generally required before the SaMD can be put to clinical use.

Key HSA guidelines relevant to SaMD include the recently updated Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach (March 2024) ("**Guidelines for Software MD**") and the Regulatory Guideline for Telehealth Products (April 2019). The HSA has also issued Guidelines for Classification of Standalone Medical Mobile Applications (SaMD) and Qualification of Clinical Decision Support Software ("**CDSS**") in April 2022, with the aims of harmonising the HSA's approach in determining the risk classification of SaMD with the International Medical Device Regulators Forum's guidance on SaMD and providing better clarity on the qualification of CDSS as medical devices.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Where AI/machine learning- ("**ML**") powered digital health devices or software solutions fall within the definition of a medical device, these are generally regulated under the HPA regime (see the response to question 2.1).

Particular guidelines have also been promulgated by relevant authorities to guide organisations in the deployment of AI medical devices ("**AI-MD**"). These include Part 9 of the HSA's Guidelines for Software MD, as well as the Artificial Intelligence in Healthcare Guidelines ("**AIHGIe**") (October 2021), which were co-developed by the MOH, the HSA and Synapxe Pte Ltd (the national HealthTech agency formerly known as the Integrated Health Information System). The PDPC has also articulated a technology- and sector-agnostic AI governance approach to AI, known as the *Model Artificial Intelligence Governance Framework* (2nd ed., January 2020) ("**Model AI Framework**").

More recently, the growing prevalence of generative AI has seen an associated need to consider and manage the risks associated with its use, including the need for improved AI governance. In this regard, the IMDA, Aicadium (a global technology company founded by a state-owned investment company for creating and scaling AI solutions), and AI Verify Foundation (a not-for-profit foundation launched under the IMDA to gather contributions of the global open-source community in developing AI testing tools to support responsible AI use) jointly published a *Discussion Paper on Generative AI: Implications for Trust and Governance* (June 2023) identifying certain key risks associated with generative AI.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Where AI/ML-based digital health solutions fall within the definition of "medical devices" under the HPA, they are regulated as such under the HPA regime (see the response to question 2.1). The processes of obtaining registration and dealers' licences in respect of such AI-MD would thereby follow the general processes applicable to medical devices in Singapore. On our understanding that the reference to the "*dynamic nature of AI/ML-based digital health solutions*" refers to the fact that AI-MD have continuous learning capabilities, the regulator has taken this into account in the relevant guidelines. For example, Part 9 of the HSA's Guidelines for Software MD sets out guidelines targeted at AI-MD. These include that at the pre-market registration stage, information regarding the ML model used in the AI-MD must be submitted and if the AI-MD has continuous learning capabilities and can change its behaviour post-deployment, the learning process must be defined by the manufacturer of the medical device, and appropriate measures implemented to control and manage the learning process. After deployment in the market, AI-MDs are also subject to continuous monitoring of real-world clinical performance where data is collected to verify that the software continues to meet safety and effectiveness claims and allow for timely detection of new and evolving risks arising from the use of the AI-MD (see further details in the response to question 2.7). Finally, a Change Notification must be submitted if there is any change to a registered medical device that affects (i) the particulars provided upon registration, or (ii) the safety, quality and efficacy of the medical device pursuant to the Health Products (Medical Devices) Regulations 2010. Bearing in mind that AI-MDs are particularly susceptible to change due to their continuous learning capabilities, further guidance on when a Change Notification is required in relation to AI-MDs is set out in Part 9.4 of the Guidelines for Software MD. The AIHGIe also contains similar recommendations at paragraph 6.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Post-market monitoring of AI/ML-based digital health solutions is an important part of the Singapore regulatory regime. The HSA's Guidelines for Software MD and the AIHGIe provide further details on the role played by clinical validation data. For instance, developers and distributors of deployed AI-MD are expected to collaborate with the implementers and users of AI-MD to ensure software traceability, monitor and review the performance of AI-MD. Developers are also expected to introduce protocols to log factors that cause changes to the model to ensure traceability. This is considered especially pertinent for AI-MDs with continuous learning algorithms, to ensure that the AI-MD remains accurate and to prevent concept drift. Developers are also expected to apply appropriate control measures on any findings after deployment. In addition, periodic post-market reports are also to be submitted to the HSA, to enable the HSA to intervene in a timely manner if necessary.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Singapore is a single-state jurisdiction with no distinction between state/regional and federal/country regulation.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Digital health products and solutions are generally regulated as medical devices and the regulator's enforcement powers are therefore those available in respect of medical devices (see Part 10 of the HPA).

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

The following paragraph relates to the following technologies: telemedicine/virtual care; robotics; wearables; virtual assistants (e.g. Alexa); mobile applications; SaMD; CDSS; AI/ML-powered digital health solutions; Internet of Things and connected devices; 3D printing/bioprinting; digital therapeutics; digital diagnostics; electronic medical record management solutions; big data analytics; blockchain-based healthcare data sharing solutions; and natural language processing.

The following issues generally apply to all the above technologies: (i) categorisation of the relevant devices as medical devices under the HPA, and if so, determining the applicable risk classification (which has an impact on registration and licensing requirements); (ii) data protection and security; (iii) obtaining informed consent from patients to the use of such technologies; and (iv) maintaining standards of healthcare that are comparable to traditional modes of delivery.

Technologies that involve AI/ML and continuous learning capabilities, in particular, raise issues concerning ensuring that the deployment of AI in decision-making is done in a way that ensures that the decision-making process is explainable, transparent and fair, and that the use of AI solutions prioritises the well-being and safety of the humans it affects.

Technologies that involve the processing, sharing and management of confidential patient data in a digitised form also particularly raise issues of the consent required in relation to the collection, use and disclosure of patient data, as well as the need for regulation to ensure that data is not only kept secure from inadvertent data leaks and cyberattacks, but also kept accurate and safe from tampering or corruption (see further comments on this and related issues in the responses to question 2.2, section 4 and question 9.4).

Under the Cybersecurity Act 2018, acute hospital care services and services relating to disease surveillance and response have been identified as essential services. Therefore, information technology systems relevant to the provision of such services could potentially be designated as critical information infrastructure and require compliance with the obligations under the Cybersecurity Act 2018.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Please see the response to question 3.1.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Key issues to be considered include transfers of personal data outside of Singapore (if the digital health technology provider stores personal data outside of Singapore), ensuring the security of users' personal data and the purposes for which personal data of users will be put to (beyond providing the service or product to users); for example, whether the personal data will be used for health/clinical research by a third party.

In relation to the use of personal health data:

- the HCSA contains prescriptions on safeguards to be implemented to protect healthcare records and ensure their confidentiality, integrity and availability;
- the Health Products (Clinical Trials) Regulations 2016 requires appropriate consent to be obtained from, and sufficient information on intended uses of personal health data to be provided to, clinical trial participants;
- the Human Biomedical Research Act 2015 requires appropriate consent to be obtained from, and sufficient information on intended uses of personal health data to be provided to, human biomedical research participants, or a tissue donor for the removal, donation or use of human tissue; and
- the upcoming HIB is likely to make the misuse of healthcare data obtained from the NEHR an offence.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Singapore is a single-state jurisdiction with no distinction between state/regional and federal/country regulation.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The considerations change if one entity is acting as a data intermediary (e.g. data storage provider) of another entity (e.g. product owner) that collects the users' personal data. A data intermediary is an entity that processes personal data on behalf of another entity under a contract. It has fewer obligations under the personal data protection regime and is only required to: protect the personal data in its possession or under its control with reasonable security arrangements; cease to retain documents containing personal data (or remove the means by which personal data can be associated with individuals) if the purpose for which the personal data was collected is no longer served by the retention and there are no legal or business purposes for the retention; and notify the entity that it is processing personal data on behalf of any occurrence of a data breach. In contrast, the entity for whom the data intermediary processes personal data is responsible for the personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the entity itself.

The considerations also change depending on the nature of data – for dealings with personal health data, depending

on the context, entities may have additional obligations to comply with under the personal health data-related legislation mentioned in the response to question 4.1. Further, while the PDPA does not prescribe any additional legal requirements for information that may be considered sensitive, the sensitivity of data may simply be a factor for consideration in the application of the requirements under the PDPA, e.g. personal health data should be safeguarded by a higher level of protection and data breaches involving personal health data may attract higher penalties.

4.4 How do the regulations define the scope of personal health data use?

Generally, the regulations do not define the scope of data use. This depends on the nature of the digital health technology and the purposes for the collection, use and disclosure and whether users consent to the purposes. However, there are certain purposes for which consent of users is not required and this list was expanded in 2021. Accordingly, if the scope of data use falls within such purposes, the regulations could be said to affect the scope of data use, assuming separate consent cannot be obtained.

Depending on the context, the personal health data-related legislation mentioned in the response to question 4.1 may additionally affect the scope of personal health data use (e.g. where specific consent is sought from a research subject for human biomedical research).

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

The types of personal data collected, used and disclosed, the purposes for which the personal data collected will be used and disclosed, and the parties to whom the personal data will be disclosed to should be clearly identified when obtaining consent from users. If there is to be any cross-border transfers of personal data, relying on contractual terms to comply with relevant data protection requirements is common, and this should be considered when entering into/preparing the relevant contract. Depending on the context, contractual terms may also provide that an entity will comply with relevant additional obligations under the personal health data-related legislation mentioned in the response to question 4.1.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Data inaccuracy, depending on the cause of the inaccuracy, is potentially a breach of the obligation under the personal data protection regime in Singapore, as well as regulations applicable to healthcare services providers and healthcare professionals to ensure that personal data and patient records are accurate. The PDPC has the power to investigate any complaints of potential breaches and impose fines, if it is of the view that there was a breach. Where the technology concerned is regulated as a medical device, data inaccuracies would have implications under the medical device regulatory regime (e.g. adverse event reporting, field-safety corrective actions, product recalls). The same risks identified may similarly apply in relation to data bias and/or discrimination that give rise to errors or safety issues, particularly for digital health solutions that are regulated as medical devices.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

Please refer to the personal health data-related legislation mentioned in the response to question 4.1.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Whether the users have consented to the sharing of their personal data, the purpose for which the personal data is shared and whether any exceptions are applicable. If the sharing of personal data involves data transfers out of Singapore, the requirements for data transfers must be complied with.

Patient confidentiality is another key issue, and healthcare service providers and healthcare professionals need to be particularly cautious when allowing patients' medical information to be shared, including not to run afoul of ethical duties. For example, doctors need to be mindful of the provisions of the SMC's ECEG regarding medical confidentiality. Further, a breach of patient confidentiality could attract civil liability as a breach of confidence.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Singapore is a single-state jurisdiction with no distinction between state/regional and federal/country regulation.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

The considerations change if an entity is a data intermediary. Please see the response to question 4.3.

The sources, expression and nuances of the obligations of patient confidentiality may be different depending on the nature of the entities/persons in question (e.g. different professional bodies may articulate obligations of confidentiality differently), although the gist of the obligations are unlikely to vary hugely between healthcare service providers and healthcare professionals generally.

The considerations also change depending on the nature of data – for dealings with personal health data, depending on the context, entities may have additional obligations to comply with under the personal health data-related legislation mentioned in the response to question 4.1.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Please refer to the personal health data-related legislation

mentioned in the response to question 4.1, as well as the last paragraph of the response to question 1.2 (on the NEHR and HIB).

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Please see the response to question 10.8 – in order to facilitate greater integration of the healthcare ecosystem, the HIB is planned to be implemented in the future, but presently, details on how this is to be done and the language of the Bill have not been announced.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Patent protection is available for an invention that is new, involves an inventive step and is capable of industrial application. Under the patent examination guidelines, for computer-implemented inventions, it must be established that said computer (or other technical) features, as defined in the claims, is integral to the invention in order for the actual contribution to comprise said computer (or technical features). Patents are protected for a period of 20 years from the date of application, once granted.

The Intellectual Property Office of Singapore ("**IPOS**") has also recently released Supplemental Guidance for Examination of AI-related Patent Applications, as a quick patentability reference for applicants seeking to protect their AI-related inventions.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Copyright protects expression of original works. Computer programs and software are literary works in which copyright can subsist. Copyright lasts for the life of the author plus 70 years (or 70 years after the year the work is first published if the author is not identified).

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secrets are protected through the law of confidence in Singapore. The protection of trade secrets is enforced through actions for the breach of confidence for any unauthorised access, use, referencing or disclosure. Trade secrets must be demonstrated to be information that is of a sufficiently high degree of confidentiality (e.g. secret processes of manufacture such as chemical formulae or special methods of construction) and not every piece of confidential information will constitute a trade secret.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

There are no laws that apply specifically to academic technology transfers in Singapore. The National IP Protocol may apply to academic technology transfers if the technology transfer takes place in the context of publicly funded research and development ("**R&D**") activities. Please see the response to question 6.7.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Copyright would protect the SaMD as a literary work. Whether patent protection is available depends on the scope of the invention and whether it fulfils the requirements of being new and involving an inventive step (the third requirement of being capable of industrial application would be satisfied).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

This issue has not yet been tested before the Singapore courts. There is case law that interprets "inventor" under the Patents Act 1994 as being a natural person.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

There are no laws that apply specifically to government-funded inventions in Singapore. However, the National IP Protocol applies to all public agencies and R&D activities funded by public agencies. It sets out a general framework and principles for how intellectual property ("**IP**") arising out of public agencies/publicly funded R&D activities should be owned, protected, used and commercialised. It states that public agencies should generally reserve a royalty-free, irrevocable, worldwide, perpetual and non-exclusive right to use any licensed or assigned IP for their statutory functions, non-commercial and/or R&D purposes. Public agencies should consider the commercial interest of the third party before applying this principle and act in a manner that supports the effective commercialisation of the IP by the third party. Commercialisation of IP created using public funds should also benefit the researchers who are the inventors or creators of the IP.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

The Supplemental Guidance for Examination of AI-related Patent Applications was issued by IPOS recently in October 2024. While it is a guide and not in the nature of legislation or binding case law, it provides guidance to digital health innovators who may be looking at exploring patent protection for AI-related inventions.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

Singapore law allows parties to determine *inter se* the ownership of IP in collaborative improvements. Whilst parties

generally gravitate towards some type of co-ownership, and setting up a regime for this is possible as a matter of law, we would generally suggest that parties designate a single owner.

Parties may also contractually provide for ownership and rights of control of data generated from such collaborative improvements, e.g. controlling future uses of the data.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

No special considerations apply, beyond the need for the healthcare company to comply with its usual regulatory obligations (and to check if any are specifically triggered by the agreement in question).

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Parties should consider contractually allocating the risk arising from additional obligations that may apply in the case of accidental or unauthorised re-identification of improperly anonymised healthcare data.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Parties who are users should contractually ensure that relevant data is not used for training or fine-tuning/customisation and improve coverage of certain associated risks that may arise from the use of generative AI (e.g. data protection and confidentiality issues, copyright infringement issues).

Strategically, for digital health solution providers, parties should consider how they intend to position the product in the local market and keep in mind the intended prescribed use(s) of the digital health solution in the healthcare context as this has an impact on the regulatory risk classification and extent of regulatory controls over the solution.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

There is no specific or overarching AI/ML legislation in Singapore. Various regulatory authorities have sector-specific initiatives related to AI/ML. That being said, the IMDA has been closely involved in several initiatives relating to AI/ML in Singapore.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

Presently, there is no specific legislation for the regulation of AI in Singapore, or AI-specific legislation applicable for the healthcare sector. Singapore has adopted a light-touch approach to AI governance and regulation where various regulatory authorities have issued guidelines/frameworks relating to AI, including:

- The PDPC's Model AI Framework.
- The IMDA and AI Verify Foundation's *Model AI Governance Framework for Generative AI: Fostering a Trusted Ecosystem* (30 May 2024) ("**Model GenAI Framework**"), and its companion material like the Implementation and Self-Assessment Guide for Organizations.
- The PDPC's Advisory Guidelines: Use of Personal Data in AI Recommendation and Decision Systems (March 2024).
- The CSA's Guidelines on Securing AI systems (October 2024).
- The AIHGIe.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

This issue has not yet been tested before the Singapore courts. Current case law requires that there must be a human author identified before a literary work will be an original work in which copyright subsists. Works created by humans with the assistance of AI may be protectable by copyright on the basis that the human is the author.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Common commercial considerations include the value of the data (e.g. whether other third parties have similar data), which may have an impact on whether the party providing the data can negotiate for any rights to any IP/value that is generated through the use of the data for ML. Since no IP subsists in data (except as a compilation, provided the compilation was created through the application of intellectual effort, creativity or exercise of skill or judgment), protecting the use of data by the receiving party through contractual restrictions and obligations (including confidentiality) is important.

The same commercial considerations apply when licensing healthcare data.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

See the response to question 8.2 – different guidelines issued by different regulatory bodies have specific guidelines for AI/ML, and some are targeted specifically at generative AI to address the different risks arising from each technology.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

See the response to question 8.2 – at present, Singapore has adopted a light-touch approach to AI governance and regulation

where in place of legislation, a risk-based, accountability-based, light-touch and voluntary governance approach is adopted through providing guidance to the industry.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

In Singapore, it is permitted (i.e. not an infringement) to use copyright-protected works for "computational data analysis", which would include training AI/ML. This exception is limited to training and does not extend to commercial applications of the AI/ML model. There are also certain purposes under the PDPA for which consent of users is not required, such as where personal data is used for business improvement or research.

There are currently no data disgorgement laws or initiatives in Singapore. Legal remedies generally available for infringement would be applicable such as injunctions, damages, account of profits and statutory damages. Regulatory authorities can also mete out financial penalties for unauthorised data uses and breach of the relevant regulations.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

In Singapore, liability for adverse outcomes in digital health solutions is typically based on tort or contract law. For example, actions for injuries caused by the use of faulty digital health products are typically founded on the tort of negligence, which requires that the elements of negligence (i.e. a duty of care, breach of the standard of care, causation and damage that is not too remote) be proven. Further, actions for breaches of patient confidentiality could amount to the tort of breach of confidence.

In addition, a contractual claim may lie if a contractual relationship exists between the claimant and defendant, and the adverse outcome arises due to breach of term of a contract and/or the contract prescribes remedies for the adverse outcome.

9.2 What cross-border considerations are there?

Increased popularity of digital health solutions gives rise to the increased potential for cross-jurisdictional delivery of healthcare (e.g. through telemedicine) or cross-jurisdictional manufacture or marketing of digital health equipment. This raises questions of, amongst others: (i) the proper forum for pursuing a claim; (ii) the applicable law for the purposes of determining liability if an adverse outcome occurs; and (iii) the enforcement of any award/judgment where a defendant's assets are situated in a foreign jurisdiction.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

In addition to complying with the regulatory requirements relating to ongoing clinical validation and post-market surveillance in place for AI-MDs set out in the responses to questions 2.6 and 2.7 above, the *Model AI Framework* and *Model GenAI Framework* also describe some best practices that may help organisations deploying AI technologies minimise the associated risks. These include: (i) ensuring that responsibility for and oversight of the various stages and activities involved in AI deployment are allocated to the appropriate personnel and/or departments, and ensuring that relevant personnel are aware of their responsibilities, properly trained, and provided with resources and guidance needed to discharge their duties; (ii) using reasonable efforts to ensure that data sets used for training the AI model are adequate for their intended purpose and to manage the risk of inaccuracy and bias, as well as reviewing exceptions identified during model training; (iii) establishing monitoring and reporting systems/processes to ensure that appropriate parties are kept informed should there be any issue relating to the deployed AI; and (iv) adopting third-party testing to enable independent verification of quality of the AI/ML.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

In Singapore, liability for the misuse of such healthcare data includes criminal liability under the PDPA for acts such as the unauthorised disclosure of personal data and improper use of personal data without authorisation to cause harm/loss to another or gain to oneself. Additionally, if the misuse leads to a breach in patient confidentiality, there may be civil liability under the torts of breach of confidence and/or negligence. Finally, if a contract governs the use of the data, civil liability may lie for breach of contract.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cybersecurity and data protection (in particular where electronic health records of patients are involved) issues apply equally for Cloud-based services for digital health. Please see the responses to question 3.1, and sections 4 and 5.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Depending on the manner of entry, there may be additional regulatory requirements, such as those highlighted in our responses above.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

The healthcare industry in Singapore is a highly regulated space, and specific regulations/requirements may apply depending on the precise operations/transactions in play. Venture capital and private equity firms should consider and seek advice on the relevant regulations (including the need for due diligence on potential regulatory exposure) before investing in digital healthcare ventures in Singapore. Depending on the technology involved and the area of application in digital health, it may also be necessary to consider

freedom-to-operate searches to assess third-party IP infringement risks and whether sufficient steps have been taken to protect IP rights that may subsist in the digital health solution.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Digital health solutions are increasingly available in Singapore. However, key challenges for widespread clinical adoption of digital health solutions include:

- Costs of digital transformation: Costs may include initial set-up costs and costs of maintaining digital systems, as well as employee training, creation of compliance strategies and the implementation of security measures to protect data.
- Singapore's ageing population: Many elderly Singaporeans remain unfamiliar with technology and digital health solutions, and training programmes/outreach efforts may be costly.
- The inability of digital health solutions to replicate the compassion and empathy associated with the healthcare profession: Patients may prefer the face-to-face interactions of visiting their doctor or healthcare professional.

In the context of implementing AI solutions, challenges include resolving questions of whether use of patient data and other confidential health information in the use, development and training of AI programs may infringe upon healthcare services providers' obligations in respect to the use of such data/information, and obtaining informed consent from patients for the use of AI-MD in the delivery of care (which raises novel issues of the extent of information that a clinician has to give a patient about the nature of the AI input and the risks involved in the use of AI as compared to conventional management).

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

Clinician certification bodies (such as the Specialists Accreditation Board under the Medical Registration Act 1997) do not routinely have the clinical adoption of digital health solutions as a focus. Instead, the clinical adoption of digital health solutions is heavily influenced by the Singapore Government. In this regard, the MOH has set up an Office for Healthcare Transformation, which aims to evolve the healthcare system into one that is data-driven and digitally enabled. Further, there are government efforts in place such as the Smart Nation initiative, which seeks to leverage digital technologies to enhance Singapore's economy and society. Beyond the Government, sentiments of healthcare professionals and the public and practical issues such as the costs of implementation influence the adoption of digital health solutions.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

Patients who use digital health solutions in Singapore can be reimbursed by government insurers or private insurers. Details of the extent to which reimbursement will be provided and the requirements for reimbursement, including whether there are any requirements on the digital health solution provider, would depend on the specific coverage agreed between the insured and insurer.

Business entities that wish to adopt digital health solutions may be eligible for funding under the Enterprise Development Grant, which provides funding support for businesses to improve resource efficiency through automation and technology.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Due diligence gaps in the context of digital health solutions arise in relation to ensuring the AI/ML-based solution's reliability, which is likely to have an impact on patient safety (whether directly or indirectly). In this regard, the AIHGIe has identified a non-exhaustive list of areas in which these gaps may occur in the context of digital health solutions in the healthcare ecosystem, particularly for digital health solutions that would be regulated as medical devices using AI/ML with continuous learning capabilities:

- inappropriate initialisation parameters (i.e., incorrect or unsuitable starting settings);
- biased or unrepresentative input data that ultimately affect the algorithms behind the AI/ML-based solution;
- difficulties in fully validating the accuracy of updates to the model algorithms to ensure clinical validity and accuracy due to continuous learning capabilities;
- abnormal behaviour (e.g., maliciously introduced data) and/or end-user manipulations (e.g., the introduction of rare yet valid and important data); and
- ensuring clinical viability of synthetic data sets used in training and development of algorithms.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

Given various trends, such as an ageing population, there is an increasing focus on primary care to prevent illness, including increasing the support for private general practitioners. The HIB is planned to be introduced to facilitate greater integration of the healthcare ecosystem, by requiring licensed healthcare providers (including private providers) to input patients' medical records into the NEHR. This enables important patient data to be made accessible to various care providers and facilitate good continuity of care, and also enhances overall efficiency of the healthcare system.

From a legal perspective, issues such as risks of potential mismanagement of/improper access to patient data, and cybersecurity lapses, arising from expanded collection, storage and sharing of patient data, will become more acute. Adequate safeguards will need to be considered and implemented. How the law attributes responsibility and liability for breaches will be closely examined. Patient preferences, including, for example, the choice and extent thereto to restrict the sharing of their data in the NEHR, will also have to be considered.

Acknowledgments

The authors would like to thank Sreshya Kamakshi Vishwanathan and Charlene Tan, Associates at Allen & Gledhill LLP, for their valuable assistance in the preparation of this chapter.

Gloria Goh is a Counsel in the Technology & Corporate Intellectual Property Practice. Her areas of expertise are in intellectual property, technology and pharmaceuticals, health products, cosmetics and food regulation. She has expertise in the regulatory aspects of pharmaceuticals, medical technology, health products, clinical and biomedical research, cosmetics and food law. Her experience includes advising clients on clinical trial agreements, informed consent documents for use in clinical trials and other commercial agreements relating to pharmaceuticals and health products. Her experience also includes a broad range of contentious and non-contentious matters involving trade mark, copyright, patent, domain names, confidential information and data protection. She has also conducted intellectual property audits for clients, advised clients on intellectual property management and strategy, the acquisition and licensing of intellectual property.

Allen & Gledhill LLP
One Marina Boulevard, #28-00
Singapore 018989

Tel: +65 8318 0162
Email: gloria.goh@agasia.law
LinkedIn: www.linkedin.com/in/gloria-goh-283546186

Koh En Ying specialises in litigation and dispute resolution. Her work involves court disputes, arbitrations and mediations in a range of civil litigation areas, with a focus on medical malpractice and construction disputes. She has experience dealing with medical negligence claims, disciplinary proceedings and Coroner's inquiries, and has advised and represented a medico-legal defence organisation, insurers, healthcare professionals and healthcare institutions in matters across a range of general and specialist medical practices. Her practice also includes advising on healthcare regulatory issues, such as the regulation of healthcare professionals, healthcare service providers and health products, including where relevant to operational matters and corporate transactions. She presently sits on the Advisory Board of the Singapore Psychological Society.

Allen & Gledhill LLP
One Marina Boulevard, #28-00
Singapore 018989

Tel: +65 9730 9974
Email: koh.enying@agasia.law
URL: www.allenandgledhill.com/sg/partners/5019/koh-en-ying

Tham Hsu Hsien regularly advises healthcare professionals, healthcare institutions, and professional indemnifiers and insurers on contentious and non-contentious healthcare matters. In particular, he regularly acts for medical and dental professionals in contentious malpractice claims in the Courts and disciplinary actions before the Singapore Medical Council and Singapore Dental Council. He also advises and acts for banks in major banking and trusts disputes, and for creditors and debtors in restructuring and insolvency matters. He has an active contentious employment practice, with particular interest and experience in wrongful dismissal and restraint of trade matters.

Allen & Gledhill LLP
One Marina Boulevard, #28-00
Singapore 018989

Tel: +65 9798 0538
Email: tham.hsuhsien@agasia.law
URL: www.allenandgledhill.com/sg/partners/4971/tham-hsu-hsien

Alexander Yap is the Co-Head of the Firm's FinTech Practice and a Partner in the Technology & Corporate Intellectual Property Practice. He advises on three key pillars:

- the acquisition, divestiture, provision, sharing and receipt of data, technology and intellectual property-related services and assets, including cryptographic tokens and digital assets;
- data breach and cybersecurity strategy, communications, management and compliance; and
- emerging and frontier technologies, such as autonomous driving, metaverses, large language models, transformer neural networks and generative AI.

Allen & Gledhill LLP
One Marina Boulevard, #28-00
Singapore 018989

Tel: +65 9010 3081
Email: alexander.yap@agasia.law
LinkedIn: www.linkedin.com/in/alexander-yap-a327471b

Switzerland


Dr. Tobias Meili


Dr. Carlo Conti


Dr. Martina Braun


André S. Berne

Wenger Plattner

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no common general definition of "digital health" in Switzerland. Medicinal products (i.e., pharmaceuticals) and medical devices are subject to general regulation by the Federal Therapeutic Products Act (TPA). Detailed provisions are regulated in several ordinances. However, neither the TPA nor its ordinances contain a legal definition of the term "digital health".

The Federal Office of Public Health (FOPH), which by default acts as the competent authority for all public health matters, defines "digital health" applications and devices as products that use digital technology to accomplish their medical objectives. This includes telemedicine, telemonitoring, mobile applications and other similar applications, but not digital applications that solely assist healthcare professionals in their duties (such as controlling a device or reading and analysing data).

Swiss scholars partially use the term "digital health" as a collective term for "eHealth" (i.e., the use of ICT in healthcare) and "mHealth" (i.e., the use of mobile devices for patient care, such as smartphones or tablets).

1.2 What are the key emerging digital health subsectors in your jurisdiction?

Growing use of telemedicine: Telemedicine solutions enjoy an extensive presence, are widely recognised in Switzerland and continue to further emerge. For instance, one of the largest medical telemedicine centres in Europe is managed by the Swiss digital health company *Medgate* in Basel, providing health insurance providers with the opportunity to serve as their policyholders' family physicians and/or gatekeepers. *SWICA*, a health insurance provider, among others, also provides telemedicine solutions, telemedical consultations and remote monitoring of vital parameters. Based on this, further telemedicine models enter the sector. Hence, an important part of the Swiss population has already been exposed to telemedicine.

Electronic Patient Record (EPR): In April 2017, the Federal Electronic Patient Record Act (EPRA) came into force. The purpose of the law is to establish a basis that, in the future, all patient records are maintained exclusively digitally and that all vital health documents (e.g., nursing and hospital reports, examination results, X-rays) are centrally stored and securely shareable among healthcare professionals. The EPRA and its implementing ordinances regulate the framework conditions for the introduction and dissemination of EPRs in Switzerland. Therefore, all hospitals are required to join a state-certified parent organisation that provides EPRs to private individuals. The use of an EPR is, nevertheless, voluntary for physicians (so far), as well as the general public, and funds for implementation are lacking. Consequently, implementation is currently advancing only incrementally, although there is great public interest and extensive media coverage. Therefore, and to assist the EPR in reaching a breakthrough, the EPRA is currently undergoing a comprehensive revision to mandate all healthcare providers to use the EPR and a provisional financing arrangement was implemented on 1 October 2024 to allow companies to receive financial state aids.

Wearables: Wearable technology monitoring personal health information in real time is fashionable and gaining users steadily. Since the COVID-19 pandemic, wearables have experienced additional expansion: the rise in interest in personal health monitoring and the adoption of remote work have both contributed to this development.

eMedication: "eMedication" refers to electronic systems that furnish data regarding the prescription, dispensation and processing of a patient's medication. This feature facilitates a multitude of operations, including the establishment of a medication schedule and a medication reminder system and is intended to increase process efficiency and patient safety. eMedication is a prevalent use case within the EPR framework. For instance, the EPR can be integrated with reminder functions that prompt patients to take their prescribed medications.

E-commerce of therapeutic products: In Switzerland, medicinal products do not necessarily have to be purchased in brick-and-mortar pharmacies or physicians' practices, but pharmacies may upon request be granted the permission to engage in mail-order sales under certain conditions (Art. 27(2-4) TPA). Patients can therefore order medicinal products and certain medical devices online from a Swiss mail-order pharmacy and have them delivered at home. Over 30 mail-order pharmacies are currently active in Switzerland. However, following a Federal Supreme Court (FSC) ruling in September 2015, such pharmacies must request a prescription for both prescription-only and over-the-counter (OTC) medicinal products (FSC 142 II 80). Thus, prior consultation with a physician remains mandatory.

1.3 What is the digital health market size for your jurisdiction?

The Swiss market for digital health products and services is expanding rapidly. Several market size estimates exist, contingent upon the pertinent key performance indicators

and the definition of digital health (see question 1.1). A study by McKinsey assumes that the potential for utilising digital health in Switzerland amounts to around CHF 8.2 billion.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

A considerable number of digital health-specialising companies are also engaged in other technology or health-related industries. Thus, there are no reliable data regarding what the largest digital health companies in Switzerland are. Global technology companies, including Apple, Google, Huawei, IBM, Samsung and Xiaomi, are important players in the Swiss digital health market, as in other countries. Furthermore, several companies have established themselves in the field of telemedicine and e-commerce with therapeutic products (see question 1.2). In addition, more and more spin-offs, particularly from the two Swiss Federal Institutes of Technology in Zurich and Lausanne, are entering the market and often arise foreign investors' interest.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

In Switzerland, there are nearly 200 companies engaged in the digital health sector, demonstrating varying rates of growth. Since revenue information is typically not disclosed to the public, a subjective evaluation is necessary. Furthermore, the varying levels of maturity among the companies must be considered: start-ups and scale-ups typically experience rapid growth; however, their overall market significance often remains quite limited. Some notable companies include: (i) Sleepiz, a manufacturer of medicinal products focused on sleep quality; (ii) Dacadoo, a provider of health scoring and lifestyle navigation solutions; (iii) Bluespace Ventures, which offers an integrated healthcare ecosystem platform in Switzerland under the Compassana trademark; (iv) OptiChroniX, whose solutions target modifiable risk factors for cognitive health in older adults; and (v) Holmusk, a European branch of a Singaporean company specialising in data analytics and digital therapies.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

In Switzerland, the FOPH is by default the competent authority for all public health aspects, unless the cantonal (health) authorities are in charge. In the area of therapeutic products, however, neither the FOPH nor the cantonal health authorities, but rather the Swiss Agency for Therapeutic Products (Swissmedic) acts as the competent Swiss regulatory and supervisory authority for medicinal products, including OTC products as well as medical devices (Arts 68, 69 and 82 TPA).

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

The core principles are outlined in the TPA, which refers to medicinal products and medical devices as "therapeutic products" (Art. 2(1)(a) TPA, "*Heilmittel*"). This also includes OTC medicinal products, as well as supplements to medical devices. Due to the high export rate of such products to the European Union (EU), the Swiss legislator aims at a far-reaching conformity between Swiss and EU law.

Detailed provisions that are crucial in practice are regulated in several Ordinances such as the Medical Devices Ordinance (MedDO). Since digital health technologies often qualify as medical devices, the requirements of the MedDO apply. In addition, EU regulations pertaining to medical devices must be considered in conjunction with Swiss statutory provisions when it comes to digital health technologies that qualify as medical devices.

Finally, if cantonal health authorities are competent in a certain matter (e.g. in case of authorisations for medical activities), the relevant cantonal regulations apply.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

If digital health technologies or products do not comply with the provisions of the Swiss Data Protection Act (FADP), the cantonal criminal authorities may impose fines of up to CHF 250,000 on offenders in accordance with the penal provisions of chapter 8 FADP.

Digital health technologies or products that qualify as medical devices according to the TPA must comply with the regulations of the TPA and MedDO. Failure to comply with the regulations of the TPA or the MedDO may qualify as a criminal offence (Arts 86 and 87 TPA). For example, intentional introduction, export or use of non-compliant medical devices, or the use of medical devices without meeting the necessary technical and operational requirements may be sanctioned by imprisonment of up to three years or a fine (Art. 86(1)(d) TPA).

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

Digital health solutions qualify as medical devices when they (i) are intended to be used for human beings, and (ii) serve to fulfil medical purposes, such as (a) diagnosis, prevention, monitoring, treatment or alleviation of diseases, injuries or disabilities, (b) investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, (c) providing information by means of *in vitro* examination of specimens derived from the human body, including organ, blood and tissue donations, and/or (d) control or support of conception (Art. 3(1)(c) MedDO).

According to Swissmedic, acting as the competent Swiss regulatory and supervisory authority for medical devices, software or apps are not considered medical devices if their sole purpose is related to fitness, well-being, nutrition (such as diets), hospital resource planning, reimbursement, management of doctors' visits, statistical analysis of clinical or epidemiological studies or registers, functioning as a diary, replacing paper-based health data, or serving as electronic reference works containing general non-personalised medical information. In September 2018, the Swiss Federal Administrative Tribunal (FAT) ruled in a landmark decision that an app designed to assess a woman's fertility by analysing her vital signs meets the criteria to be classified as a medical device (FAT C-669/2016).

Thus, the term "medical device" is interpreted comprehensively. Hence, if software has a medical purpose, regardless of whether it has a proven medical effect, it may qualify as a medical device. In such a case, the software must adhere to the regulatory requirements that apply to medical devices.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Current Swiss legislation does not encompass AI/machine learning (ML)-powered digital health devices or software solutions. Consequently, the overarching principles are applicable to these products; if classified as a medical device, the relevant regulations for clinical use must be adhered to (see question 2.4 above).

It is important to note that medical devices, in contrast to medicinal products (for the differentiation, see question 1.1) are not governed by a state authorisation process; instead, they adhere to the principle of self-regulation, wherein conformity is demonstrated through a declaration from the manufacturer, typically validated by a conformity assessment body. Whoever manufactures or distributes medical devices is required to establish a reporting system and notify Swissmedic of adverse effects and incidents (Art. 59 TPA). Based on such a notification or its official market surveillance, Swissmedic can take the necessary action in a particular instance, including recalls (Art. 66(2) TPA).

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Swissmedic has set itself the strategic goal of increasing its own use of AI/ML technologies by 2026. So far, no established supervisory practice has yet been developed for AI/ML-based digital health technologies.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

See question 2.6 above.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Digital health products are typically classified as medical devices (see question 2.4 above) as regulated by the TPA and the MedDO. Due to their nature as federal laws, the Cantons lack legislative authority but play a role in the law's enforcement: on the one hand, Swissmedic operates with the Cantons' involvement (Art. 68(1) TPA), as the Cantons have the right to nominate members to the Swissmedic Agency Council (Art. 72(2) TPA); on the other hand, the Cantons are tasked with regulating points of sale, particularly medical practitioners, and issuing retail trade licences for the sale of therapeutic products, including digital health products, in establishments such as pharmacies and drugstores, as well as overseeing the related inspection system.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

See question 2.6 above.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Telemedicine and virtual healthcare are well-established practices in Switzerland (see question 1.2 above). Except for specific cantonal regulations, telemedicine is not governed by any legal provision. However, telemedicine is permitted to a certain extent by the regulations that govern the professional obligations of physicians so long as it satisfies the obligations of the duty of care.
- **Robotics**
  Depending on their intended use, robotics in healthcare may be classified as medical devices and, thus, subject to the relevant medical device regulations (especially TPA and MedDO).
- **Wearables**
  Wearables collect and process vital signs (heartrate, blood pressure, etc.), which from a legal perspective qualify as personal data. Accordingly, the collection and processing of such data must comply with the FADP. Additionally, if these devices qualify as medical devices due to their potential for medical applications (refer to question 2.6) they must comply with regulatory requirements applicable to medical devices.
- **Virtual Assistants (e.g. Alexa)**
  See question 3.1, Wearables.
- **Mobile Apps**
  See question 3.1, Wearables.
- **Software as a Medical Device**
  See question 2.6.
- **Clinical Decision Support Software**
  See question 2.6.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  See questions 8.1 and 8.2.
- **IoT (Internet of Things) and Connected Devices**
  Depending on their intended use, IoT and connected devices in healthcare may be classified as medical devices.
- **3D Printing/Bioprinting**
  A fact sheet pertaining to the 3D printing of medical devices was released by Swissmedic. Swissmedic distinguishes in this regard between adaptable medical devices, mass-produced/patient-matched medical devices and custom-made devices (Art. 10 MedDO). Bioprinting technology may give rise to several regulatory and legal concerns pertaining to transplantation, gene technology, intellectual property and liability law.
- **Digital Therapeutics**
  The term "digital therapeutics" encompasses a wide range of device-controlled therapy measures. Digital therapeutics, specifically, could potentially be impacted by both the regulatory requirements applicable to medical devices and the data protection provisions outlined in the FADP.
- **Digital Diagnostics**
  In Switzerland, like in the EU, the regulatory obligations pertaining to *in vitro* diagnostics are regulated in

a specific legal statute, which is the *In Vitro* Diagnostic Medical Devices Ordinance (IvDO). The latter sets forth that it applies – *inter alia* – to software or systems, whether used alone or in combination, intended by the manufacturer to be used *in vitro* for the examination of specimens derived from the human body (Art. 3(1)(a) IvDO). Thus, digital diagnostics must meet the requirements of the IvDO. Depending on the manufacturer's intent, additional regulatory or legal requirements may apply (see also questions 2.1, 2.3 and 2.6).

- **Electronic Medical Record Management Solutions**
  See question 1.2, Electronic Patient Record (EPR).
- **Big Data Analytics**
  The regulatory approach on big data analytics is caught in a dilemma: whilst this technology raises significant data protection concerns, the purpose of a medical treatment using big data can only be achieved through transparency. Furthermore, there may be situations where legal requirements are in direct contradiction to each other.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Blockchain-based healthcare data sharing technology has the potential to streamline and increase the transparency of processes within the healthcare sector. However, Swiss healthcare regulatory authorities have not yet explicitly designated this technology as a target of regulation. Like other technologies, its legal or regulatory issues are thus contingent upon its specific objective. Accordingly, blockchain technologies that meet the criteria for medical devices might also be subject to their regulatory requirements.
- **Natural Language Processing**
  Natural language processing (NLP), i.e., the computer-based capability to comprehend spoken and written language in a manner analogous to that of humans, is not generally classified as a medical device. NLP may, notwithstanding, be susceptible to regulatory requirements applicable to medical devices, provided that the manufacturer explicitly designate it for medical use. Moreover, data protection requirements must be observed.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

In Cantons where digital platform providers are permitted to establish operations, the competent cantonal authority must issue an operating licence to such digital platform providers who wish to offer digital health services. This necessitates, *inter alia*, that the individual bearing the ultimate medical responsibility meets the prerequisites for ordinary physicians and that he/she directly and personally practises his/her profession. Nevertheless, delegation is permissible, specifically to practice assistants with sufficient training and oversight. The competent authority has the power to exercise discretion in determining the personnel that is necessary for the digital health activity.

Furthermore, it is mandatory to uphold medical confidentiality and ensure the safeguarding of patient records to prevent unauthorised access. Depending on the location of the digital platform provider, other and/or additional key issues may arise. Thus, a case-by-case assessment is always necessary.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The FADP governs the processing of personal data by private persons and federal bodies. Data processing activities of cantonal bodies are subject to the respective cantonal data protection legislation.

Personal data is defined as all information relating to an identified or identifiable natural person. Data of legal entities are not considered personal data. The FADP recognises so-called sensitive personal data for which stricter rules apply in certain aspects. Among others, health data is considered as sensitive personal data.

The FADP outlines several principles to be observed for the processing of personal data: processing must be lawful, conducted in good faith and proportionate. Personal data may only be used for the purposes for which it was collected, and those purposes must be made transparent to the data subjects. If personal data is no longer necessary for processing, it must be either destroyed or anonymised. Additionally, the processed personal data must be accurate and protected through appropriate technical and organisational measures. Finally, the law provides for several further obligations of data processors and for rights of the concerned data subjects.

It is important to note that in contrast to the EU GDPR, the FADP does not require a justification for every data processing activity by private persons. Therefore, data processing by private persons is in principle permitted unless explicitly prohibited by law.

In addition to the requirements stipulated by data protection legislation, healthcare professionals and their auxiliaries must adhere to professional confidentiality obligations, the breach of which is subject to criminal sanctions.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

As outlined above, the FADP governs the processing of personal data by private persons and federal bodies, whilst data processing activities of cantonal bodies are subject to the respective cantonal data protection legislation (see question 4.1). This also applies to personal health data.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The FADP distinguishes between private data processors and federal bodies. Federal bodies are subject to more stringent requirements. Data processing by cantonal bodies is governed by the respective cantonal data protection legislation (see question 4.1). For example, healthcare professionals employed by cantonal hospitals are subject to the cantonal data protection legislation in question. Further, the FADP recognises so-called sensitive personal data (e.g., health data), for which stricter rules apply in certain aspects (see question 4.1).

4.4 How do the regulations define the scope of personal health data use?

Personal data may only be processed for the specific purpose for which it was collected, and which purpose is transparent to the individuals whose data is being processed, unless there exist grounds for justification (e.g., the data subject's consent, an overriding private or public interest, or an explicit legal basis). Moreover, federal bodies may only process personal data if there is a statutory basis for doing so.

The FADP contains a list of circumstances in which the controller may have an overriding interest. This may be the case, among others, if the data controller processes personal data for non-personal purposes, such as research, planning or statistics, provided that the following requirements are satisfied: in such cases, the data controller must (a) anonymise the personal data as soon as the processing purpose allows, or if anonymisation is not feasible or requires disproportionate effort, implement appropriate measures to prevent the identification of the data subject, (b) disclose personal data that includes sensitive personal data (such as health data) to third parties in a manner that renders the data subject unidentifiable, and if this is not possible, guarantee that the respective third parties process the personal data only for non-personal purposes, and (c) publish the results in a way that prevents the identification of the data subject.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

The roles and responsibilities of the parties involved in data processing must be defined. In the case of the assignment of data processing to a third-party data processor, it is necessary to establish a written data processing agreement (DPA). A DPA should in particular set forth the rights and obligations of the parties, including the controlling rights of the data controller. Further, the data processor must undertake to implement and maintain adequate technical and organisational measures, which must be described in detail. For joint or independent data controllers, a contractual agreement is not mandatorily required, unlike under EU GDPR. However, it might nevertheless be advantageous in many instances to define at least the basic responsibilities of each party regarding the respective data processing activities in writing.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The principle applies that only accurate personal data may be processed. Every data subject has the right to have inaccurate personal data corrected. Furthermore, the constitutional prohibition of discriminations also applies to the processing of personal data by federal bodies.

If a decision, which produces legal effects for a data subject or significantly affects a data subject, is based on automated decision-making, the data controller shall, upon request, provide the data subject with the opportunity to make a statement. The data subject may also request that the automated decision-making be reviewed by a natural person.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The FADP and the cantonal data protection laws set forth the principles governing the collection and use of personal health data. Further, the Swiss Federal Health Insurance Act (HIA) imposes strict limits on how insurers can use health data, ensuring it is only processed for specific purposes, namely the provision of insurance services. The Swiss Federal Electronic Health Records Act (EHR) and, more generally, the eHealth Switzerland initiative aim at facilitating the secure exchange and management of health information, whilst giving patients control over who accesses their data. Finally, the Swiss Medical Association (FMH) has issued several guidelines directed at healthcare professionals, which outline the applicable data protection principles, and emphasise patient confidentiality and the necessity of informed consent.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Under the FADP, it is crucial to distinguish between sharing personal data with a data processor and sharing it with a third party. Subject to statutory or contractual confidentiality obligations (such as, for example, medical professional confidentiality obligations), the sharing of personal data with a data processor is generally permitted, requiring only a DPA, assurance of the data processor's data security and informing data subjects about the categories of recipients receiving their personal data. If the data controller is bound by professional confidentiality obligations, generally the consent of the data subject is necessary.

If personal data is shared with third parties, stricter rules apply when it comes to the disclosure of special categories of personal data such as health data. The disclosure of such data by private processors requires either consent of the data subject, an overriding private or public interest or justification by law. Moreover, federal bodies may only disclose personal data (irrespective of whether sensitive or not) to third parties if there is a statutory basis for doing so, or if one of the statutory exceptions apply (see question 5.2).

Another critical consideration is the location where the shared data is processed. Personal data may only be transferred to countries that afford a level of protection which is deemed adequate from a Swiss law perspective. If personal data is disclosed to countries with data protection legislation of a comparatively lower standard, this is permissible only (a) with the data subject's consent, (b) under contractual agreements ensuring a level of data protection equivalent to Swiss standards, or (c) if any of the other statutory exceptions apply.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

See questions 5.1 and 5.3.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Here again, a distinction is made as to whether the data controller is a private person or a federal body.

For the processing of personal data (including disclosure) by a data controller who is a private person, see question 5.1.

Personal data may only be processed and disclosed to third parties by a federal body if there is a statutory basis or if one of the statutory exceptions apply (see questions 4.4 and 5.1). Additionally, personal data may be disclosed in the context of public information if it pertains to a public duty and there is an overriding public interest. The data subjects may object to the disclosure of certain personal data by federal bodies if they can demonstrate a protected interest. However, the federal body may disregard the objection if there is a legal duty to process the data or if fulfilment of the respective body's tasks would otherwise be jeopardised.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

As laid out, the FADP imposes requirements on the collection, processing and sharing of personal health data (see question 5.1). The HIA regulates the exchange of data between those responsible for implementing, monitoring or supervising the implementation of said act (see also question 4.7). The eHealth Strategy, overseen by the FOPH, aims at establishing an interoperable digital healthcare ecosystem that promotes secure and efficient data exchange. In particular, the EHR shall be revised comprehensively and facilitate secure data sharing across healthcare providers, with patient consent as a central principle. Further, see also question 5.5.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Federated models of healthcare data sharing must navigate complex regulatory considerations and technical challenges. Interoperability standards are the basic prerequisite to enable seamless data exchange across decentralised systems. Security measures, including encryption, access controls and audit trails, are essential to protect sensitive health information. Contractual frameworks, such as DPAs, clarify responsibilities and liabilities, particularly in the event of data breaches. In order to promote the digital transformation in the healthcare sector, the Federal Council has launched the so-called "*Digisanté* Project", to be implemented from 2024 onwards. This project aims at creating a nationwide digital healthcare system for the secure and seamless exchange of data, including a medical register. All stakeholders shall obtain access to the relevant health information in accordance with data protection legislation. Data entry shall be performed in a uniform and standardised way, which shall improve the quality and safety of the entire treatment chain, from prevention to diagnostics, treatment and care. Secure access to standardised data shall also help to promote academic and industrial medical research and the professional and political management of the healthcare system.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Digital health products regularly encompass both software and hardware elements. Patents for inventions are granted for new inventions applicable in industry. There exist no specific requirements for innovations in the digital health sector. However, exclusions from patentability cover, among others, methods for treatment by surgery or therapy and diagnostic methods practised on the human or animal body. Also excluded are computer programs as such, which are protected by copyright law (see question 6.2). However, computer-implemented inventions, which solve a technical problem, are patentable.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

The Swiss Federal Copyright Act (CopA) protects literary and artistic intellectual creations of individual character, irrespective of their value or purpose. Computer programs are explicitly recognised as copyright-protected works. Digital health software can therefore be protected by copyright if the requirements are met. It is worth mentioning that there are no specific formal requirements to obtain copyright protection in Switzerland. Copyrights are automatically established upon the creation of the respective work.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secrets are protected by provisions of the Federal Unfair Competition Act and the Swiss Criminal Code. Furthermore, the Swiss Code of Obligations stipulates that an employee may not utilise or disclose to others any facts to be kept secret, in particular manufacturing and business secrets, of which he or she becomes aware in the service of the employer. No specific provisions apply to digital health technologies.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Based on the laws described above, universities and colleges issue their own regulations concerning the utilisation of intellectual property in the context of university activities.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

See questions 6.1–6.4.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

No, in principle only individuals can be named as inventors.

Whilst a device or AI may contribute to the invention process, only a human being may be named as inventor. Nevertheless, there is an ongoing debate in Switzerland regarding whether it is necessary for an inventor to be a natural person. A notable case regards the AI system DABUS. On 15 October 2024, the Swiss Federal Administrative Court held a public hearing on this case, with arguments and counterarguments for AI inventorship being discussed. The court's final decision, which decision may have significant implications for the future of AI-based inventions in Switzerland, is still pending at the time of writing.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

The Federal Act on the Promotion of Research and Innovation sets the legal basis for the promotion of research and of aspects of innovation in Switzerland. Together with the Federal Act on Funding and Coordination of the Swiss Higher Education Sector it defines the legal framework for scientific activities in Switzerland.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

Several key precedents in the realm of intellectual property rights concern digital health innovation. Besides the ongoing DABUS case (see also question 6.6), it is worth mentioning that the Swiss Federal Patent Court has issued several rulings clarifying the scope of patentability for digital health technologies. Finally, an example relating to trademark law regards the rejection of the registration of the trademark "ID NOW" for medical devices by the Federal Administrative Court, based on the grounds that said sign was considered descriptive of the respective goods (ruling B-1776/2023). The ruling clarifies the high standards of distinctiveness required for trademarks and reiterates that trademarks must not give rise to misleading expectations as to the functionality or performance of the respective products, which also applies in the area of medical devices.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

In practice, collaborative agreements are frequently entered into with universities, non-university research institutions and/or other industrial partners, in addition to internal research and development activities. As a starting point, the involved parties need to determine whether they are interested in engaging in a research collaboration or in conducting contract research. Research cooperation agreements are frequently considerably more complex than mere research agreements due to various regulations governing the transfer of IP rights and their compensation.

Furthermore, to facilitate the commercial exploitation of the work results from such collaboration, it is essential that the respective party's intellectual property rights be protected. Additionally, publication rights, marketing rights, regulatory responsibility and product liability ought to be contractually agreed upon.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

In addition to the aforementioned aspects (see question 7.1) and the core healthcare regulatory schemes to be complied with (see question 2.1 *et seq.*), particular attention must be given to ensuring that healthcare companies and their employees do not obtain undue benefits (Art. 55(1) TPA). The existence of an undue benefit must be determined on a case-by-case basis; benefits of modest value (up to CHF 300 annually) or in support of research, further education or training, contingent upon fulfilling specific criteria are, for example, not considered as "undue" (Art. 55(2)(a)(b) TPA).

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Federated learning (FL) in healthcare is the process of developing ML models over datasets that are distributed across various data centres (e.g., hospitals, clinical research labs and mobile devices) without exchanging the data itself. Companies dealing with agreements establishing such collaboration and data sharing must determine whether they are members of a FL consortium in which all other parties are trustworthy prior to proceeding (i.e., whether attempts to corrupt the model or intentionally extract sensitive information can be excluded). Furthermore, by definition, FL systems prevent the exchange of health-related data among participating institutions. However, through reverse engineering, the shared information may still indirectly expose private (highly sensitive) health data (i.e., leakage risk). Mitigation of the results from all these risks is required.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

See questions 8.3, 8.4 and 9.3.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

See questions 2.5, 2.6 and 2.8.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

See questions 2.4 and 2.8.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Intellectual property may only be created by a natural person (i.e., a human being) in accordance with Swiss copyright and patent law (Art. 6 CopA; Art. 3(1) Patent Act). As a result, advancements achieved through ML without explicit human intervention do not qualify as inventions protected under Swiss intellectual property law. Nevertheless, dissenting views exist regarding the allocation of credit to the algorithm's owner (e.g., programmer) for works and inventions generated by algorithms. However, ownership cannot be acquired by or through an algorithm.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

When procuring data for ML, it is crucial to consider significant commercial factors. These include, but are not limited to: (i) establishing data ownership and intellectual property rights; (ii) defining financial terms including fees and royalties; (iii) addressing concerns related to data security and confidentiality; and (iv) ensuring adherence to applicable laws and regulations, with particular emphasis on privacy. The application of ML in digital health technologies may potentially involve sensitive personal data, which raises several obligations under the FADP (see question 1.3).

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

As far as can be seen, no established practice has yet emerged among regulatory bodies overseeing AI/ML technologies to differentiate between standard AI and generative AI technologies and products.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

See question 8.5 above.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

If AI/ML models are trained on data for which the developer lacks the appropriate data rights, the developer may face legal consequences under the FADP (see question 4.1 *et seq.*). Any person may request from a data controller information about the processing of personal data concerning him or her, which he or she has provided to the data controller, in a commonly used electronic format, if (i) the controller processes the data by automated means, and (ii) the data are processed with the consent of the data subject or in direct connection with the conclusion or performance of a contract between the controller and the data subject (Art. 28(1) FADP).

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Digital health solutions are subject to the general rules on contractual and tort law liability. In addition, the regulations governing therapeutic products stipulate that whoever manufactures or distributes therapeutic products (including but not limited to digital health solutions) is required to establish a reporting system and notify Swissmedic of adverse effects and incidents that (i) are attributable to the therapeutic product itself, its use or improper instructions for use, or (ii) may endanger the health of consumers, patients, third parties or animals (Art. 59(1) TPA). Furthermore, quality issues must be reported to Swissmedic (Art. 59(2)(3) TPA).

Violations of the reporting obligations primarily trigger criminal law consequences (Art. 87(1)(c) TPA). However, civil liability may also apply based on (i) the Swiss Product Liability Act, which is based on the EU product liability directive, (ii) contract law, and/or (iii) tort law. In addition, a manufacturer may be held jointly and severally liable with any authorised representative in Switzerland of a person injured by a digital health solution that qualifies as a defective medical device (Art. 47d(2) TPA).

A certificate of conformity (CoC) for a digital health solution that qualifies as a medical device may be an indicator that the product is not defective. However, such CoC does not exempt a manufacturer of the respective product from potential product liability claims.

9.2 What cross-border considerations are there?

Anyone who manufactures a digital health solution that qualifies as a medical device in Switzerland, or who makes it available in Switzerland, must report any adverse reactions suspected of being associated with this medical device to Swissmedic (Art. 66(1) MedDO). The response to such alerts is entirely up to Swissmedic's discretion. However, recalls in the US and/or the EU may encourage Swissmedic to consider similar administrative measures in Switzerland, as well.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

When deploying generative AI in Swiss digital health solutions, (i) compliance with the FADP, (ii) assurance of transparency and informed consent from users, as well as (iii) maintenance of accuracy and dependability via routine validation and documentation should take precedence. The incorporation of professional oversight and human intervention mechanisms are crucial in the healthcare decision-making processes. User agreements should incorporate unambiguous liability disclaimers and limitations, which underscore the technology's supportive nature. Furthermore, it is imperative to enforce strict cybersecurity protocols and to ensure ongoing training for healthcare professionals.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

Swiss Civil law may hold entities accountable under contractual and non-contractual theories for harm caused by negligent or improper use of AI/ML models, including medical malpractice claims if AI decisions lead to medical errors or harm. Furthermore, under the FADP, misuse can lead to violations of privacy rights and data protection, especially if sensitive health data is processed without consent or adequate safeguards. Additional liability provisions may apply.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Cloud-based digital health services and their interfaces are usually hosted on external systems and sometimes even spread across several platforms. Therefore, when sharing data with other parties, key concerns are data security, namely the potential for unauthorised disclosure of personal data, the encryption and interoperability of data, the coordination of access and incident management, as well as data protection issues since cloud-based services for digital health store substantial quantities of very sensitive data (see question 4.1). In addition, it is necessary to ascertain whether the cloud-based services for digital health meet the criteria to be classified as a medical device (see question 2.3).

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Digital health products and/or services are subject to rigorous regulation and oversight. Therefore, regulatory and data protection considerations necessitate a thorough assessment of the respective company's business model and its intended use of products and/or services. A comprehensive compliance organisation considering, among others, the aforementioned factors should be established prior to the entry of non-healthcare companies into the digital healthcare market. Ultimately, we recommend evaluating whether Swiss compulsory health insurance may potentially cover the cost of the digital health products and/or services in question (see questions 2.2 and 10.6).

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

Key topics that should be considered before investing in digital healthcare ventures are the adherence to the constantly evolving data protection requirements, the necessity for comprehensive title-chain documentation, the ramifications of employee stock option plans, and the identification and adherence to relevant healthcare regulatory schemes (see questions 2.1 *et seq.*).

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

High market-entry barriers, a complex procedure for registering new products or services for reimbursement by compulsory health insurance, and a complex regulatory framework in general are the key barriers for new digital health solutions in Switzerland. In addition, Switzerland is a federal state comprising 26 Cantons, each of which may have its own regulatory requirements on certain healthcare aspects. Moreover, the presence of four official languages in Switzerland may necessitate the employment of multilingual staff depending on the business model, products or services.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

The FMH is the professional association of all Swiss physicians and issues the FMH Code of Ethics and its appendices, which must be observed by all physicians. Given that the implementation of digital health solutions is essentially governed solely by law, the FMH's influence is limited to political advocacy work for its members' interests and those of patients to influence the respective legislative process.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

The possibility of reimbursement by mandatory health insurance for the use, rental or sale of digital health solutions is governed by the HIA and its ordinances. The FOFP is the competent authority in all matters relating to this. Several digital health solutions already exist in Switzerland, which are reimbursed by mandatory and/or private insurances. Nevertheless, the approaches utilised for this are highly dependent on the structure of this digital health solution. For instance, in most Cantons, the reimbursement application for a telemedicine solution can be submitted together with the request to carry out such an activity. Therefore, a case-by-case assessment is recommended.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

In Switzerland, certain due diligence gaps within the healthcare ecosystem for evaluating digital health solutions may create challenges for stakeholders in maintaining safety, compliance and ethical standards. Identified gaps encompass: (i) data governance, characterised by insufficient clarity regarding data ownership, consent management and compliance with data protection requirements, especially for sensitive health data; (ii) algorithm transparency, marked by limited understanding of AI/ML models' decision-making processes, which may give rise to liability and unfair competition risks; (iii) regulatory oversight, with the absence of specific regulations for AI/ML in healthcare (see question 2.5), resulting in uncertainties related to compliance with medical device regulations and standards for safety and efficacy; (iv) interoperability, emphasising challenges in ensuring secure and effective integration of digital health solutions with existing healthcare systems and standards; and (v) clinical validation, indicated

by the lack of robust frameworks for the ethical evaluation and clinical validation of AI/ML models in medical contexts, potentially undermining trust and effectiveness.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

In addition to the issues mentioned above, the evolution of Swiss regulatory (digital) health policy is to be seen in conjunction with similar EU policy. Given that Switzerland's largest trading partner is the EU, and that Switzerland exports a significant quantity of therapeutic products to EU Member States, the Swiss legislator strives for a comprehensive harmonisation of Swiss and EU legislation. Consequently, developments in Swiss digital health are also profoundly influenced by EU regulatory developments.

Dr. Tobias Meili is a Partner in the practice groups Governance & Compliance, Life Sciences & Health law, and Corporate & M&A. He advises clients, particularly in the life sciences sector, on commercial and corporate law, especially on corporate governance (including corporate responsibility issues), restructuring, M&A, and contract and technology law. His area of expertise also includes internal investigations as an examiner or investigator appointed by FINMA or companies.
Due to his many years of experience in a leading position in the legal department of a formerly SMI-listed multinational corporation and an international consulting and technology company, Tobias is familiar with the structures, processes and challenges of large companies. In his legal practice, he combines an authentic, pragmatic and solution-oriented advisory approach with solid legal expertise and negotiation skills.

Wenger Plattner
Aeschenvorstadt 55, 4010 Basel
Switzerland

Tel: +41 61 279 70 00
Email: tobias.meili@wenger-plattner.ch
LinkedIn: www.linkedin.com/in/tobiasmeili

Dr. Carlo Conti is an Of Counsel in the field of Life Sciences and Health law. He advises institutions and organisations on issues related to life sciences and health law, as well as on constitutional and administrative law matters. He is President or member of various boards of directors. He has many years of professional experience and profound knowledge in all areas of life sciences and health law, as well as in constitutional and administrative law. For more than 15 years, he held executive positions in the pharmaceutical industry. Subsequently, Carlo became a member of the state government in Basel-Stadt and head of the public health department. He was also President of the Swiss Conference of Public Health Ministers and Chairman of the board of Swiss DRG AG, as well as Vice President of the board of Swissmedic (the Swiss Agency for Therapeutic Products).

Wenger Plattner
Aeschenvorstadt 55, 4010 Basel
Switzerland

Tel: +41 61 279 70 00
Email: carlo.conti@wenger-plattner.ch
URL: www.wenger-plattner.ch/en/team/conti-carlo

Dr. Martina Braun is Counsel and a member of the practice groups IP, IT & Data Protection and Sports law. She advises and represents companies, foundations and individuals in all areas of intellectual property law and information technology, with a particular focus on copyright and trademark law as well as data protection law. Her key area of expertise is advising on contract law. She specialises in particular in licensing and sponsorship agreements in the sports and entertainment sectors. Furthermore, she deals with various questions to personality rights.
Martina has written a dissertation on copyright law and completed a CAS in international sports law.

Wenger Plattner
Seestrasse 39, CH-8700 Küsnacht-Zurich
Switzerland

Tel: +41 43 222 38 00
Email: martina.braun@wenger-plattner.ch
LinkedIn: www.linkedin.com/in/martina-braun-81930b20

André S. Berne is a Senior Associate and primarily deals with commercial and regulatory issues. His main areas of focus include life sciences law, health law and competition law, as well as data protection. Furthermore, he advises companies and organisations on Swiss commercial and corporate law, administrative law and EU law, and represents them before courts and authorities in German and French. In addition to his advisory and litigation activities, André prepares expert opinions in his areas of specialisation. He regularly publishes and lectures in these fields.

Wenger Plattner
Aeschenvorstadt 55, 4010 Basel
Switzerland

Tel: +41 61 279 70 00
Email: andre.berne@wenger-plattner.ch
LinkedIn: www.linkedin.com/in/andr%C3%A9-s-berne-866b0199

Wenger Plattner has been advising and representing clients in all areas of business law for over 40 years, with more than 100 employees in its offices in Basel, Zurich and Bern. The firm's lawyers identify practical, workable solutions and help clients implement these to achieve the best possible commercial outcomes. Wenger Plattner has a team of experts, many of whom are involved in decision-making as members of public authorities and other bodies, giving them an in-depth understanding of client needs. As a fully integrated partnership, the firm places a strong emphasis on teamwork and co-operation. Wenger Plattner's clients have access to dedicated, highly experienced specialists who offer top-level advice to help them meet their specific objectives efficiently and effectively.

www.wenger-plattner.ch

Wenger Plattner

Taiwan


Tsung-Yuan Shen


Rachel Chen


Nita Ye

Lee and Li, Attorneys-at-Law

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no clear definition of "digital health" under Taiwanese law.

The definition of "digital medicine" provided in Article 4, Paragraph 1, Item 7 of the Act for the Development of Biotech and Pharmaceutical Industry may serve as a reference. Under such Act, "digital medicine" refers to an innovative product or technology that is applied in the field of healthcare with big data, cloud computing, Internet of Things (IoT), artificial intelligence (AI) and/or machine learning (ML) technologies, and is used to enhance the prevention, diagnosis and treatment of diseases, as approved by the competent authority in conjunction with the central governmental authority in charge of the subject industry. Notably, the medical device software using AI or ML technology shall be subject to the approval of the central governmental authority in charge of the subject industry.

Generally, "digital health" encompasses various domains, including mobile health, health information technology, wearable technology, telehealth and telemedicine, personalised medicine, and other uses of information and communication technology within the healthcare fields.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

In recent years, there have been significant investment in and development of medical technologies and digital health solutions. These include healthcare big data, IoT, AI, 5G technology, biomedical chip technology, sensors, wearable devices, biobanks, telehealth and telemedicine. Much of this investment and development has been encouraged by government organisations.

1.3 What is the digital health market size for your jurisdiction?

There are no official statistics regarding the digital health market size in Taiwan. According to data published by the Industrial Technology Research Institute, Taiwan's precision health market was estimated to be about NT$8.75 billion (around US$300 million) in 2020 and is expected to reach NT$14.2 billion (around US$490 million) in 2025.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

In Taiwan, the digital health market is primarily funded by leading electronic technology companies. Since these companies report their revenue based on overall enterprise performance, it is challenging to isolate their earnings or establish a ranking specifically within the digital health sector.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

As noted above, it is currently not easy to quantify or rank companies' performance in digital health. Many Taiwanese companies are investing considerable resources and efforts in this emerging industry. Benefitting from the advanced technologies, these companies are developing rapidly and each company has its own strengths.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The Ministry of Health and Welfare (MOHW) is the competent authority responsible for supervising healthcare-related matters, products and industries. The MOHW has a wide-ranging mandate aimed at enhancing the quality of healthcare service.

Under the MOHW, the Food and Drug Administration (TFDA) oversees the regulation of food, drugs, medical devices and cosmetics to ensure their safety and quality. The TFDA is responsible for granting product registrations and approving clinical trials, as well as monitoring manufacturing processes and imports. The TFDA also conducts safety surveillance activities for health-related products.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

The Medical Devices Act provides core regulations governing medical devices. Regarding digital health in the context of

a medical device, such aspect falls under the purview of the Medical Devices Act. According to the Medical Devices Act, the term "medical device" refers to instruments, machines, apparatuses, materials, software, reagents for *in vitro* use and related articles thereof, whose design and use achieve one of the following primary intended actions in or on the human body by means other than pharmacological, immunological, metabolic or chemical means: (a) diagnosis, treatment, alleviation or direct prevention of human diseases; (b) modification or improvement of the structure and function of the human body; and (c) control of conception.

From a legal perspective in Taiwan, the manufacture or import of medical devices can only be conducted once a medical device permit licence, which provides registration and market approval, has been issued by the MOHW. Furthermore, the production of medical devices must adhere to the guidelines established in the Good Manufacturing Practice (GMP) under the Pharmaceutical GMP Regulations.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The Medical Devices Act establishes a three-tiered classification system for medical devices based on risk levels: Class I for low-risk products; Class II for medium-risk products; and Class III for high-risk products.

Separately, any person who manufactures or imports medical devices without obtaining the prior approval could face imprisonment for up to three years, along with the possibility of an administrative fine not exceeding NT$10 million.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

In addition to the regulations discussed in our response to question 2.2, the Guidance for Medical Software Classification issued by the TFDA is also relevant to software as a medical device. On December 24, 2020, the TFDA published a revision to this Guidance, clarifying that medical software designed to monitor heart rate and blood oxygen levels (including wearable devices) for everyday health management of the general public is not classified as a medical device, provided it is not intended for disease diagnosis or treatment. On September 15, 2022, the TFDA published another revision to the Guidance, which adds multiple examples not classified as a medical device and the evaluation criteria for classifying medical software. However, the actual classification for a particular device is determined at the discretion of the competent authority.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

There are currently no specific regulations established particularly for AI/ML-powered digital health devices or software solutions. All medical devices fall under the purview of the Medical Devices Act, with Chapter IV outlining regulations related to the management of clinical trials for such devices. In addition to the Medical Devices Act, the relevant rules such as the Regulations on Good Clinical Practice for Medical Devices, the Human Subjects Research Act and the Regulations on Human Trials should be taken into consideration.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

On September 11, 2020, the TFDA published the Guidance for the Inspection and Registration of Medical Software of AI/ML-based Technologies. The Guidance describes the inspection and registration checkpoints for medical software using AI/ML-based technologies. Additionally, such Guidance is also applicable to the medical devices using AI/ML-based technologies.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Currently, all medical devices fall under the purview of the Medical Devices Act. In accordance with Article 37, Paragraph 1 of the Medical Devices Act, before initiating any clinical trial, the clinical trial institutions or trial sponsors shall file an application with the TFDA for prior approval.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

All digital health products and solutions classified as medical devices are regulated by the Medical Devices Act. The applicability and regulatory density do not vary between regional and country levels.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

The TFDA has published several guidelines that take into account the progress and advancement of technologies such as AI and ML for applicants' reference.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine and Virtual Care**: Under the Physicians Act, physicians are generally prohibited from treating or prescribing medication for patients they have not personally diagnosed, except in urgent situations or for those in remote areas. The Rules of Medical Diagnosis and Treatment by Telecommunications specify which locations qualify as mountainous, outlying islands or remote areas.
- **Robotics, Wearables and Related Technologies**: The legal and regulatory issues for robotics, wearables, mobile apps and software as medical devices align closely with those for telemedicine, particularly regarding medical device regulations, personal data protection and product liability.
- **Clinical Decision Support Software and AI Solutions**: These technologies face regulatory scrutiny similar to that applied to robotics, especially concerning the Physicians Act, if AI assumes roles traditionally held by physicians.

- **IoT, 3D Printing, Digital Therapeutics and Diagnostics**: These areas are governed by regulations similar to those applied to wearables and robotics, with specific concerns regarding the Physicians Act for AI applications.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

The Personal Data Protection Act (PDPA) serves as the primary legislation regulating the use, collection and processing of personal data to protect individual rights and ensure the responsible use of such information. Digital platform providers must adhere to the requirements outlined in the PDPA whenever personal data is involved in their products or services.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The PDPA serves as the primary legislation for personal data protection. Key considerations for the use of personal data under the PDPA include, but are not limited to, the following points:

- Determining whether the data qualifies as "personal data" under the PDPA.
- Assessing whether the "personal data" is considered "sensitive personal data" as defined in our response to question 4.4.
- Ensuring that the use of personal data adheres to the relevant regulations of the PDPA, including the necessity of obtaining informed consent from the data subject, or whether there is any exemption from the applicable requirements.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Personal data, including personal health data, is regulated by the PDPA. The applicability and regulatory density do not vary between regional and country levels.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

The considerations listed in our response to question 4.1 remain consistent, irrespective of the nature of entities involved. However, the types of exemptions from the requirement to obtain informed consent from the data subject vary between non-governmental and governmental entities.

4.4 How do the regulations define the scope of personal health data use?

Under the PDPA, "personal data" is defined in a broad manner to encompass various types of information, including: name; date of birth; identification card number; passport number; physical characteristics; fingerprints; marital status; family details; educational background; occupation; medical records; information regarding medical treatment; genetic data; details about sexual life; health examinations; criminal history; contact information; financial status; social activities; and any other information that could directly or indirectly identify an individual.

Furthermore, personal data related to an individual's medical records, healthcare, genetic information, sexual life, physical examinations and criminal record is categorised as "sensitive personal data", which is subject to more stringent regulations under the PDPA.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

If any collection, use or processing of personal data is contemplated under a contract, it is suggested that the "informed consent" requirement be fully complied with, unless any applicable exemptions are met.

Adhering to the PDPA, especially in securing the necessary "informed consent" for the use, collection and processing of personal data, as well as ensuring that the use and processing of such data remain within the defined scope of specific purposes, is a critical legal concern. Any breach of the PDPA, such as the unlawful use, collection or processing of personal data, could result in civil, criminal and/or administrative penalties.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Regarding personal health data inaccuracies, the PDPA grants data subjects the right to correct or supplement their personal information, as well as the right to request the deletion of the data.

In respect of data bias and discrimination, there are currently no specific laws or regulations in place to tackle such issues. However, we anticipate that discussions will increasingly arise in various legal fields, including labour and employment law (concerning factors such as gender, race, religion or beliefs, and political views), privacy law, antitrust law and other areas where concepts of "equality" and "fairness" are significant to social and economic activities. This is particularly relevant in light of challenges that may arise from the use of AI algorithms and big data analytics.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

Since its launch in 1995, Taiwan's National Health Insurance (NHI) system has been managed by the National Health Insurance Administration (NHIA), which oversees a vast amount of personal data. The NHIA delegated data management to the National Health Research Institute, which created the National Health Insurance Research Database for external research from 2000 to 2016. In response to concerns about data privacy, seven individuals objected in 2012 to the NHIA's release of their personal data to third parties, leading to petitions and lawsuits that were ultimately unsuccessful. In 2017,

they sought a constitutional interpretation regarding the legality of the data release.

In August 2022, Taiwan's Constitutional Court ruled that laws must be revised within three years to enhance personal data protection under the PDPA. Key requirements included establishing an independent oversight mechanism, clarifying regulations for NHI data usage, and allowing individuals to opt out of data usage. To comply, the PDPA was amended in May 2023, designating the Personal Data Protection Commission (PDPC) as the authority overseeing these regulations. A Preparatory Office for the PDPC has been established, with the official commission expected to launch soon.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Please refer to our response to question 4.1 above, as sharing personal data would be classified as "processing" and/or "use" of personal data under the PDPA.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Please refer to our response to question 4.2 above, as sharing personal data would be classified as "processing" and/or "use" of personal data under the PDPA.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

Please refer to our response to question 4.3 above.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

Please refer to our response to question 4.7 above.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Regarding federated models for sharing healthcare data, the concerns outlined in our answers to questions 4.1 through 5.4 are relevant and should be noted. For instance, the requirement for "informed consent" should be adhered to unless any of the applicable exemptions are met.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

The Patent Act defines patentable subjects as inventions, utility models and designs. An invention refers to technical ideas that leverage natural laws, while a utility model pertains to the shape or structure of an article, also based on natural laws. Designs focus on the aesthetic aspects, such as shape, pattern or colour, and can include applications for computer-generated icons and graphic user interfaces. For any of these categories to be patentable, they must meet requirements of novelty, inventive step and enablement. However, diagnostic, therapeutic and surgical methods for human treatment are excluded from patentability, which may affect digital health technologies that incorporate such methods.

Additionally, digital health inventions may involve software or algorithms, which are assessed under the Examination Guidelines for Computer-related Inventions. These guidelines classify software patents into three categories: process (specific operational steps using a computer); product (programmable devices directed by software); and computer-readable storage medium (articles that instruct a computer to perform functions). Software patents are deemed patentable if they effectively interact with computer systems to deliver technological advancements.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Under the Copyright Act, a "work" refers to a creation in the literary, scientific, artistic or other intellectual domains. This encompasses oral and literary works, musical compositions, dramatic and choreographic pieces, artistic creations, photographic images, pictorial and graphical works, audio-visual materials, sound recordings, architectural designs and computer programs. While there are no registration or filing requirements for copyright, certain criteria must be met for a work to qualify for protection, including "originality" and "expression". Additionally, software developed for "digital health" is eligible for copyright protection.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secrets are protected when they meet the following criteria: the information must be applicable in production, sales or operations; the information must possess a degree of secrecy; the information must have economic value; and the owner must have taken reasonable steps to maintain its confidentiality. There are no registration or filing requirements for legal protection of a trade secret. To maintain confidentiality during court proceedings, trials may be conducted privately if deemed appropriate by the court or agreed upon by the parties involved. In intellectual property (IP) lawsuits, parties can request the court to issue a "protective order". Individuals bound by such an order are prohibited from using the trade secrets for any purpose unrelated to the trial and must not disclose the secrets to anyone not covered by the order.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Academic institutions typically establish internal guidelines regarding academic technology transfers. In general, these internal policies outline the ownership and management of technologies developed by scholars, researchers,

graduate students and staff. Furthermore, institutions have the authority to license or assign their IP to third parties for commercial purposes, ensuring that the innovations generated within academia can be effectively utilised in the marketplace while adhering to established legal frameworks.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

Software can be protected through various rights, including patents, copyrights and trade secrets. Specifically, for software-implemented inventions that combine software and hardware to process information and achieve a technical effect, patent protection is often available. This legal framework ensures that developers can safeguard their innovations, fostering an environment conducive to technological advancement in the medical field.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

The Taiwan Intellectual Property and Commercial Court has specifically determined that AI cannot be designated as an inventor of a patent. Judicial practice, particularly rulings from the Taiwan Intellectual Property and Commercial Court, holds that patent inventions stem from the creative capacities of the human spirit, which AI lacks. According to Taiwanese law, only natural or legal persons are entitled to hold such rights.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

Government-funded inventions are governed by specific IP rights as outlined in the Fundamental Science and Technology Act and the Government Scientific and Technological Research and Development Results Ownership and Utilization Regulations. When projects in scientific and technological research and development (R&D) receive government support, the management and utilisation of the resulting R&D outcomes must adhere to such regulations.

Notably, the R&D results and any income generated may be partially or wholly assigned to the executing R&D units for ownership or licensing, and are exempt from the National Property Act. Furthermore, the determination of ownership and utilisation rights is guided by principles of fairness and effectiveness. This assessment considers various factors, including the contributions of capital and labour, the nature of the R&D results, their potential applications, societal benefits, national security implications and market impact.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

In Taiwan, there are currently no notable judicial precedents specifically addressing IP rights concerning digital health innovations. The Taiwan Intellectual Property and Commercial Court has determined that AI cannot be recognised as an inventor for patent purposes, and that patent inventions must originate from human creativity, as only natural or legal persons can hold such rights under Taiwanese law.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

Effective collaboration relies on well-defined agreements concerning IP ownership, obligations and responsibilities. It is crucial to evaluate applicable laws and agreements among involved parties, especially between funding providers and inventors or developers. Typically, IP laws state that ownership of collaborative improvements is governed by existing agreements; in their absence, rights generally belong to the inventor or developer, while the funding provider may utilise the invention.

In copyright scenarios, the creator is recognised as the author and retains economic rights unless a mutual agreement specifies otherwise. Although the funding provider can use the work, ownership rights remain with the author. Co-ownership of improvements requires adherence to specific provisions in the Patent Act. Joint patent applications must be filed collectively, and any independent filing by a co-owner risks patent cancellation by others. Furthermore, joint patent rights cannot be assigned or abandoned without unanimous consent from all co-owners; if a co-owner abandons their share, such share reverts to the remaining owners. Ultimately, clear agreements are essential for clarification of IP rights in collaborative endeavours.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

As stated in our response to question 2.2 above, the manufacturing or importation of medical devices is permitted only after a medical device permit licence has been issued, granting registration and market approval. Therefore, determining whether the company possesses or is required to obtain such permit licence is a crucial matter.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Please see our response to question 5.5 above.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

In general, when two or more parties are involved in the use of generative AI, they should consider several factors, including the internal allocation of risks related to contractual liabilities, tort liabilities and criminal liabilities, as well as agreements on the ownership of IP rights (if applicable) and data sharing or transfer.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

In Taiwan, the principal regulatory authorities overseeing AI and ML enforcement include the Executive Yuan and the National Science and Technology Council (NSTC). In February 2023, the Executive Yuan launched the Taiwan AI Action Plan 2.0 (2023–2026) to guide government policy. The NSTC is currently drafting the Fundamental Law on Artificial Intelligence, which aims to promote human-centric AI development while safeguarding citizens' rights and well-being. This law outlines principles such as sustainability, human autonomy, privacy protection, cybersecurity, transparency, fairness and accountability. Additionally, the Ministry of Digital Affairs will establish AI information security standards and risk management frameworks in alignment with international norms.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

As indicated in our response to question 8.1 above, there are currently no comprehensive regulations governing AI/ML; however, a draft of the Fundamental Law on Artificial Intelligence was provided in July 2024. The government has initiated several policies, including the Taiwan AI Action Plan (2018–2021) and its subsequent version (2023–2026), focusing on ethical principles, national policy, privacy protection and regulatory sandboxes.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

A letter from Taiwan's Intellectual Property Office (2018) states that AI is not recognised as a legal "person", meaning AI-generated works lack copyright protection.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

If any "personal data" is collected, used or processed in relation to training data or data licensing, the PDPA regulatory framework (including our responses to questions in sections 4 and 5 above) will apply. Specifically, for any "sensitive personal data", additional restrictions will be in place, such as the requirement for "informed consent" to be obtained in writing (as discussed in our response to question 4.3). We believe that PDPA compliance, as outlined, should be carefully considered in the context of data licensing.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Regulatory bodies overseeing AI and ML technologies are starting to distinguish between standard AI and generative AI using a risk-based framework, as detailed in the draft of the Artificial Intelligence Basic Law. This framework emphasises the necessity for the Ministry of Digital Affairs to refer to international standards, such as the EU AI Act, to create a risk classification system. Although specific regulations are still being developed, the legislative rationale reflects a commitment to ensuring the safety and stability of AI by categorising risks, including prohibiting certain AI practices.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

As noted in our response to question 8.2 above, the legal and regulatory landscape for generative AI technologies is evolving, primarily through the Fundamental Law on Artificial Intelligence, which is still in draft form and has not yet been legislated. This framework emphasises ethical principles, national policy, privacy protection, and the establishment of regulatory sandboxes and guidance mechanisms. While it outlines general principles, specific regulations are being developed by various departments for different sectors. Key issues include: copyright disputes, as current laws do not recognise AI as a copyright holder; privacy concerns, as detailed in our prior answers regarding privacy regulations; and discrimination and fairness, which are addressed by the Ministry of Science and Technology's guidelines established in September 2019.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

The protection of personal data in AI applications is primarily regulated by the PDPA. The PDPA requires non-public entities to establish specific purposes and legal grounds for collecting or processing personal data. The draft of the Basic Law on Artificial Intelligence highlights the importance of minimising unnecessary data collection and incorporating data protection measures into AI development. Additionally, the Ministry of Digital Development has released guidelines on privacy-enhancing technologies to effectively address these issues.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

The theories of liability related to adverse outcomes are primarily categorised as follows:

- Civil Liability: This includes breaches of contract, torts and product liability, and is governed by the Civil Code and the Consumer Protection Act.
- Criminal Liability: This pertains to injuries resulting from intentional acts or negligence, as well as the manufacturing or importation of goods without the necessary permits or approvals. Relevant legislation includes the Criminal Code, the Physicians Act, the Pharmaceutical Affairs Act and the Medical Devices Act.

- Administrative Liability: This involves the manufacturing or importation of goods without the required permits or approvals, specifically under the Medical Devices Act.

9.2 What cross-border considerations are there?

If any digital health-related services are provided to individuals in Taiwan from offshore entities, there may be questions regarding the necessity for those offshore entities to comply with Taiwan's regulatory requirements, particularly concerning licensing (e.g., prior approval, permits, or licences needed to operate a medical device company or engage in healthcare-related activities), as healthcare is a regulated industry in Taiwan. For further details on these regulatory requirements, please refer to our response to question 10.2.

From a contractual perspective, even if the governing law of the contract for the digital health-related service is a foreign law (i.e., non-Taiwanese law) and a foreign court is designated for dispute resolution, we cannot entirely dismiss the possibility that, in the event of a dispute where Taiwanese individuals file a suit in a Taiwanese court, such court may still review the case and determine that Taiwanese laws (such as the Taiwan Consumer Protection Act) apply to protect those individuals.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

To mitigate liability risks associated with the use of generative AI, product and solution providers should ensure that their offerings meet applicable technical and professional standards, as well as reasonably expected safety requirements, before bringing them to market, in accordance with Taiwan's Consumer Protection Act.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

The misuse of healthcare data in AI/ML models raises legal concerns under various regulations. According to the Hospital Personal Data Security Maintenance Implementation Guidelines, hospitals must promptly address incidents of data theft, leakage or alteration to protect individuals' rights. This includes taking measures to mitigate harm, investigating the cause, and notifying affected parties within 72 hours. Additionally, the PDPA stipulates that non-public entities violating data protection laws may face penalties, including bans on data collection, mandatory deletion of data and public disclosure of violations.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Regarding cloud-based services for digital health, the PDPA is applicable, as organisations utilising these services may collect data from individuals, which is then forwarded to a service provider for processing and use. Consequently, from a legal perspective in Taiwan, the primary concern with cloud-based services for digital health is compliance with the PDPA. Please refer to our responses to the questions in sections 4 and 5 above, particularly where personal data is classified as "sensitive personal data". In such cases, written informed consent is required. Additionally, there are exemptions from the informed consent requirement for use by non-government entities or academic institutions under specific circumstances.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

Healthcare is a regulated industry in Taiwan. For instance, operating a medical device company, as well as manufacturing and selling medical devices, necessitates obtaining prior approvals and permits in accordance with current regulations. Furthermore, under the Physicians Act, individuals cannot practice medicine as physicians without the required licence. In the context of telemedicine, physicians are prohibited from treating patients, issuing prescriptions or certifying diagnoses for patients they have not personally examined, except in specific circumstances such as remote areas or urgent situations (refer to our response to question 3.1 above for more details). Given such considerations, it is advisable for non-healthcare companies to thoroughly evaluate the licensing and regulatory requirements before entering the digital healthcare market in Taiwan.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

From a legal standpoint, it is advisable for venture capital and private equity firms to thoroughly assess whether the business model of the target digital healthcare venture aligns with Taiwan's regulatory framework during the due diligence phase. This includes a critical evaluation of compliance with licensing and regulatory requirements, as outlined in our response to question 10.2, as well as adherence to the PDPA, particularly if the personal data collected by the target company meets the definition of "sensitive personal data".

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Based on our observations, the current legal obstacles in Taiwan that may impede the development of digital health solutions include the following: (i) as noted in our response to question 3.1, physicians are generally prohibited from treating, prescribing medicine for, or certifying diagnoses for patients they have not personally examined, except in specific situations such as remote areas or urgent circumstances – consequently, the provision of telemedicine services by physicians is largely restricted under current Taiwanese law; and (ii) there are typically more stringent regulations governing the collection, use and processing of "sensitive personal data", which is often integral to the development of digital health solutions.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

In Taiwan, physician certification bodies, such as the Taiwan

Surgical Association, do not significantly influence the clinical adoption of digital health solutions. Adherence to existing regulatory requirements is paramount. For details on the licensing and regulatory requirements from a Taiwanese perspective, please refer to our response to question 10.2 above.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

To our knowledge, no private insurers specifically exclude patients who use digital health solutions from filing insurance claims for covered incidents, provided that no additional documentation is required unless stated in the insurance policy. Regarding government reimbursement, the NHIA announced a pilot plan in 2020 aimed at including virtual care for remote areas under NHI coverage. Under this pilot plan, patients receiving care from approved medical institutions offering virtual services may only need to pay registration fees, subject to certain exceptions outlined in relevant regulations.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

There is a lack of transparency concerning data privacy and protection, as many digital health solutions fail to adequately disclose their practices related to data collection, usage, storage and sharing, especially during AI model training, which may involve insufficiently anonymised data. The opacity of AI/ML algorithms complicates the understanding of their decision-making processes, potentially leading to accountability issues when errors arise. The legal framework governing liability and risk allocation remains ambiguous, particularly regarding the responsibilities of developers, healthcare providers and users. Regulatory compliance and market entry standards for digital health products are still evolving, with existing guidelines lacking comprehensive adjustments to effectively address these challenges.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

As indicated in our response to question 5.4, Taiwan's Constitutional Court ruled in August 2022 on the PDPA, mandating the amendment of relevant laws within three years. Consequently, the PDPA was revised in May 2023, and the preparatory office for the independent PDPC was established in December 2023. Looking ahead, it is essential to monitor the PDPC's development and any further amendments to related legislation. Notably, the PDPC has announced plans for additional revisions to the PDPA by December 2024, focusing on data breach notifications, the introduction of data protection officers and prioritising administrative inspections in high-risk sectors.

Tsung-Yuan Shen specialises in the fields of biomedical and food technology law, IP protection, unfair competition, construction/BOT and dispute resolution. His professional background spans biotechnology, law and economics.
Mr. Shen has represented many biotech-related companies in the fields of pharmaceuticals, medical instruments, chemicals, health food and GMO, and governmental research organisations in IPR matters and legal matters. He has also advised high-tech companies in the fields of electronics, optoelectronics, communications, precision industry and multinational construction companies on matters of IPR, high-tech laws and public construction disputes.
Clients served by Mr. Shen include Pfizer, Merck Sharp & Dohme, DuPont, TSMC, AU Optronics, Qualcomm, Molex, Lockheed Martin, and other leading companies or organisations.
Mr. Shen has also utilised his background in economics in cases involving the management or licensing of IP portfolios. In addition, he has acted on behalf of companies during governmental investigations of unfair competition and in administrative lawsuits with outstanding results.

Lee and Li, Attorneys-at-Law
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei 110055
Taiwan

Tel: +886 2 2763 8000 ext. 2539
Email: tsungyuanshen@leeandli.com
LinkedIn: www.linkedin.com/in/tsung-yuan-shen-沈宗原-02401019

Rachel Chen is a senior attorney in Lee and Li's Hsinchu Office. With backgrounds in both finance and law, her practice areas include corporate investment, corporate governance and compliance, securities law and labour law, with a special focus on M&A as well as commercial contract review and drafting.

Lee and Li, Attorneys-at-Law
No. 1, Gongye E. 2nd Rd.
East Dist., Hsinchu 300091
Taiwan

Tel: +886 3 579 9911 ext. 3206
Email: rachelchen@leeandli.com
LinkedIn: www.linkedin.com/in/rachel-chen-93018726a

Nita Ye is an attorney at Lee and Li, Attorneys-at-Law. Ms. Ye's practice focuses on arbitration, labour disputes, investment and personal data protection, regarding which she provides clients with consultation and professional advice.

Lee and Li, Attorneys-at-Law
No. 1, Gongye E. 2nd Rd.
East Dist., Hsinchu 300091
Taiwan

Tel: +886 3 579 9911 ext. 3269
Email: nitaye@leeandli.com
URL: www.leeandli.com/EN/Professions/901/529.htm

Lee and Li is now the oldest and largest law firm in Taiwan and is highly sought after by clients worldwide for its comprehensive and premium legal services. Our services are performed by a total of around 860 employees, including around 200 attorneys, as well as many patent attorneys, patent agents and trademark attorneys and over 100 professionals with backgrounds in technology and other fields. Many members of our team hold advanced degrees in law and IP rights from internationally renowned institutions. A number of our colleagues are also certified lawyers or patent agents in the United States and mainland China.
Lee and Li has established various practice groups based on our specialisations in banking and finance, capital markets, corporate matters and investment, trademarks and copyrights, patents and technology, and litigation and dispute resolution, as well as our Japan Practice Department. Practice groups put the formidable resources of a large firm and the highly customisable services of a boutique firm at our clients' disposal. We also have special task forces that corral experts from different departments and practice groups to tackle unusual challenges.
Our close rapport with prominent international law firms and business consultancies, accounting firms and financial institutions allows us to swiftly mobilise resources and expertise across disparate fields, and to devise optimal legal solutions for transnational matters. We collaborate with L&L-Leaven, Attorneys-at-Law in Shanghai and Lee and Li-Leaven IPR Agency Ltd. in Beijing to assist clients in the Greater China region with cross-strait legal matters and IP rights. This cross-strait platform saves our clients the effort of finding lawyers and agents in mainland China and prevents misunderstandings due to differences in Taiwanese and mainland Chinese legal systems and practices.
Lee and Li's services and expertise have earned high praise from clients both at home and abroad. In international surveys of law firms and IP firms, we are consistently rated as the best legal services provider in Taiwan.

www.leeandli.com

理律法律事務所
LEE AND LI
SINCE 1965 ATTORNEYS-AT-LAW

United Kingdom


Pieter Erasmus


Emma Drake


Tristan Sherliker


Mario Subramaniam

Bird & Bird

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

There is no specific definition of "digital health" in the United Kingdom (**UK**). The term generally refers to the use of technology (such as apps, programmes, software, etc.) in healthcare – either standalone or combined with other products such as therapeutics, diagnostics or medical devices.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

The key emerging digital health technologies in the UK include the following:

- Digitised health systems – in particular, the wholesale digitisation of patient data and prescription delivery in the UK National Health Service (**NHS**).
- mHealth – apps on mobile and connected wearable devices to monitor and improve health and wellbeing.
- Telemedicine – delivery of health data from mHealth apps to the patient's clinician, and the provision of remote support and care to patients, either through healthcare practitioners, allied service providers or AI. There is a trend towards the integration of telemedicine services with digitised health systems.
- Health data analytics – the digital collation, analysis and distribution (including on a commercial basis) of patient health data.
- Personalised medicine – using genomics to get a faster diagnosis of a condition and being given personalised treatments based on that diagnosis.
- Artificial intelligence (**AI**) and machine learning (**ML**) – these technologies are being used to enhance digital health more broadly and improve operational efficiencies.

1.3 What is the digital health market size for your jurisdiction?

Given the breadth of the market and underlying technology, there is not a specific estimate of the digital health market in the UK; however, certain sources suggest that the UK digital health market will reach approximately £15 billion by 2025, although this is likely to be an underestimation.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

Based on certain sources, examples of the more prominent digital health companies operating in the UK include:

- Cerner Corp.
- Teladoc Health.
- Cera.
- CMR Surgical.
- Veradigm (formerly Allscripts).
- Thriva.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Based on certain sources, examples of growing digital health companies operating in the UK include:

- Doccla.
- Huma.
- Snap40.
- Oviva.
- AccuRx.
- Medbelle.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The Medicines and Healthcare products Regulatory Agency (**MHRA**) regulates medical devices, including digital health technologies, ensuring they meet safety, quality and performance standards. NHS Digital is responsible for the national digital infrastructure and services, ensuring the secure and efficient use of data and technology in the NHS.

The National Institute for Health and Care Excellence (**NICE**) provides guidance and sets standards for health and social care practices, including the evaluation of digital health technologies.

With respect to the use of such digital health technologies in healthcare settings, the healthcare regulatory regimes in the four nations of the UK are regulated by the following regulatory authorities:

- England – Care Quality Commission.
- Scotland – Healthcare Improvement Scotland.

- Wales – Care Inspectorate Wales.
- Northern Ireland – The Regulation and Quality Improvement Authority.

The Information Commissioner's Office (**ICO**) regulates the use of personal data in accordance with the UK General Data Protection Regulation (**UK GDPR**) and the Data Protection Act 2018 (**DPA**).

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

In an increasingly multi-disciplinary area, the core healthcare regulatory schemes related to digital health in the UK are numerous. In addition to software as a medical device (**SaMD**) and AI as a medical device (**AIaMD**) regulation, these include data protection and privacy; the use of personal data in digital health is regulated primarily by the UK GDPR, the DPA and laws on confidentiality that vary between the different parts of the UK (England, Northern Ireland, Scotland and Wales). Further examples include cybersecurity, data compliance and governance.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

Key areas of enforcement include:

- **Data protection and privacy**: Ensuring compliance with the UK GDPR and the DPA. This includes safeguarding patient data and ensuring proper data handling practices.
- **Medical device regulation**: The MHRA oversees the safety, quality and performance of digital health technologies (including software) classified as medical devices.
- **Telemedicine and remote care**: Ensuring that telehealth services meet the required standards for safety and quality, including proper registration and compliance with healthcare regulations.
- **Clinical safety and effectiveness**: Ensuring that digital health solutions provide clinically safe and effective care, adhering to standards set by bodies such as NICE.

Emerging areas of enforcement include:

- **AI and ML**: As AI becomes more integrated into healthcare, there is increasing focus on ensuring these technologies are safe, effective and ethically used.
- **Cybersecurity**: With the rise of digital health technologies, protecting against cyber threats and ensuring the security of health data is becoming a critical area of enforcement.
- **Interoperability standards**: Ensuring that digital health systems can effectively communicate and share data across different platforms and healthcare providers (**HCPs**).
- **Digital therapeutics**: As digital therapeutics become more prevalent, there is a growing need to regulate these solutions to ensure they meet clinical standards and provide real therapeutic benefits.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

SaMD is primarily governed by the UK Medical Devices Regulations 2002, as amended (**MDR 2002**). The MHRA has issued guidance specifically dealing with SaMD, which assists with determining whether software is regulated under the MDR 2002. The MHRA has been working towards the reform of the general medical device regulatory framework in Great Britain (being England, Scotland and Wales). Post-market surveillance draft regulations were laid before Parliament on 21 October 2024 and are expected to come into force mid-2025. A consultation was further launched on 14 November 2024 regarding "Pre-market" regulations with the view that new draft regulations will be put before Parliament during 2025. This area of regulation remains in flux, so it should be monitored closely.

From a SaMD perspective, in 2022, the MHRA published a "roadmap" for its *Software and AI as a Medical Device Change Programme* published the previous year. The programme consists of work packages with problem statements, objectives and deliverables, one of which is "The Transparency for machine learning-enabled medical devices: guiding principles" (published in October 2021), which sets out guiding principles for good ML practice that were jointly established by the US Food and Drug Administration, Health Canada, and the MHRA.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

See response to question 2.4 above.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

See response to question 2.4 above.

The MHRA launched the *AI Airlock* in May 2024 (in collaboration with the Department of Health and Social Care, the NHS AI Lab and Team AB), which is the first regulatory sandbox for AIaMD. The pilot project will run until April 2025. The objective of this project is to identify regulatory challenges associated with AIaMD, to help manufacturers explore how to best collect evidence as support for the approval of their product, and to understand and mitigate any risks that are uncovered through the project. Additionally, and by way of further example, in January 2025 the MHRA launched a pilot real-world evidence Scientific Dialogue Programme, which is designed to help innovators refine their evidence-generation strategies while providing clear guidance on regulatory expectations. This programme aims to facilitate robust decision-making across the entire lifecycle of products, benefitting both regulatory and health technology assessment evaluations relevant to the UK.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation data plays a key role in the regulatory considerations for AI/ML-based digital health solutions. The MHRA requires robust clinical validation data to approve AI/ML-based medical devices. This data helps regulators assess the accuracy, reliability and clinical relevance of the AI/ML algorithms. Clinical validation data also supports ethical

and transparent use of AI/ML in healthcare. It helps in understanding the decision-making process of AI algorithms, and ensuring they are fair and unbiased.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Regulation in this area remains broadly aligned at the UK national level, subject to the nuance brought about by the Northern Ireland Protocol whereby the regulatory regimes differ between Great Britain and Northern Ireland. Therefore, while the primary regulatory framework is set at the national level, regional health authorities and NHS Trusts may have additional requirements or guidelines for the implementation and use of digital health technologies. These can include specific data-sharing agreements, local clinical governance standards and region-specific pilot programmes.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

As mentioned in the response to question 2.6, examples include the MHRA introducing the *AI Airlock* pilot scheme to test and refine the regulatory framework for AI-powered medical devices. This initiative allows for real-time performance monitoring and continuous validation of AI technologies. In addition, regulatory bodies such as the MHRA and NICE are developing dynamic guidance that can be updated as new evidence and technologies emerge. This ensures that regulations remain relevant and effective.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  - Determining whether any of the devices used qualify as medical devices.
  - Determining whether such activity requires registration as a regulated activity.
  - Data protection and patient confidentiality compliance – determining the roles of the parties involved, appropriate notice and consent practices; determining an appropriate method of handling patient records and sharing with primary care trusts; implementation of necessary security measures; and ensuring that algorithms are robust and unbiased.
  - Contractual issues between the various suppliers of services and devices.
  - If telemedicine is included, compliance with the local pharmacy and prescribing rules and regulations will be necessary.
  - Cybersecurity.
- **Robotics**
  - Liability allocation for poor outcomes – designer, manufacturer, HCP or even power supplier.
  - Compliance with Regulations: e.g. for waste electrical and electronic equipment (**WEEE**).
  - Compliance with MDR 2002.
- **Wearables**
  - Determining whether any of the devices used qualify as medical devices.
  - Data protection compliance – assessing whether health data is collected by publishers or whether this is strictly limited to the local device, ensuring a lawful basis for processing (likely to be consent), ensuring privacy by design, explaining data processing to individuals, implementation of necessary security measures and retention of necessary information.
  - Contractual issues between the various suppliers of services and devices.
- **Virtual Assistants (e.g. Alexa)**
  Similar issues as for Telehealth.
- **Mobile Apps**
  Similar issues as for Telehealth.
- **Software as a Medical Device**
  - Compliance with MDR 2002.
  - Data Protection compliance. Similar issues as for Telehealth.
- **Clinical Decision Support Software**
  Similar issues as for Telehealth.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  Similar issues as for Telehealth.
- **IoT (Internet of Things) and Connected Devices**
  Similar issues as for Telehealth.
- **3D Printing/Bioprinting**
  - Liability allocation for poor outcomes – designer, manufacturer and/or HCP.
  - Contractual issues between the various suppliers and customers of services/products.
  - IP ownership issues.
- **Digital Therapeutics**
  Similar issues as for Telehealth.
- **Digital Diagnostics**
  Similar issues as for Telehealth.
- **Electronic Medical Record Management Solutions**
  - Data protection and patient confidentiality compliance – determining the roles of the parties involved, appropriate notice and consent practices; determining an appropriate method of handling patient records and sharing with primary care trusts; implementation of necessary security measures; and ensuring compliance with data retention rules.
  - Cybersecurity.
  - Contractual issues between the various suppliers of services.
- **Big Data Analytics**
  - Data protection and patient confidentiality compliance – determining the roles of the parties involved, appropriate notice and consent practices; determining an appropriate method of handling patient records and sharing with primary care trusts; implementation of necessary security measures; and ensuring that algorithms are robust and unbiased.
  - Liability allocation for poor outcomes – algorithm designer and/or HCP.
  - Contractual issues between the various suppliers of services.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Data protection and patient confidentiality compliance – determining the roles of the parties involved, difficulties with amending records, issues with "right to be

forgotten" and erasure of data, appropriate notice and consent practices; determining an appropriate method of handling patient records and sharing with primary care trusts; and implementation of necessary security measures.

- **Natural Language Processing**
  To the extent applicable, similar issues as for Telehealth and Big Data Analytics.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Data protection and especially the lawful transmission, storing, processing and use of data – and ensuring adequate consent to such use has been obtained. International data transfers remain a compliance hot topic.

The digital platform provider must ensure, to the extent it is responsible: (i) that advice and services provided on the platform are fit for purpose as failure to process information resulting in personal injury may result in liability; and (ii) where the activity requires registration as a regulated activity, such activity is registered and complies with relevant regulations.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

- The UK GDPR and DPA are the primary laws to consider in relation to data use in the UK. Patient confidentiality is separately regulated as a matter of common law, and is also relevant to the legality of processing personal data.
- Key issues include determining whether relevant data is personal data or has been sufficiently anonymised. Anonymisation is recognised as difficult to achieve in practice, and may reduce the utility of the relevant dataset. Simply removing identifiers may result in pseudonymous data, which is still caught by the UK GDPR.
- Also important is confirming the roles of the parties involved in the processing – which parties are controllers or processors – and putting appropriate contracts in place.
- Identifying whether data is *concerning health* (and therefore subject to more stringent rules, as are other categories of "special-category" data such as personal data on sex life or religion), *versus* less sensitive data that might, for instance, be collected for wellness purposes is usually a key consideration for technologies (e.g. step counts, sporting performance, etc.).
- An important requirement is identifying the appropriate legal basis for processing data and obtaining any necessary consent.
- Health data uses almost always require the carrying out of a Data Protection Impact Assessment (**DPIA**), and ensuring that appropriate risk mitigations are put in place, including measures to ensure data minimisation, privacy by design, data retention limits and appropriate information security measures.
- As mentioned above, ensuring that any overlapping requirements related to rules on patient confidentiality are met is also vital.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

This is not applicable, except as relates to the NHS – see question 4.3 below.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

There is a significant distinction between the use of data within *versus* outside the NHS; the impact of "soft law", such as restrictions deriving from NHS policy and "Directions" issued by the UK Secretary of State, will be more acutely felt when working with NHS-originating data, compared to data in (or sourced from) private or consumer settings.

Even in public sector contexts, the rules differ between different parts of the UK. An important example is the "National Data Opt-out", a scheme allowing NHS patients to easily opt out from certain secondary uses of their personal data in England. This does not apply to patient data from Northern Ireland, Scotland or Wales.

4.4 How do the regulations define the scope of personal health data use?

The GDPR/DPA generally prohibit the use of health-related personal data without prior, explicit consent, but list exemptions from that restriction – e.g. use of personal data to provide healthcare (by or under the responsibility of a person bound by a duty of confidentiality) is permitted. Similarly, they allow non-consensual scientific research in the public interest (provided that such research does not entail the taking of decisions affecting the relevant individual(s), unless the project has ethical committee approval).

However, as noted in the response to question 4.7 below, there are overlapping restrictions under contract, soft law and confidentiality/misuse of private information (**MoPI**) rules, which may affect the need to obtain consent.

Although this consent does not have to meet the same standard as explicit consent under the UK GDPR, care should be taken (and specialist advice obtained) to ensure that, where relying on UK GDPR/DPA grounds for processing personal data, these restrictions do not apply to the use of personal data.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

Digital health companies will often find themselves subject to heavy requirements imposed by NHS customers. Organisations not dealing with the NHS will often have greater freedom to operate.

More generally, a key consideration for the design and negotiation of contracts is whether, for UK GDPR purposes, the different parties are "processors" or "controllers" of the data – and in the latter case, whether two or more parties are "joint" or "independent" controllers. That classification will dictate the UK GDPR-imposed terms that must be included in the contract, and also inform each party's compliance strategy

and required risk protections (indemnities, warranties, due diligence and insurance).

If personal data is travelling internationally, then the UK GDPR will often require that additional contractual terms (typically based on a pre-approved set of "standard"/"model" contractual clauses) must be put in place between the data's exporter(s) and importer(s), and onward transferees.

By contrast, UK data protection laws generally have little impact on contracts with individuals; data protection-related matters should be dealt with outside of those contracts (e.g. through dedicated privacy notices, and stand-alone consent requests).

The legality of planned and future uses of personal data will be conditional on ensuring that notices, consents, contracts and/or lawful exemptions cover all anticipated uses – or expose an organisation to significant investigations and civil and/or criminal liability. In parallel, failure to secure appropriate IP rights from rights holders can expose the organisation to a risk of being sued by that organisation, and/or additional criminal liability under the DPA (if the data is personal data).

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The UK GDPR requires controllers to ensure that data is accurate, up to date and processed fairly. It also requires controllers to notify individuals about how their data may be processed, including the logic used in automated decisions made about them. It further requires controllers to ensure that any individuals are not subject to substantial and entirely automated decision-making without explicit consent, contractual necessity or legal obligation.

The ICO has released detailed guidance on the use of AI, including guidance on addressing risks associated with automation such as bias, automated decision-making and risks of discrimination. The ICO is also carrying out active investigations into the use of AI tools in certain sectors, such as recruitment, and the potential for bias in the use of these tools.

The NHS in England has an active AI Ethics Initiative, run by the NHS AI Lab, which has various projects considering bias and risk in AI datasets.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The use of personal data in digital health is regulated primarily by the UK GDPR, the DPA and laws on confidentiality that vary between the different parts of the UK.

In addition, a substantial body of "soft law" tends to be imposed by other stakeholders' policies and contracts.

Additional legislation can apply for specific data uses, e.g. the Privacy and Electronic Communication Regulations restricts non-consensual access to and storage of data on Internet-connected devices. Medical device or clinical trial laws further limit the use of personal data.

- The UK GDPR imposes significant restrictions on the use of health data without providing notice of that use and demonstrating an appropriate legal basis for processing the special-category data. Often, explicit consents from individuals will be necessary. This must be specific, informed and freely given.
- Operators in England and Wales (in particular) must also deal with more restrictive requirements of "common law", particularly surrounding patient confidentiality and MoPI. Without consent (which for confidentiality/MoPI purposes could be implied or explicit), or a clear statutory permission, only uses of patient personal data that are necessary for patient care or in the public interest, are permitted under English and Welsh law on confidentiality and MoPI.
- The UK GDPR also imposes additional requirements, including to keep data secure, maintain its availability and accuracy, report data incidents, appoint a Data Protection Officer and/or a "Representative", conduct DPIAs, and generally ensure that usage of personal data is fair, lawful and does not involve excessive amounts of data.
- The UK GDPR grants individuals substantial personal data rights, e.g. to access or delete their data. The DPA adds certain additional rules, including criminal offences for re-identifying personal data, or selling it after it has been improperly obtained.
- Data protection law also includes laws that regulate the use of automated means to take significant decisions that have legal or "substantially similar" effects on an individual. This will need to be borne in mind as software (e.g. AI) becomes increasingly capable of replacing (rather than merely supporting) human decision-making in healthcare settings.
- Organisations should be aware that the UK Government has recently laid draft legislation to review UK data protection law, including provisions that will alter requirements on accountability, further processing and definitions of consent. A stated aim of the Government is the lessening of the burden on organisations carrying out research. A close eye should be kept on these developments throughout 2025.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

As with general use of such data, the key laws are the UK GDPR, the DPA and patient confidentiality derived from common law. The sharing of personal data means that confidentiality and privacy concerns will often be more acute than simply using data within a single organisation. For example, in England and Wales, even greater attention needs to be paid to the existence of a care need, consent, statutory permission and/or a public interest justification for the proposed data sharing if it involves patient data processed for the purposes of providing care. To complicate matters, that legal basis might be different for the different parties, and thus subject to differing restrictions and conditions.

Sharing personal data also introduces potentially significant counterparty risk: both parties to a data-sharing arrangement might face legal risk even if just one of the parties misuses the data. Due diligence, contracting and clear compliance arrangements are therefore important.

Key aspects of the data sharing may need to be explained to individuals, in accordance with the GDPR's transparency obligations. Finally, sharing personal data across borders – even just by providing remote access to it – raises GDPR data transfer compliance issues.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

This is not applicable.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

As with data use, key legal variations tend to be driven by differences in the purpose of data sharing, not the nature of the entities involved. That said, certain public sector entities (particularly, those within the NHS) might have specific legal powers – or restrictions – regarding data sharing and the performance of their public duties. This could also vary depending on their location within the UK.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

There are numerous NHS initiatives for the sharing of healthcare data. For example:

- NHS England has a role as statutory custodian for health and social care data for England, taking a role in creating data collections, data sets and allowing specific authorised access to third parties.
- The Health Research Authority's (**HRA**) Confidentiality Advisory Group provides independent expert advice to the MHRA and the Secretary of State for Health on whether applications to access confidential patient or service user information without consent should or should not be approved.
- The Clinical Practice Research Datalink, a real-world research service supporting retrospective and prospective public health and clinical studies collecting data from a network of services.
- The NHS Federated Data Platform.
- The NHS Data Security and Protection Toolkit, for those who have access to NHS data.
- NHS pilot programmes, including Improving Elective Care Coordination for Patients and Dynamic Discharges.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

Where a choice has been taken to consider federated learning data sharing for the purposes of protecting patient confidentiality and personal data, it is key to ensure that appropriate protections are offered by the tools, software and contracts establishing this framework to ensure these purposes are fulfilled – there must be appropriate security, use of sufficient anonymisation tools and restrictions on sharing to ensure the intended benefits are achieved.

The preceding responses, in particular to questions 4.1, 4.5, 5.1 and 5.3, have covered the key regulatory requirements applicable to the sharing of personal data in a digital health context.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Patent protection is still available for digital health technologies that satisfy the requirements for the grant of a patent in accordance with the UK Patents Act 1977 (**PA**).

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

Copyright protection is still available for digital health technologies that satisfy the requirements of the UK Copyright, Designs and Patents Act 1988 (**CDPA**); see also response to question 6.5 with respect to protection of software.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Digital health technologies that satisfy the requirements of a trade secret and/or confidential information will continue to be protected as a trade secret (protection under statute) and by the common law of confidence, which protects information that:

- has a quality of confidence;
- is disclosed under an express or implied obligation of confidence; and
- is used or further disclosed in an unauthorised manner.

The UK Trade Secrets (Enforcement, etc.) Regulations 2018 also prevent acquisition, use or disclosure of trade secrets where this would constitute a breach of confidence in confidential information.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

IP rights in technology developed in academic institutions usually vests in the academic institution, as a result of employment or other contractual arrangements. Absent contractual arrangements, the ownership of IP rights can be more complicated. Academic institutions typically seek to commercialise technologies by way of licensing arrangements (for example, to existing businesses, commercial research partners, or via the creation of a spin-out company dedicated to commercialising the technology).

There are no specific laws governing academic technology transfer. In very rare cases, under the PA, the publication of a patent or disclosure of related information may be restricted if it might be prejudicial to national security or public safety, with resulting effects on technology transfer.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

A software-implemented invention is only patentable in the UK to the extent that it meets the requirements in the PA. While

inventions implemented in software are patentable, software *per se* is not. The requirements are stringent and difficult to meet. Generally, software *per se* will be protected as a literary work under the CDPA (although the protection applies to the particular expression of ideas and principles that underly an algorithm and not to the ideas and principles themselves) (see response to question 6.2).

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

No. Following the decision of the UK Supreme Court in *Stephen L Thaler v The Comptroller- General of Patents, Designs And Trade Marks* [2023] UKSC 49, an AI device cannot be named as an inventor of a patent in the UK under current legislation. In October 2021, the UK Intellectual Property Office (**UKIPO**) (the executive Government Department) issued a public consultation on whether the PA should be amended to permit an AI system to be named as an inventor or whether the definition of inventor should be expanded to include humans responsible for an AI system that devises inventions. The outcome of the consultation was that AI was not considered advanced enough to invent without human intervention and that there was therefore no planned change to UK patent law for AI-devised inventions.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

Government funding for innovation is available in the UK. This funding is classed as a subsidy and therefore must be consistent with the UK subsidy control regime, WTO rules, the EU–UK Trade and Cooperation agreement and other bilateral UK Free Trade agreements.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

The following guidelines and IP decisions are particularly relevant with regard to the AI and software aspects of digital health innovations. The UKIPO and the European Patent Office (**EPO**) have established guidelines on the patentability of AI-related innovations. The various responses to the UK Government's 2024 consultation into the general regulatory landscape regarding AI and ML also provide useful guidance on the rationales that may inform future decisions from regulators.

Patent case law emphasise the importance of demonstrating that the software component of the digital health product has a technical effect, beyond the mere implementation of a mathematical method on a computer. For instance, the EPO's decision in G 1/19 (Simulations) and the UK court's decision in *Aerotel v Telco and Macrossan's Application* [2006] EWCA Civ 1371 clarified the approach to computer-implemented inventions, which can be relevant to AI in digital health.

Copyright case law in relation to software programming highlight that ideas and principles (such as operational methods, mathematical concepts and procedures) in software are not protected by copyright (*SAS Institute v World Programming*, Case C-406/10; *Nova Productions Ltd v Mazooma Games Ltd* [2007] EWCA Civ 219). Therefore, a competitor can develop a competing software product that does effectively the same thing or operates according to the same principles, as long as the competitor did not copy the code or other pivotal structural design aspects of the original product.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

It is often suggested that joint ownership of IP/improvements is the fairest way of approaching collaborations. The downside of this blanket approach is that treatment of jointly owned IP varies from jurisdiction to jurisdiction and also by IP right. The consequence is that the joint owner might be unclear as to their rights to exploit such IP if not expressly set out in the collaboration agreements.

Alternative ways of approaching collaborative improvements would be for ownership to follow the ownership of background on which the improvement is made or to assign such collaborative improvements in accordance with predetermined fields of use. In all instances, it would be prudent to include relevant licences to background and royalty provisions, as applicable.

More broadly, parties should consider including robust provisions relating to confidentiality to protect sensitive information shared during the collaboration, as well as clearly defining performance obligations and milestones to track progress and ensure accountability. The parties should be prepared to adapt to changing circumstances and new information and rightsholders, as flexibility is crucial for navigating the dynamic nature of collaborative projects in digital health technologies.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

As with any agreement, the allocation of rights and obligations should be set out clearly, especially in relation to liability. It is likely that the parties will have responsibilities related to their respective expertise, and these should be specified, as well as responsibility for data protection compliance.

Public sector HCPs often have very strict rules (even to the extent of bureaucracy) which can mean that negotiation of IP rights, for example, can be difficult to deviate from standard form agreements. The parties should therefore ensure that the agreement includes provisions for compliance with relevant healthcare regulations and standards.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Agreements should carefully outline the terms of the data sharing, specifying who has control over the data and how decisions regarding data usage will be made. Issues related to data access, modification and deletion should also be addressed. Rules around ownership of the model itself should also be established.

As the raw data is not shared, parties should agree on common data formats and standards to ensure interoperability. Ideally, the data sharing agreement should facilitate

seamless integration of data from different sources, potentially by using established healthcare interoperability standards such as Fast Healthcare Interoperability Resources.

Agreements should also comply with data protection laws, for example, setting out rules around data minimisation and purpose limitation.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Parties should ensure clear data ownership agreements that respect the interests and expectations of both parties, as well as data subjects and stakeholders involved.

The quality and availability of data is another consideration. It may be difficult to obtain large amounts of high-quality data to train the AI model due to the sensitive and confidential nature of most healthcare data. Biased, inaccurate or unrepresentative data in datasets could lead to bias or inaccuracies in the results.

Navigating rules around patient privacy and data protection will also be an issue, along with rules and regulations governing generative AI itself, which are rapidly evolving from country to country.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

There is currently no AI-dedicated regulator in the UK. Regulators have been encouraged by the Government to develop approaches specific to their own domains, and the wider approach to legislation and development is under development. See response to question 8.2 below for information about important programmes of relevance to AI/ML in healthcare.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

For now, unlike the EU, there is currently no specific regulatory regime in relation to AI/ML in the UK, although the Government is developing an AI Opportunities Action Plan over the course of 2025. At the moment, there are cross-sector guiding principles published by the UK Government that are implemented by various regulatory authorities using their existing powers and under existing regimes. However, the landscape is developing. In particular:

- The Government Department for Science, Innovation and Technology has a special division, the AI Safety Institute – a state-backed organisation to conduct research and safety assessments for AI in the UK.
- In early 2024, a Government consultation concluded into the general regulatory landscape under AI and ML topics was conducted. The consultation involved communication with, and consultation responses from, many interested regulators including the MHRA, ICO and Office for Statistics Regulation (the body governing official statistics in the UK). The regulator responses to the Government consultation, and the consultation itself, are useful resources for understanding the direction of movement, albeit that the incumbent Government has changed in the UK since that consultation took place and, to the extent that regulation is enacted pursuant to Government policy, the policy objectives may differ (as to which, see below).
- The MHRA in particular has been active in developing its regulatory posture and has conducted consultation and development activities since at least 2021.
- In December 2024, a Government consultation and call for views began in the field of copyright and AI. The consultation will run until at least February 2025.
- The Government has stated its policy goals in relation to AI generally, and the overlap between AI and IP specifically, to be broadly in favour of promoting the development and adoption of AI technologies in the UK.
- It is therefore likely that the regulatory response to AI will develop significantly throughout the course of 2025.

Some regulatory programmes with specific relevance to digital health include:

- **Personal Data**: The ICO lists AI as a "priority area" due to the potential effects on individuals. The ICO operates a regulatory "Sandbox" programme, which is a free service designed to give access to regulators themselves, for businesses in need of specific guidance. The ICO lists digital healthcare companies as examples of beneficiaries of this programme.
- **SaMD**: The MHRA operates a dedicated Software Group for the regulation of SaMD *per se*. In October 2022, the agency published a Roadmap for the regulation of AIaMD. The Roadmap indicated a blend of recommended legislative, regulatory and best-practice guidelines in that context. The recommendations ranged from passing new laws, to changing the use of nomenclature and increased monitoring and surveillance of SaMD in use.
- **Health Data Governance**: NHS Digital and the HRA oversee the use of health data in AI/ML applications. They regulate the use of data in healthcare AI in respect of compliance with data protection laws and ethical standards, particularly in research contexts.
- **AI in Clinical Trials and Research**: For AI/ML technologies used in clinical trials, the HRA and MHRA provide guidance on ethical considerations, data management and regulatory compliance. This includes ensuring that AI systems used in research are transparent, explainable and subject to rigorous evaluation.
- **Ethical Standards and Best Practices**: NICE has, in 2024, published an AI Code of Ethics, covering seven topics (plus sub-topics) for the adoption of AI in clinical and research settings. The principles touch on broad matters including integrity, transparency and accountability, as well as addressing specific concerns such as bias mitigation, and the use of quality checks and regular assessments.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Under English law, algorithms are potentially protectable by copyright as original literary works, although the protection

applies to the particular expression of ideas and principles that underly an algorithm and not to the ideas and principles themselves.

Where an algorithm is written by a human, the author of that work is the person who creates it (Section 9(1) CDPA). This is taken to be the person responsible for the protectable elements of the work, being those elements which make the work "original" (i.e. those parts that are the "author's own intellectual creation").

First ownership of a work and the duration of the protection available are defined with reference to the author. However, where an algorithm is written using ML without active human involvement, it may not be possible to identify a human who can be said to have created the work, i.e. there is no human author such that the work qualifies as "computer generated" under Section 178 CDPA. In these circumstances, Section 9(3) CDPA deems that the author of the work is the "person by whom the arrangements necessary for the creation of the work are undertaken". This can potentially be one or more natural or legal persons. Under Section 12(7), the duration of protection of a computer-generated work is 50 years from the end of the calendar year in which it is created.

While the test set out in Section 9(3) CDPA determines the identity of the author of a computer-generated work, it is not currently clear as a matter of English law whether such work will qualify as copyright work. Under Section 1(1) CDPA, copyright only subsists in original literary works, which requires an intellectual creation by the author which reflects an expression of their personality. It is questionable whether an algorithm developed by ML without human involvement could be said to be an intellectual creation reflecting the personality of the person making the arrangements necessary for its creation.

As a result, such an algorithm may not qualify for copyright protection under English law. An alternative view is that Section 9(3) CDPA in fact creates its own *sui generis* right for computer-generated works which is not subject to the usual requirement for originality. These issues have not thus far been addressed by the English courts and claims to copyright (or an absence of rights) in algorithms developed by ML without human intervention must therefore be treated with caution.

In October 2021, the UKIPO issued a public consultation seeking views on possible reforms to the protection of computer-generated works in the UK. The options under consideration included retaining the existing position under Section 9(3) CDPA, removing protection for computer-generated works or replacing Section 9(3) with a new and narrower form of protection with a limited duration, e.g. five years from creation. The UKIPO published its response to the consultation on 28 June 2022. It concluded that AI was still in its early stages, and it was not possible to undertake a proper evaluation of any changes to the law, which may have unintended consequences. The Government therefore proposed to make no changes to the current law, while keeping a decision of whether to amend, replace or remove protection under Section 9(3) under review.

Note that over the course of 2025, the UK Government is expected to continue to develop and set out its approach on AI regulation and will act to ensure the UK has a competitive copyright regime that supports the UK's AI sector. The Government has cited AI technology as a major part of its policy focus.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Many ML projects often involve collaboration between a party with expertise in deploying ML and another party with access to the data required to train a ML system to solve a particular problem. Common commercial issues that arise in this context include the rights each party obtains in the resulting system, e.g. can the resulting system be resold to others or adapted for purposes that go beyond those originally envisaged?

Similar considerations apply to the future use and disclosure of the training data itself, e.g. is the recipient allowed to retain the data after the project is complete and can it be re-used for other purposes (either in its original form or in some aggregated/derived form) and/or shared with third parties (and if so, under what terms)? Where the data is provided on a long-term basis with a defined scope of use, the licensor may wish to include audit rights to ensure the data continues to be used and disclosed in compliance with the terms of the licence.

Data licences will need to address potential liabilities arising from use of the licensed data. These will include any harm arising from defects in the licensed data, e.g. systematic inaccuracies in training could give rise to models that do not perform as required. A licensor will generally try to disclaim liability for errors or inaccuracies in a dataset. Liabilities could also arise through infringement of third-party rights in the data. These could include infringement of IP rights and other related rights, e.g. infringement of copyright in scientific publications or breach of an obligation of confidence owed by the licensor to a third party with respect to a particular dataset. In addition to conducting pre-contract due diligence on the legal rights affecting datasets, licensees will also often seek warranties and indemnities in the licence agreement to reduce their exposure to these risks.

Issues regarding use of training data commonly arise in the context of AI service agreements. An AI service provider will commonly wish to re-use data received from a customer during the course of providing the service to further improve the AI system that is used to provide the service, or potentially to develop new AI models for use in a different context.

Customers may resist contractual terms that permit this re-use of their data for these purposes, considering it to be a net value transfer from them to the service provider. Provisions relating to the use of derived data and meta-data, anonymisation and data retention post-termination may all be affected by this issue.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

At present, UK regulatory bodies have not established distinct regulatory frameworks specifically differentiating between standard AI and generative AI technologies. However, they are aware of the unique challenges and considerations that generative AI presents. For instance, the MHRA is working with a developer of a generative AI tool that helps users write documents or analyse data. Additionally, the Digital Regulation Cooperation Forum – formed of the ICO, Ofcom, Competition and Markets Authority (**CMA**) and Financial Conduct Authority – undertook joint consumer research on generative AI; the joint report found that consumers tend to assume regulation is in place if using generative AI in certain settings (financial services in particular) and expect organisations deploying generative AI tools to be accountable if things go wrong; as such, warnings and messaging can increase consumers' sense of personal responsibility.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

IP: In the field of IP, the dominant conversation concerns the use of copyright-protected works for the training of ML models, and the effect of the use of ML models on IP rights ownership in their outputs. The UK Government's *AI Opportunities Action Plan* (2025) highlights that it will act to ensure there is a competitive copyright regime that supports the UK's AI sector, and states that it may take forward the recommendation of establishing a copyright cleared training data set that can be licensed internationally at scale.

Misinformation, Deepfakes and Defamation: The UK Government's ongoing open consultation on copyright and AI includes assessing whether the current legal framework is sufficient to provide individuals with control over use of their likeness and whether further intervention is required. The ICO is also currently reviewing the application of UK data protection rules in this area and will issue guidance in due course.

Bias and Discrimination: Fairness is one of the UK Government's guiding AI principles and is therefore a key aspect implemented by regulatory authorities such as the ICO and CMA and NICE (as referred to above). Additionally, in 2023–2024, a UK Government scheme offered £400,000 in investment to fund innovative solutions to tackle bias and discrimination in AI systems. One of the winners of the scheme was King's College London, who will design a solution to address bias and discrimination in healthcare, in particular in early warning systems used to predict cardiac arrest in hospital wards.

Data Privacy and Confidentiality: This continues to raise issues with respect to: the use of personal data and training materials; the potential applications of synthetic data; and security issues arising from the risk of AI-powered malware.

Accountability and Liability: This will be a significantly developing issue. Questions of responsibility for actions attributable to AI are not clear under the current law. The regulatory response is being developed, and accountability is one of the UK Government's guiding AI principles and is therefore a key consideration for regulatory authorities.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

These are difficult issues under the UK law and are currently before the courts in at least one major dispute. It is likely that the first half of 2025 will begin to bring clarity to the assessment of these questions, at least from a jurisdictional standpoint. It is also highly likely that some legislative or policy developments will emerge from the open consultation on copyright and AI that is currently underway.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Liability for adverse outcomes in digital health is governed both by the law of contract (where services are delivered in accordance with a contract) and by the common law of tort/negligence where, whether or not a contract is in place, a duty of care exists between parties, and a breach of that duty (by falling below the reasonable standard expected in carrying out that duty) causes loss (including personal injury).

Additionally, the UK Consumer Protection Act 1987 sets out a strict liability regime for consumer products, including medical devices. In summary, under such claims a claimant does not need to show any fault on the part of the defendant. Instead, a claimant needs to demonstrate: (i) the presence of a defect in a product according to an objective standard of safety as reasonably expected by the public; and (ii) a causal link between that defect and the loss suffered.

Finally, the UK GDPR might create joint and several liability between partnering organisations if non-compliance led to an adverse outcome – for example, basing clinical decisions on inaccurately-recorded patient data or a biased algorithm.

9.2 What cross-border considerations are there?

Previously, under EU law (the Rome Regulations), generally, UK national (English and Welsh, Scots or Northern Irish) laws have applied to non-contractual (e.g. personal injury) and contractual claims based on digital health delivery to consumers/patients in the UK, whatever the country of origin of the provider. In accordance with retained EU law, the situation is not expected to change significantly in the short term.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Developers of generative AI products bear a duty towards the end-users, especially when the AI's decision-making mechanisms are unclear or complex. However, software developers may counter this by stating that generative AI-based healthcare solutions are designed to work in conjunction with HCPs who can overrule them if they propose a potentially harmful path, thereby shifting responsibility to the HCPs.

The British Medical Association's principles for the application of AI in healthcare (2024) provides some best practices to follow, such as ensuring HCP staff and patient involvement throughout the development and implementation process, ensuring HCP staff are initially and continuously trained on new technologies, and allowing HCPs to challenge decisions made by AI.

In the absence of legislation clearly governing liability of parties, it is essential that commercial contracts spell out which party is liable for errors when using generative AI in digital health solutions. Indemnification clauses could limit the liability of HCPs and AI algorithm creators. Alternatively, a special adjudication system could be considered. This would establish a separate legal pathway for addressing claims related to generative AI usage in healthcare, particularly for those claims that are challenging to resolve under current liability structures.

Insurance could serve as a safeguard against the financial risk linked with the application of generative AI by compensating for any potential damages and promoting responsible AI use among HCPs.

When building new generative AI tools, HCPs should insist that developers' models follow the MHRA's 10 guiding principles in relation to good ML practice for medical device development.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

The general principles briefly set out in the response to question 9.1 above apply. There may also be breach of patient confidentiality if patient data is used without appropriate anonymisation and without consent or other lawful exemption to consent.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Key issues include: (i) data security; (ii) commercial re-use of the data by the Cloud-based service provider; and (iii) whether data will leave the UK.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

It is a complicated and heavily regulated area, with regulations varying, in some instances, within the UK. There is no single, broad-brush approach and given the rapid development of digital health technologies, monitoring regulatory changes will be essential.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

When considering a target:

- Ensure that procedures are in place for compliance with relevant areas, especially data protection, patient confidentiality, and the variety of medical device regulations and guidance.
- Consider IP ownership and protection – do they own all necessary IP and have steps been taken to secure protection for all material IP, for instance including trade secrets?
- Competitive landscape – what other competing digital health technologies are in the market and what are their competitive advantages, e.g. advanced relationship with NHS, etc.?
- Do they have good supply and service contracts in place, and secure sources of hardware, software and labour?

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

Generally, the use of digital health solutions in the UK is well established. The COVID-19 pandemic has increased the prevalence of digital health solutions.

However, regarding the delivery of telemedicine services specifically, there remains some legal uncertainty because the UK healthcare regulatory environment is not yet fully updated to deal with the issues arising from the delivery of telemedicine services. However, programmes like the Government's *Life Sciences Vision* and the MHRA's plans for reform to medical device regulation indicate that the regulatory environment is undergoing significant change to address these challenges.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

While not a clinician certification body *per se*, in the UK, the Association of British HealthTech Industries plays a key role in representing the industry to stakeholders, such as the Government, NHS and regulators.

There is continued need for leadership by the UK Government and its relevant ministries, for instance by ensuring that standardised and easily accessible criteria, such as the NICE Evidence standards framework for digital health technologies, are adopted in a risk-based manner.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

This would depend on the digital health solution and in which country in the UK it was deployed. In England, while there may not yet be specific publicly funded provision of general health apps *per se* direct to patients, the provision of, for example, telemedicine may, under certain circumstances, be funded via the NHS. The recent launch of the NICE Office for Digital Health, which will work with strategic partners to improve digital health approval pathways and reimbursement policy, may see future development of funding arrangements for digital health solutions.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

There may be various gaps depending on the complexity of the digital health solution in question, but potential due diligence gaps may include matters relating to data provenance, quality and integrity, regulatory compliance (from a data protection and medical device perspective, among others), interoperability issues, relationships with the NHS and HCPs, ethical considerations, etc.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

A key trend to watch in 2025 is the increased use of genomic data and the resulting growth of precision diagnostics. As part of the Genome UK: 2022 to 2025 implementation plan, the UK Government is investing a total of £178 million for the research and implementation of genomic medicine. While the regulatory and data concerns highlighted above are sure to apply as genomic data is harnessed at scale, other concerns may develop as the regulatory landscape struggles to cope with such rapid developments in genomic technologies.

We can expect to see further disruption to the medical device and life science sectors, as the use of smartphones

and social media continue to transform the way that people manage their health. The practice of medicine has already been transformed by software and we expect this trend to continue, whilst interactions between patients and providers are fundamentally altered and boundaries blurred. Some of the key UK regulatory frameworks applicable to digital health products are also going to be subject to change from 2025.

Acknowledgments

The authors would like to thank David Pemberton and Quinn Liang for their invaluable contributions in the preparation of this chapter.

Pieter Erasmus is a senior associate in the IP Group in London, with a focus on regulatory and commercial matters primarily in the life sciences and healthcare sectors.
Having a keen interest in all things life sciences and healthcare, he specialises primarily in providing regulatory and commercial advice in relation to a broad range of matters in these sectors. His experience includes advising on the regulation of pharmaceuticals, medical devices, general healthcare services, clinical trials, marketing and advertising of health products, borderline products, food and beverages (including food supplements and novel foods), cosmetic products and legislative drafting in the healthcare context. A key focus area is advising on all aspects relating to digital health, including software as medical device, the impact of AI and telemedicine.

Bird & Bird
12 New Fetter Ln
City of London, London EC4A 1JP
United Kingdom

Tel: +44 207 905 6217
Email: pieter.erasmus@twobirds.com
LinkedIn: www.linkedin.com/in/pieter-miguel-erasmus

Emma Drake is a partner working on data and online safety compliance from the London office. She works with a wide variety of organisations, particularly in the media, sports and life sciences sectors. She also advises extensively on children's and employee privacy matters. Her work covers all aspects of data protection, e-privacy and online safety law, including advice on compliance documentation, policy and procedure, risk and impact assessment and individual rights. She has a particular focus on digital regulation that impacts on the handling of special category data or vulnerable groups, including employees and children. She regularly helps clients with assessment of new products or processes, including across multiple jurisdictions and defence in front of regulators.

Bird & Bird
12 New Fetter Ln
City of London, London EC4A 1JP
United Kingdom

Tel: +44 207 415 6728
Email: emma.drake@twobirds.com
LinkedIn: www.linkedin.com/in/emma-drake-43a3573b

Tristan Sherliker specialises in resolving IP disputes before the Courts in London, where he is of counsel in the IP practice.
He is a solicitor advocate working in leading IP cases and high-technology disputes. His focus is on litigation in the High Court and Court of Appeal, and advisory work to prevent disputes that could otherwise go there. He builds close working relationships with clients with a deep knowledge of their business, their needs and their technology. In disputes, he acts in the dual role of solicitor and counsel. Before law, his background was in biomedical engineering, combining more traditional engineering disciplines (such as electronics, mechanics, materials science and computing) with medical concepts (including anatomy, drug delivery and biochemistry).

Bird & Bird
12 New Fetter Ln
City of London, London EC4A 1JP
United Kingdom

Tel: +44 207 415 6641
Email: tristan.sherliker@twobirds.com
LinkedIn: www.linkedin.com/in/sherliker

Mario Subramaniam is a partner in our highly rated (*The Legal 500* and *Chambers*) Life Sciences and IP Team, advising Life Science clients on strategic licensing, collaboration and partnering transactions.
He has over 15 years of experience in advising Life Science clients on the development and exploitation of pharmaceutical, biotech, medtech and digital health technologies, with a particular emphasis on strategic IP licensing, collaboration and partnering transactions, as well as joint ventures, high-value manufacturing, supply and outsourcing arrangements. He also provides strategic support on M&A and asset acquisitions and disposals for Life Science clients.

Bird & Bird
12 New Fetter Ln
City of London, London EC4A 1JP
United Kingdom

Tel: +44 207 415 6000
Email: mario.subramaniam@twobirds.com
LinkedIn: www.linkedin.com/in/mariosubramaniam

USA


Roger Kuan


Jason Novak


Apurv Gaurav

Norton Rose Fulbright

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

Digital health is a technology sector that is a convergence of high technology with healthcare. The result is a highly personalised healthcare system that is focused on data-driven healthcare solutions, individualised delivery of therapeutics and treatments to patients powered by information technologies that enable seamless integration and communication between patients, providers, payors, researchers and health information depositories.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

The key emerging digital health subsectors are:

- Personalised/Precision Medicine (treatments tailored to an individual's uniqueness);
- Clinical Decision Support Tools (analytics tools used to assist physician decision-making);
- Remote Patient Monitoring and Delivery of Care (e.g., Internet of Medical Things, telemedicine, virtual healthcare, mobile applications, wearables, etc.);
- Big Data Analytics (clinically relevant inferences from large volumes of medical data);
- Artificial intelligence/machine learning (AI/ML)-powered Healthcare Solutions (e.g., diagnostics, digital therapeutics, intelligent drug design, clinical trials, etc.);
- Robot-Assisted Surgery (precision, reduced risk of infection);
- Digital Hospital (digital medical information management, optimised hospital workflows);
- Digital Therapeutics (use of digitally enabled devices or software to provide therapeutic treatment to patients); and
- Generative AI – generative AI models, such as generative adversarial networks, can be used to generate training data that are used to train traditional AI/ML models that are used for intelligent drug design and AI-powered diagnostics.

1.3 What is the digital health market size for your jurisdiction?

Depending on the source and how they define the digital health market, estimates of the digital health market size in the USA for 2025 range from a low of $54 billion to a high of $95 billion.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

- UnitedHealth Group.
- CVS Health.
- Oracle (Cerner Corporation).
- McKesson Corporation.
- Teledoc Health.

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

- Teledoc Health.
- Omada Health.
- Amwell.
- Modern Health.
- Doximity.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

In the United States, the U.S. Department of Health and Human Services (HHS) regulates the general health and safety of Americans through various programmes and divisions, including the U.S. Food and Drug Administration (FDA), Centers for Medicare and Medicaid Services (CMS), Office of Inspector General and Office for Civil Rights (OCR), among many others.

The Federal Trade Commission (FTC) regulates digital health through the Health Breach Notification Rule (HBNR). The HBNR requires companies that manage digital health records to notify consumers and the FTC if there is a breach of personal health information. The rule applies to most health apps that are not covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The FDA is the principle regulatory body charged with administering and enforcing the provisions of the Federal Food, Drug & Cosmetic Act, including those that relate to medical devices and Software as a Medical Device (SaMD). The FDA's jurisdiction covers all products classified as food, dietary supplements, drugs, devices or cosmetics, which have been introduced into interstate commerce in the United States.

In respect of the FDA's regulatory review of digital health technology, the Digital Health Center of Excellence (a part

of the FDA based in the Center for Devices and Radiological Health) aligns and coordinates digital health work across the FDA by providing regulatory advice and support to assist in its regulatory review of digital health technology.

The Digital Health Center of Excellence provides services in the following functional areas of digital health:

- Digital health policy and technology support and training.
- Medical device cybersecurity.
- AI/ML.
- Regulatory science advancement.
- Regulatory review support and coordination.
- Advanced manufacturing.
- Real-world evidence and advanced clinical studies.
- Regulatory innovation.
- Strategic partnerships.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

HIPAA, as amended by the Health Information Technology for Economic and Clinic Health Act (HITECH Act), is a core healthcare regulation related to digital health. HIPAA sets forth the federal privacy and security requirements for how certain entities must safeguard protected health information (PHI) (inclusive of electronic PHI (ePHI)) and how to handle security breaches of PHI or ePHI. In the U.S., individual states may also have state-specific healthcare privacy laws that pertain to their state residents that may apply to digital health offerings in a particular state and that may also be more strict than HIPAA.

In addition, a provider of digital healthcare will also be subject to various healthcare laws and regulations designed to promote transparency and prevent fraud, abuse and waste. Such laws and regulations to the extent applicable may include, but are not limited to, the federal Anti-Kickback Statute, the Ethics in Patient Referrals Act (or "Stark Law"), the federal False Claims Act, laws pertaining to improper patient inducements, the federal Civil Monetary Penalties Law, and state-law equivalents of each of the foregoing.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

The FDA has expressed its intention to apply its regulatory oversight to only those digital health software functions that are medical devices and whose functionality could pose a risk to a patient's safety if the device were to not function as intended. From a digital health perspective, this is a key area of enforcement, particularly in regard to digital health medical devices that are being marketed without the necessary FDA clearances or approvals in violation of applicable FDCA regulations.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

SaMD is regulated by the FDA and is defined by the International Medical Device Regulators Forum (IMDRF) as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device". SaMD can be used across a number of technology platforms, including medical device platforms, commercial platforms and virtual networks. For example, SaMD includes software with a medical purpose that operates on a general-purpose computing platform.

If the software is part of a hardware medical device, however, it does not meet the definition of SaMD and is not regulated by the FDA. Examples include: software that relies on data from a medical device, but does not have a medical purpose (e.g., encryption software); or software that enables clinical communication such as patient registration or scheduling.

Consistent with the FDA's existing oversight approach that considers functionality of the software rather than platform, the FDA has expressed its intention to apply its regulatory oversight to only those software functions that are medical devices and whose functionality could pose a risk to a patient's safety if the device were to not function as intended. For software functions that meet the regulatory definition of a "device" but pose minimal risk to patients and consumers, the FDA exercises its enforcement discretion and will not expect manufacturers to submit premarket review applications or to register and list their software with the FDA. Examples of such minimal-risk software includes functionalities that help patients self-manage their medical condition without providing specific treatment suggestions or that automate simple tasks for healthcare providers. The FDA publishes a more detailed list of examples of device software functions that are not the focus of FDA oversight.

In regard to the clinical evaluation of SaMD, the FDA issued the *Software as a Medical Device: Clinical Evaluation* final guidance to describe an internally agreed upon understanding of clinical evaluation and principles for demonstrating the safety, effectiveness and performance of SaMD among regulators in the IMDRF. The guidance sets forth certain activities SaMD manufacturers can take to clinically evaluate their SaMD.

It should be noted that the FDA considers mobile medical apps (mHealth apps) to be medical devices if they meet the definition of a medical device and are an accessory to a regulated medical device or transform a mobile platform into a regulated device. The FDA has published guidance that explains the FDA's oversight of mobile medical apps entitled the *Policy for Device Software Functions and Mobile Medical Applications Guidance*.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

Digital health devices and software solutions that are powered by AI and ML technologies are subject to FDA regulations and related review. In April 2019, the FDA published the *Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) – Discussion Paper and Request for Feedback*. The FDA remarked in its proposal that "[t]he traditional paradigm of medical device regulation was not designed for adaptive AI/ML technologies, which have the potential to adapt and optimise device performance in real-time to continuously improve healthcare for patients". The FDA also described in the proposal its foundation for a potential approach to premarket review for AI- and ML-driven software modifications.

In January of 2021, the FDA published the *Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a*

Medical Device (SaMD) Action Plan that included the FDA's plan to update its proposed regulatory framework through a five-part action plan that addresses specific stakeholder feedback. The five-part plan includes the following actions:

- Develop an update to the proposed regulatory framework presented in the AI/ML-based SaMD discussion paper, including through the issuance of a Draft Guidance on the Predetermined Change Control Plan (PCCP).
- Strengthen the FDA's encouragement of the harmonised development of Good Machine Learning Practice through additional FDA participation in collaborative communities and consensus standards development efforts.
- Support a patient-centred approach by continuing to host discussions on the role of transparency to users of AI/ML-based devices. Building upon the October 2020 Patient Engagement Advisory Committee meeting focused on patient trust in AI/ML technologies, hold a public workshop on medical device labelling to support transparency to users of AI/ML-based devices.
- Support regulatory science efforts on the development of methodology for the evaluation and improvement of ML algorithms, including for the identification and elimination of bias, and on the robustness and resilience of these algorithms to withstand changing clinical inputs and conditions.
- Advance real-world performance pilots in coordination with stakeholders and other FDA programmes, to provide additional clarity on what a real-world evidence generation programme could look like for AI/ML-based SaMD.

The FDA highlighted that its work in this area will be coordinated through the Center for Devices and Radiological Health's new Digital Health Center of Excellence.

2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Agencies, such as the FDA, have historically struggled with the dynamic nature of AI/ML-based digital health solutions. Even in the recent FDA guidance regarding PCCPs for ML-enabled medical devices, the guidance seems to still lean towards versioning. This is understandable given that versioning gives all involved a snapshot of a moment, and all the details that surround that moment, which is consistent with the FDA's traditional approach for static approvals. It also requires that manufacturers have clear foresight as to how they are going to modify their software, or else be subject to a new FDA submission. This call for intense pre-planning around post-launch updates puts a lot of pressure on these product companies to predict change, perhaps sooner than is reasonable.

It is clear the FDA realises the importance of automatic modifications to the software through consistent model retraining, especially with new data inputs. In a 2023 paper discussing FDA market submission recommendations for PCCPs, the FDA effectively noted that while automatic modifications are key in AI/ML, these modifications are more complex and that applying this new FDA policy would be difficult and the FDA's experience will play a part. Further, the Modification Protocol Section of the 2023 paper, particularly the host of questions posed in Appendix A, is seemingly thorough but also seems to lean towards versioning.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation data is essential in regulatory review, as it ensures that AI/ML-based digital health solutions perform accurately, safely, and effectively. Companies seeking FDA approval must prioritise well-designed clinical studies and adhere to Good Machine Learning Practices (GMLP) to navigate regulatory pathways successfully.

Clinical validation data factors into the regulatory process as follows:

1. Demonstrating Safety and Effectiveness: The FDA may require AI/ML-based digital health solutions to provide clinical validation data proving that the technology is safe and effective for its intended use. This typically involves:
   - Clinical trials or studies to assess performance.
   - Real-world evidence demonstrating accuracy and reliability.
   - Comparisons to standard care or existing approved devices.
2. Regulatory Pathway Considerations: AI/ML-based digital health solutions may fall under different FDA pathways depending on risk classification:
   - 510(k) Clearance (for moderate-risk devices with a predicate device).
   - *De Novo* Classification (for novel moderate-risk devices without a predicate device).
   - Premarket Approval (PMA) (for high-risk devices, requiring rigorous clinical evidence).

   In all cases, clinical validation data strengthens the submission by proving that the AI/ML model generalises well across patient populations.
3. GMLP: The FDA emphasises GMLP, which includes:
   - Ensuring that AI/ML models are transparent and reproducible.
   - Validating the AI/ML models with diverse datasets to avoid bias.
   - Continuous monitoring and post-market surveillance.

   Aligning clinical validation studies with these principles helps ensure unbiased, reliable AI performance.
4. Adaptivity and Real-World Performance: For continuously learning AI/ML models, clinical validation extends beyond initial approval:
   - The FDA has proposed a Predetermined Change Control Plan, where manufacturers outline how they will validate future model updates.
   - Post-market clinical validation may be required to ensure the model remains safe and effective as it evolves.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In the United States, digital health products and solutions are regulated at both the federal and state/regional levels, with differences in oversight based on the type of product, intended use, and risk to patients.

They are differentially regulated as outlined below.

Federal regulation

At the federal level, multiple agencies oversee digital health, with the FDA playing the most significant role.

1. FDA Regulation:
   - The FDA primarily regulates digital health products that qualify as medical devices (i.e., software or hardware used for diagnosis, treatment, or prevention of disease).
   - The level of oversight depends on the product's risk classification:
     - Class I (low risk): Minimal oversight (e.g., wellness apps).
     - Class II (moderate risk): Requires premarket review (e.g., some diagnostic tools).
     - Class III (high risk): Requires rigorous PMA (e.g., AI-powered decision-support tools for critical care).
   - The Digital Health Center of Excellence (part of the FDA) focuses on regulation and guidance for SaMD, AI in healthcare, and cybersecurity.
2. The Office of the National Coordinator for Health Information Technology (ONC):
   - Oversees health IT standards and interoperability, ensuring that electronic health records (EHRs) and digital tools meet federal standards.
   - Implements certification programmes for EHRs and interoperability rules under the 21st Century Cures Act.
3. The FTC:
   - Regulates consumer protection aspects of digital health tools, including data privacy, false advertising, and deceptive marketing claims.
   - Enforces compliance with the HBNR for apps and devices handling sensitive health data.
4. The HHS OCR:
   - Enforce HIPAA for digital health solutions handling PHI.
   - Ensure privacy and security standards are met by telehealth providers, health apps, and cloud-based healthcare services.

State/regional regulation

States have additional authority over digital health solutions, particularly in areas such as telehealth, professional licensing, and data privacy.

1. Telehealth regulation:
   - States determine licensing requirements for healthcare providers delivering telehealth services.
   - Some states participate in interstate compacts (e.g., the Interstate Medical Licensure Compact) that allow providers to practise across state lines with a streamlined licensing process.
   - Reimbursement policies for telehealth services vary by state Medicaid programmes and private insurers.
2. Data privacy and security:
   - Some states have stricter privacy laws than HIPAA, such as:
     - The California Consumer Privacy Act (CCPA), which provides additional protections for consumer health data beyond federal requirements.
     - The California Genetic Information Privacy Act, which focused on maintaining the privacy of genetic information.
     - Washington's My Health My Data Act, which regulates health data not covered by HIPAA.
   - Several states are adopting AI and cybersecurity regulations affecting digital health applications.
3. Consumer protection and digital health companies:
   - State Attorneys General can investigate misleading health claims or unfair business practices related to digital health products.
   - Some states have specific regulations for digital pharmacies, remote prescribing, and direct-to-consumer health apps.

The federal government provides overarching regulations for digital health, especially for medical devices, health IT standards, and data privacy under HIPAA. However, states retain authority over telehealth practice, professional licensing, and consumer protection, leading to variability in how digital health products and solutions are regulated across the U.S. Companies operating in this space must navigate both FDA and state-specific laws to ensure compliance.

Key differences in regulation by federal and state/regions

Aspect	Federal Regulation (FDA, FTC, HHS)	State/Regional Regulation
Medical device oversight	FDA regulates SaMD and digital health tools based on risk.	States do not regulate medical devices but can regulate their use.
Telehealth licensing	No federal licence; CMS sets reimbursement rules.	States regulate provider licensing and practice requirements.
Privacy and security	HIPAA applies to covered entities.	Some states (e.g., CA, WA) have stricter laws.
Consumer protection	FTC regulates false advertising and data breaches.	State Attorney-Generals enforce local consumer protection laws.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Regulatory enforcement actions for digital health products and solutions in the United States are being tailored through a combination of existing laws, new guidance, and risk-based approaches by agencies like the FDA, FTC, and HHS, among others.

Enforcement is evolving as follows:

1. Risk-based FDA oversight: The FDA has adopted a risk-based approach to digital health regulation, focusing on SaMD, while exercising enforcement discretion for lower-risk products. Key actions include:
   - Guidance on AI/ML in medical devices: The FDA is developing frameworks for ML-based software that adapts over time.
   - Pre-Certification Pilot Program: Aimed at streamlining approvals for trustworthy developers rather than individual products.
   - Digital health software exemptions: Certain mobile health apps and wellness products are not actively regulated if they pose low risk to patients (e.g., fitness tracking apps).

2. The FTC's focus on consumer protection and privacy: The FTC enforces privacy, data security, and deceptive advertising regulations for digital health companies. Notable actions include:
   - HBNR enforcement: Targeting health apps and digital platforms that fail to safeguard sensitive health data.
   - False advertising claims: Taking action against companies that make unproven health benefit claims about digital therapeutics or wearables.
3. HHS and HIPAA enforcement for health data: OCR enforces HIPAA compliance, focusing on how digital health apps and telehealth services handle patient data. New rules under HHS expand protections around health data sharing, particularly as part of interoperability and information blocking regulations.
4. State-level regulations and Attorneys General actions: State Attorneys General are also stepping in to enforce consumer protection laws on digital health tools, particularly around:
   - Data privacy (CCPA in California, for example).
   - Telehealth licensing and reimbursement policies.
   - AI-driven healthcare decision-making.
5. Emerging regulatory trends: FDA's new Digital Health Center of Excellence to refine oversight strategies, such as:
   - AI-specific regulations are being debated in Congress, particularly for bias and explainability in healthcare algorithms.
   - Cybersecurity enforcement is increasing for connected medical devices.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  - State-specific practice of medicine licensing laws and requirements.
  - Data privacy laws including HIPAA, CCPA and HITECH Act with respect to health data that is collected from patients during consultation.
  - Data rights to health data collected from patients during consultation.
  - FDA regulatory issues such as SaMD, 510k certification and PMA.
  - Stark Law and Anti-Kickback statutes.
- **Robotics**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with respect to health data that is collected and used to train software used to operate the robotic device.
  - Tort liability (products liability or negligence theories) for injuries sustained by patients during surgery.
  - FDA regulatory issues such as 510k certification and PMA.
- **Wearables**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to health data that is collected by devices.
  - Data rights to health data that is collected from device wearers.
  - FDA regulatory issues such as SaMD, 510k and PMA if the manufacturer seeks to make diagnostic or therapeutic claims for their devices.
- **Virtual Assistants (e.g. Alexa)**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to voice and Wi-Fi signal data that is collected by the virtual assistant.
  - Data rights to the voice and Wi-Fi signal data that is collected by the virtual assistant.
  - FDA regulatory issues such as SaMD, 510k and PMA if the manufacturer seeks to make diagnostic or therapeutic claims for the virtual assistant.
- **Mobile Apps**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to health data that is collected by the mobile app.
  - Data rights to the health data that is collected by the mobile app.
  - FDA regulatory issues such as SaMD, 510k and PMA if the manufacturer seeks to make diagnostic or therapeutic claims for the mobile app.
  - Tort liability (products liability or negligence) for injuries sustained by patients using mobile apps for diagnostic or therapeutic purposes.
  - Issues related to the patentability of software or diagnostics inventions.
- **Software as a Medical Device**
  - FDA regulatory issues such as SaMD, 510k and PMA if the manufacturer makes diagnostic or therapeutics claims for the software. Unique issues with evaluating safety and efficacy of software used to diagnose or treat patients.
  - Issues related to patentability of software of diagnostics inventions.
- **Clinical Decision Support Software**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to health data that is used in the software.
  - FDA regulatory issues such as SaMD, 510k and PMA if the developer seeks to make diagnostic or therapeutic claims for the software.
  - Tort liability (products liability or negligence) for injuries sustained by patients using the software for diagnostic or therapeutic purposes.
  - Issues related to the patentability of software or diagnostics inventions.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  - Inventorship issues with inventions arising out of AI/ML algorithms.
  - Clinical adoption of AI/ML software that is used in a clinical setting.
  - FDA regulatory issues such as SaMD, 510k and PMA if the manufacturer makes diagnostic or therapeutics claims for the AI/ML-powered software. Unique issues with evaluating safety and efficacy of AI/ML-powered software used to diagnose or treat patients.
  - Data rights issues related to the data sets that are used to train AI/ML software. This is even more complicated if the training data set includes data sets from multiple parties with differing levels of data rights.
- **IoT (Internet of Things) and Connected Devices**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to health data that is collected by the IoT and connected devices.
  - Data rights to the health data that is collected by the IoT and connected devices.

- **3D Printing/Bioprinting**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to handling patient imaging data used as 3D printing templates.
  - FDA regulatory issues such as SaMD, 510k, PMA and Biologics Licence Application depending on whether the manufacturer is making and selling rendering software, printing equipment and bioink with cells or other biological compositions.
- **Digital Therapeutics**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to health data that is used in or collected by the software and/or devices.
  - FDA regulatory issues such as SaMD, 510k and PMA if the developer seeks to make therapeutic claims for the software and/or devices.
  - Tort liability (products liability or negligence) for injuries sustained by patients using the software or devices for therapeutic purposes.
  - Issues related to the patentability of software or diagnostics inventions.
- **Digital Diagnostics**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to patient health data (e.g., biomarkers) that is used in or collected by the software and/or devices for the purpose of diagnosing medical conditions.
  - FDA regulatory provisions, such as SaMD, 510k and PMA, if the developer seeks to commercialise the digital diagnostics product (e.g., SaMD).
  - Tort liability (products liability or negligence) for injuries sustained by patients relying on a digital diagnostics product to undertake decisions that lead to the injury.
  - Issues related to the patentability of software or diagnostics inventions.
- **Electronic Medical Record Management Solutions**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to patient health data that is used in or collected by the software and/or devices, and then processed and/or stored by electronic medical record (EMR) systems and/or other hospital information systems.
  - Data rights to the patient health data that is collected by software and/or devices and then processed and/or stored by EMR and other hospital information systems.
  - Issues related to the patentability of software, data processing or EMR management inventions.
- **Big Data Analytics**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to any PHI or other sensitive data that is used in or collected by the software and/or devices.
  - Data rights to the PHI or other sensitive data that is collected by software and/or devices.
  - Issues related to the patentability of big data analytics inventions.
- **Blockchain-based Healthcare Data Sharing Solutions**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to any protected health data that is used in or collected by the software and/or devices, rendered accessible to others in the blockchain network, or shared to other software and/or devices.
  - Data rights to the patient health data that is used in or collected by software and/or devices the software and/or devices, rendered accessible to others in the blockchain network, or shared to other software and/or devices.
  - Issues related to the patentability of software or blockchain-based healthcare data sharing inventions.
- **Natural Language Processing**
  - FDA regulatory issues if the natural language processing (NLP) software is used as part of a medical device or SaMD used as a diagnostic or therapeutic purposes.
  - Tort liability (products liability or negligence) for injuries sustained by patients using these apps or devices, that incorporates the NLP software, for diagnostic or therapeutic purposes.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

The key issues for digital platform providers are:

- Compliance with data privacy laws including HIPAA, CCPA and HITECH Act with regard to health data that is collected by the providers.
- Obtaining data rights to the health data collected from customers/patients by complying with informed consent requirements.
- Data sharing and intellectual property (IP) provisions in agreements.
- Tort liability (products liability of negligence) for injuries sustained by patients using these platforms for diagnostic or therapeutic purposes.
- Issues related to the patentability of software or diagnostics inventions.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

HIPAA is the primary and fundamental U.S. federal law related to protecting patient health information. In relation to HIPAA, the HITECH Act, signed into law in 2009, further increased patient rights by financially incentivising the adoption of EHRs and increased privacy and security protection, and also increasing penalties to Covered Entities and their Business Associates for HIPAA violations. The CCPA, enacted in 2018, is an example of a state statute primarily focused on addressing the enhancement of privacy rights and consumer protection for that state's residents. Similar applicable laws exist in many U.S. states. Especially for data transactions with the EU, the General Data Protection Regulation (GDPR), in force since May 2018, protects natural persons in relation to the processing and movement of personal data.

There are a myriad of considerations that may arise from these laws and regulations. For example, what type of personal data is being used? If it is PHI, it would thereby be subject to HIPAA. Contrast this with wellness data, for example, which would appear to be health-related but in reality, is separate and distinct and, therefore, not regulated by HIPAA. Of course, personal data in general is subject to various state, federal and international data privacy laws.

Furthermore, what is the intended purpose of this data? Defining this purpose early and often is essential as it will become core to the metes and bounds of the data transaction and will help with the initial undertaking of seeking appropriate (patient) consents, which is far easier to do at the outset.

Even further, what are potential secondary uses of the data? Defining secondary uses up front is also important as a data user must maximise the value of the data transaction. Failing to set the expectation early may result in a data transaction of limited scope, forcing a data user to either seek amendment to the existing transaction or the need for a second agreement. In either case, leverage in negotiation will quickly pivot to the data holder, who will now have a clear idea of the importance to the data user of these secondary users.

Even further, where is the data coming from and where is it going? To answer this, detailed data maps need to be developed, tracing the path of data across various states and nations, thereby identifying the jurisdictions that will define the scope of data compliance requirements for a data user. As stated above, each impacted territory, whether state or country, may have unique data compliance (data privacy) laws that must be accounted for in executing the data strategy. Of note, data mapping is a requirement under several of the potentially applicable healthcare laws and as such, it factors into several parts of the data strategy.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

In the United States, personal health data is regulated at both the federal and state levels, with some variations in scope and strictness. The federal government sets baseline protections, while states can impose additional or stricter regulations. Below is a breakdown of how these regulations differ:

1. Federal-level regulation: At the national level, the key laws governing personal health data include:
   - HIPAA:
     - Regulates how covered entities (healthcare providers, insurers, and clearinghouses) handle PHI.
     - Requires patient consent for data sharing, with exceptions for treatment, payment, and healthcare operations.
     - Enforced by the HHS OCR.
   - 21st Century Cures Act and Information Blocking Rules:
     - Promotes patient access to EHRs and prohibits providers from blocking information sharing.
     - Enforced by HHS and ONC.
   - FTC Act and Consumer Data Privacy Laws:
     - The FTC regulates consumer health apps, wearables, and other non-HIPAA-covered health data under unfair/deceptive practices rules.
     - The FTC HBNR applies to health apps and non-traditional health data handlers.
   - Substance Use and Mental Health Privacy (42 CFR Part 2):
     - Stricter than HIPAA, requiring explicit patient consent before sharing substance use disorder treatment records.
     - Enforced by the Substance Abuse and Mental Health Services Administration (SAMHSA).
2. State-level regulation: States can expand protections beyond federal laws, and many have done so, particularly regarding:
   - Comprehensive consumer privacy laws: Some states, like California (CCPA/CPRA), Virginia (VCDPA), and Colorado (CPA), have privacy laws that cover personal health data outside HIPAA (e.g., fitness trackers, genetic data, wellness apps). These laws often require opt-in consent, data minimisation, and stricter consumer rights.
   - Genetic data privacy: States like California, Arizona, and Illinois have enacted laws regulating genetic testing companies (e.g., 23andMe), requiring explicit consent for sharing genetic data.
   - Biometric data privacy: Illinois' Biometric Information Privacy Act (BIPA) is one of the strictest laws in the country, requiring informed consent before collecting biometric data, including health-related biometrics.
   - Health Information Exchange (HIE) and data sharing rules: Some states, like New York and Texas, impose additional rules on how healthcare providers and HIEs handle and share patient data.
   - Reproductive and mental health data protections: Post *Dobbs v. Jackson Women's Health Organization*, some states (e.g., California, Washington, and New York) have enacted laws protecting reproductive health data from subpoenas and law enforcement in states where abortion is restricted.

Key differences between federal and state regulation

Aspect	Federal (Nationwide)	State-Level (Varies by State)
Scope	HIPAA applies to healthcare entities; FTC oversees non-HIPAA health data.	States may regulate broader categories, including consumer health apps and genetic data.
Consent rules	HIPAA allows some data sharing without consent.	Some states require opt-in consent for data sharing.
Genetic data	Governed by the Genetic Information Non-discrimination Act, but limited.	Some states require explicit consent for genetic data use.
Enforcement	HHS (OCR), FTC, SAMHSA.	State Attorneys General, privacy commissions.
Reproductive health	No specific federal protection post-*Dobbs*.	Some states protect abortion-related data from out-of-state requests.
Penalties for violations	Civil and criminal penalties under HIPAA, FTC fines.	State-specific fines and private lawsuits (e.g., BIPA in Illinois).

In summary, the federal government provides a baseline level of health data protection through HIPAA and other laws, while states fill in the gaps and sometimes impose stricter protections. The biggest regulatory gaps occur with non-HIPAA health data (like fitness trackers, apps, and direct-to-consumer genetic tests), where state laws are stepping in to add stronger privacy safeguards.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

Assuming the data under consideration is PHI, in dealing with HIPAA, a threshold determination is whether one is an entity subject to HIPAA (referred to as a "Covered Entity"), or a "Business Associate" of said Covered Entity by way of providing certain services for the Covered Entity. Covered Entities, aside from providers of healthcare that bill through claims, include, for example, government healthcare programmes (e.g., Medicare, Medicaid, military health programmes, veteran health programmes), health maintenance organisations, employee sponsored health plans and health insurance companies. Business Associates are parties (person or entity) that are not part of a Covered Entity workforce but, by virtue of acting on behalf of, or providing certain services to, a Covered Entity, receive access to PHI that is in the possession of the Covered Entity and which the Covered Entity has responsibility for.

4.4 How do the regulations define the scope of personal health data use?

Regulations concerning PHI, HIPAA and HITECH define the allowable scope of data use. According to HIPAA, the permitted data use for PHI includes the provisioning of healthcare (e.g., the treatment of patients), processing of healthcare payments and insurance claims, and facilitating the provisioning of healthcare (e.g., internal operations in hospitals and other facilities for the treatment of patients). HIPAA additionally requires limiting the use of PHI to the minimum possible extent that is necessary to fulfil the permitted use. Any data uses not explicitly permitted by HIPAA requires patient consent. However, even in situations where data use is permitted under HIPAA, it is important to check state privacy laws as they may restrict the scope of data use or require consent.

The HITECH Act further limits the scope of data use for PHI by strengthening privacy and security protections required under HIPAA. For example, the HITECH Act expands the enforcements of HIPAA data use requirements to Business Associates of HIPAA Covered Entities (e.g., cloud storage providers and billing companies of HIPAA Covered Entities). Furthermore, the HITECH Act enables patients of the PHI to request copies of EHRs and restrict disclosures of their PHI. Additionally, the HITECH Act mandates that any Covered Entities and Business Associates need to report breaches in data security of PHI.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

The key contractual terms to consider depend on what is being contracted. For example, for a data transaction involving entities as part of collaborative research, it is essential to clearly define IP rights arising out of the research, as well as primary and secondary uses of the data. Field restriction language can also become important, as it can minimise the impact of a data transaction agreement to a company's overall business strategy. With PHI involved, if an involved entity has been identified as a Business Associate, then a Business Associate Agreement may be needed between the Business Associate and Covered Entity. With non-PHI involved, data processing agreements may still be needed for handling data, even though it is not subject to HIPAA. Other potentially important terms include terms addressing data breaches, data handling during and after the agreement period, and associated representation/warranty language associated with any breach.

Securing comprehensive rights is extremely important. Healthcare data is exceptionally valuable – valuable to both the patient and the company that is able to procure such data. Given its criticality, one must have permission to use healthcare data for a desired purpose. Regardless of whether the healthcare data is generated or acquired by the data user, the data user must have the consent of the data's ultimate owner, i.e., the patient, to use that healthcare data. In the cases where healthcare data is acquired from a third party, the data user must also have the consent of the third party to use the healthcare data for a desired purpose. Often, consent from a third party (e.g., a healthcare data warehouse or aggregator) comes in the form of a data transaction, whereby said data user will usually remunerate the third party to acquire the healthcare data for the desired purpose. Of course, the consent between data owner and data user will come via the data owner providing consent to this third party to transact the data to parties such as the data user. It is worth noting that a healthcare data warehouse or aggregator does not solely mean data mines such as personal genomics companies 23andMe and Ancestry. It also includes traditional entities such as hospitals and hospital systems, universities, research institutes and pharmaceutical companies. Consent can come in a variety of ways, but it is critical to be able to demonstrate such consent for any downstream data use.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

Although case law for issues involving data inaccuracy, bias and/or discrimination are still developing, such issues may violate civil rights laws when it causes disparate impact (e.g., in healthcare) and perpetuates inequality. For example, if the use of an AI model trained on biased data results in the prescribing of different treatment options for different protected groups, this conduct could potentially violate anti-discrimination laws present, for example in Title VI and Section 1557 of the Affordable Care Act.

Furthermore, the use of problematic AI models having the aforementioned issues for medical treatment can lead to other liabilities. For example, if a patient is harmed as a result of the use of a biased AI model by a medical doctor, the patient may be able to issue a medical malpractice claim. The developers of the problematic AI model can also be held liable if they knew of the issues but failed to correct them.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

HIPAA is very relevant here, as it serves as the primary U.S. standard governing the use and collection of healthcare data, outlining privacy and security regulations for PHI managed by healthcare providers, plans and clearinghouses, ensuring patient data is handled responsibly and with appropriate safeguards. Key portions of HIPAA include the Privacy Rule (related

to how PHI can be used, disclosed and accessed, including patient rights to access their medical records and request amendments), as well as the Security Rule (which discusses specific technical and administrative safeguards to protect ePHI, including access controls, encryption and data integrity measures). Also relevant here is the Health Level Seven (HL7) standard, which is widely used to facilitate electronic exchange of medical information between different healthcare systems. HL7 is discussed in more detail in section 5 below.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

Key issues include data privacy and security generally, regardless of whether the information is PHI. For personal data in general, as discussed herein, entities dealing in data must consider the regulatory requirements across different jurisdictions. For U.S. data sharing, federal and state laws must be considered. For international data sharing, ex-U.S. regulatory schemes must fold into a data sharing strategy.

When the personal data is PHI, the regulatory requirements only increase, with federal laws such as HIPAA and the HITECH Act to consider.

From a personal standpoint, each individual must recognise their own personal right to their data, and must consider agreeing to consent agreements that may provide entities with the right to transact one's personal data beyond the scope said individual might desire.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

This is not applicable.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

When data is PHI and subject to federal regulations such as HIPAA and the HITECH Act, entities that qualify as Covered Entities and Business Associates may have to execute Business Associate Agreements to be in proper standing, and may have to ensure that all associated parties involved meet the obligations imposed by federal laws for the handling of PHI.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

As discussed herein, HIPAA provides standards for creating, maintaining and sharing healthcare data. For example, the HIPAA Permitted Uses and Disclosures defines the circumstances in which a Covered Entity may use or disclose an individual's PHI without having to first obtain a written authorisation from the patient. State laws are known to be even more stringent in their standards for creating, maintaining and sharing healthcare data. Furthermore, both federal and state laws prohibit the use of PHI and/or other protected healthcare data beyond what is necessary, and specify deletion and/or disposal requirements. For example, the Privacy Rule in HIPAA states that "a covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request". Furthermore, HIPAA mandates that unused media containing PHI should be adequately destroyed.

There are also initiatives to create standards for creating, maintaining and sharing healthcare data that facilitate interoperability. For example, the Consolidated Health Informatics initiative announced its requirement that all federal healthcare services agencies adopt the primary clinical messaging format standards (i.e., the HL7 Version 2.x (V2.x) series for clinical data messaging, Digital Imaging and Communications in Medicine (DICOM) for medical images, National Council for Prescription Drug Programs (NCPDP) Script for retail pharmacy messaging, Institute of Electrical and Electronics Engineers (IEEE) standards for medical devices, and Logical Observation Identifiers, Names and Codes (LOINC) for reporting of laboratory results) (Office of Management and Budget, 2003).

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

In a federated model of healthcare data sharing, multiple entities may function as nodes of an interconnected but decentralised network, and each node may locally store healthcare data. Furthermore, healthcare data can be queried or otherwise analysed by other nodes in the network without the healthcare data necessarily leaving the node at which it is located.

One of the major issues to consider for federated models of healthcare data sharing is interoperability. Specifically, one should consider whether the format (e.g., structures, concepts, syntax, ontologies) of healthcare data stored by each node is harmonised or can be readily converted to a format amenable to other nodes. For example, if a given (first) node of the federated model requests healthcare data stored by another (second) node, the healthcare data stored by the second node may need to be converted into a format that is understandable by the first node. As discussed herein, various initiatives have required or encouraged data sharing formats to facilitate interoperability for healthcare data (e.g., the HL7 V2.x series for clinical data messaging, DICOM for medical images, NCPDP Script for retail pharmacy messaging, IEEE standards for medical devices, and LOINC for reporting of laboratory results).

Another issue to consider is whether the federated model ensures privacy, data security and the appropriate level of access control for healthcare data being stored at each node. For example, depending on the node (e.g., a pharmacy information system, a radiology system, a clinical research institution, etc.), different stakeholders may be granted different levels of access to healthcare data stored in the node.

Yet another issue is the need to actively manage the healthcare data stored across the different nodes of the federated model. For example, there may exist potentially incomplete, unsynchronised and heterogenous healthcare data among various nodes of the federated model. Since this could impair healthcare for patients, the various nodes of the federated model should have a system by which to ensure that the healthcare data stored across the various nodes are updated and/or complete.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

As relevant to digital health, current U.S. patent law is generally unfavourable towards the subject matter patentability of software and diagnostics inventions. As such, successfully navigating the subject matter patentability hurdle is the first step to protecting digital health solutions. Recent U.S. Supreme Court and Federal Circuit cases have begun to chip away at this hurdle for diagnostics innovation (See *Hikma Pharmaceuticals USA Inc. v. Vanda Pharmaceuticals Inc.* (https://www.scotusblog.com/case-files/cases/hikma-pharmaceuticals-usa-inc-v-vanda-pharmaceuticals-inc) and *CardioNet, LLC v. InfoBionic, Inc.* (https://law.justia.com/cases/federal/appellate-courts/cafc/19-1149/19-1149-2020-04-17.html)) and the current expectation is that future cases will continue to swing towards affirming protection for this important class of innovation. In addition to satisfying the subject matter hurdle, novelty and non-obviousness are also required for patentability.

Regarding software innovation, U.S. patent case law has established that patenting an "abstract idea" is not permitted. An abstract idea covers concepts that are considered too fundamental or theoretical, and therefore lacking practical application. This can include, for example, mathematical formulas, basic mental processes, fundamental economic principles, and methods of organising human activity. Digital health-related concepts and principles may be considered under the umbrella of abstract ideas, and thus subject to particular tests that either label or establish an inventive concept beyond that abstract idea. In the past few years, however, the U.S. Patent and Trademark Office (USPTO) has provided more guidance to overcome such rejections and more software cases are seeing positive results at the federal courts.

The term of utility patent protection (with certain exceptions) is 20 years (15 years for design patents) from the date of filing the application. A patent gives the patent owner an affirmative right to exclude others from making, using or selling the patented invention.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

For digital health solutions, copyright protects the software source code and object code as works of authorship, and databases as compilations (provided there is sufficient originality in the structure, sequence and organisation of the database to meet the originality requirement). While copyrights arise automatically, the U.S. has a formal process to register copyrights, which is a prerequisite for commencing a copyright infringement action. Registered copyrights are eligible for "statutory damages" under the Copyright Act, which can help mitigate the difficulties in establishing the monetary value damages due to the copyright infringement. Copyrights that are registered within five years of publication establish *prima facie* evidence of the validity of the copyright and facts stated in the copyright registration certificate. Also, the burden of proof of non-infringement shifts to the alleged infringer.

To register software source code (or object code) or a database with the U.S. Copyright Office (a part of the Library of Congress) a "registration deposit" copy of the software code or database must be deposited that meets the requirements under the Act. The term of copyright protection is the life of the author plus 70 years, unless the work had been created as a work made for hire, in which case the term is the shorter of 120 years after creation or 95 years after publication.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

Trade secret protection can be used to protect formulas, practices, processes, designs, instruments, patterns or compilations of information that is not generally known to the public and have inherent economic value. Trade secrets have no fixed term but require the owner to appropriately mark the information and to put in appropriate safeguard measures to guard the information from being released to the public. However, unlike patents, trade secrets cannot prevent independent development of the trade secret information.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

Most academic institutions require their professors, researchers and students to assign any IP they develop with the institution's resources or funding to back them. In some instances, the institutions, applicable departments and the professor/researcher enter into separate royalty sharing agreements.

The IP is typically out-licensed to third parties for commercialisation on terms that may include: royalties; upfront payments; milestone payments; and equity in the licensee company.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

SaMD, which the FDA defines as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device" can be protected by patents, copyrights and/or trade secrets. SaMD source code and objects can be copyrightable and protected as trade secret subject matter (providing that they are appropriately marked and appropriate protections are put into place to ensure that they are not released to the public). A SaMD can also be protectable by patents if it meets U.S. subject matter patentability requirements and is novel and non-obvious over the prior art.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

In the United States, both the courts (in *Stephen Thaler v. Andrew Hirshfeld*, E.D.Va., 2021) and the USPTO have ruled that an AI machine cannot be an "inventor" for purposes of the U.S. Patent Act (35 U.S. Code). According to the courts, the issue of whether an AI device can be considered an inventor depends on the simple question of whether an inventor needs to be a human being. The Patent Act explicitly states, in its definitions, that inventors are "individuals". Since there is sufficient

precedent supporting the conclusion that "individuals" are human beings, the courts concluded that non-humans, such as AI programs, cannot be considered individuals, and therefore cannot be considered inventors.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

In the U.S., the Bayh-Dole Act of 1980 (35 U.S.C. § 200–212) deals with inventions arising from federal government-funded research. Before the enactment of the Bayh-Dole Act, the government's consistent position was that the results of any research and development funded with taxpayer's money should be in the public domain and freely available to the public.

The Bayh-Dole Act permits qualified small businesses and non-profits to retain title to "subject inventions" arising out of federal-funded research providing that they comply with the following conditions: (1) the federal government receives a licence in subject inventions; (2) the private party has properly notified the government of the subject inventions; (3) the preference for U.S. industry that is found in all technology transfer programmes is included; and (4) the federal government retains "march-in rights". Within this framework, a "subject invention" is any invention of a qualified private party (i.e., small business or non-profit) conceived or first actually reduced to practice in the performance of work under a funding agreement. Whereas, "march-in rights" permit the federal government to order a private party to grant a compulsory licence to a third party (including competitors) when they make a determination that the private party has not: (1) taken effective steps to achieve practical application of the invention within a reasonable time; (2) reasonably satisfied national health and safety needs; (3) reasonably satisfied regulatory requirements for public use; or (4) received the required permission from the government under the U.S. industry preference provision before licensing.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

Several key legal cases and decisions have shaped IP rights protection for digital health innovations in the United States. These cases span patent law, copyright, and trade secrets, affecting how digital health technologies are protected. Below are some of the most important precedents:

1. Patent law and software-related digital health innovations

Alice Corp. v. CLS Bank International (2014) – 573 U.S. 208:

- This Supreme Court decision established the two-part test for patent eligibility of software and abstract ideas.
- Many digital health innovations rely on software-based processes, and this case has led to numerous invalidations of patents related to health IT and medical algorithms that are deemed abstract.
- It has made it harder to patent AI-driven health diagnostics and decision-support tools unless they involve a concrete technological improvement.

Mayo Collaborative Services v. Prometheus Laboratories (2012) – 566 U.S. 66:

- The Court ruled that laws of nature and natural correlations (such as biomarker-based diagnostic methods) are not patentable unless they contain an inventive step beyond merely applying a natural law.
- This case significantly affected precision medicine and digital health patents involving AI-driven diagnostics and personalised treatment algorithms.

Association for Molecular Pathology v. Myriad Genetics (2013) – 569 U.S. 576:

- The Supreme Court held that naturally occurring DNA sequences cannot be patented but synthetic DNA (cDNA) could be.
- This decision impacted digital health companies using genetic data and sequencing technologies.

2. Copyright protection in digital health

Google LLC v. Oracle America, Inc. (2021) – 593 U.S.:

- The Supreme Court ruled that Google's use of Java APIs in Android was fair use.
- This case has implications for interoperability in digital health software, especially regarding whether the reuse of APIs in health IT systems and EHRs can be protected by copyright or subject to fair use.

3. Trade secret protection in digital health

Epic Systems Corp. v. Tata Consultancy Services Ltd. (2020):

- A jury awarded Epic Systems nearly $1 billion in damages after Tata misappropriated trade secrets related to Epic's EHR software.
- This case underscores the importance of trade secret protection for digital health technologies, especially for proprietary algorithms and data analytics.

Waymo LLC v. Uber Technologies, Inc. (2018):

- Google's self-driving car subsidiary sued Uber over alleged trade secret theft involving AI and sensor technology.
- Although not strictly a digital health case, it demonstrated how AI-driven innovations can be protected under trade secret law, which applies to AI-powered health diagnostics and medical robotics.

4. FDA and regulatory considerations affecting digital health IP

Apple Inc. v. Masimo Corp. (Ongoing, 2023–2024):

- Masimo sued Apple, alleging that Apple stole its pulse oximetry technology for use in the Apple Watch.
- This case is significant for digital health wearables and raises questions about trade secrets *versus* patent protection.

These cases illustrate how digital health innovations face complex IP challenges. Patent law limits software and diagnostic method protections, copyright law affects software interoperability, and trade secrets provide alternative protections. Given the evolving legal landscape, companies developing digital health technologies must carefully navigate IP strategies, including patents, trade secrets, and regulatory compliance.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

Collaborations are commonplace in digital health and can generally be grouped into two categories: collaborations that are data driven; and those that are technology driven.

In data-driven digital health collaborations, the parties are interested in granting, acquiring or sharing access to data that is used to power digital health solution(s).

Typical data-driven collaboration scenarios are:

- A healthcare institution (e.g., hospital system, hospitals, clinics, community health organisations, etc.) sharing their patient data (typically patient medical records, biological samples used to generate data, questionnaires, etc.) with a company that utilises the data to discover or power their digital health solution(s).
- A university or non-profit research organisation sharing their research data with a company that utilises the data (typically genomic, proteomic, microbiome, study results, etc.) with a company that utilises the data to discover or power their digital health solution(s).
- Companies sharing patient or research data where the data flows from one company to the other or between the companies to discover or power their digital health solution(s).

In technology-driven digital health collaborations, the parties are interested in either obtaining technology from one another or sharing their collective technologies to develop the digital health solution(s).

Typical technology-driven collaboration scenarios are:

- A university or non-profit research organisation sharing their technology or know-how with a company that utilises that technology for their digital health solution(s).
- Companies sharing technology or know-how to develop combined digital health solution(s).

Ownership of IP rights (e.g., patents, copyrights, technical know-how, research results/data, etc.) to the collaborative improvements that result from the shared data and technologies can be governed by U.S. IP laws and/or in the terms of the agreement between the parties. Although the default stance is typically joint ownership, data owners have unique negotiation leverage to insist that they own the IP rights (with the data recipient being granted a licence or option to those rights) since their data is the core asset in the collaboration.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

The most important legal considerations to pay attention to in agreements between healthcare and non-healthcare companies are data privacy compliance and data rights.

With respect to data privacy compliance, the parties need to pay attention to their respective roles and responsibilities in the agreement as it relates to compliance with HIPAA and patient informed-consent requirements. Failure to properly develop and/or execute processes that are compliant with HIPAA or informed-consent requirements can result in patient data that is tainted, which will encumber its use by the parties.

Data rights is another important consideration in this type of agreement where data (e.g., patient medical records, questionnaires, etc.) is typically owned by the healthcare company which then shares it with the non-healthcare company. It is important for the non-healthcare company to secure the data rights it needs from the healthcare company so that they can use the data for what they need it for and to have the healthcare company warrant or represent that they have properly secured the rights to the data from their patients.

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

Although AI can revolutionise healthcare based on the large volume of medical data that is now available, AI is restricted in its ability to do so because medical data is often siloed among different entities (e.g., companies, institutions, systems) with barriers preventing access to such medical data. These barriers often arise from data privacy concerns. Federated learning may provide a solution to this problem by training AI models collaboratively without exchanging the patient-specific healthcare data itself. While the training for these AI models may occur locally (e.g., at a participating company), the results of the trained AI model (e.g., weights, parameters, etc.) can be transferred elsewhere in the federated network (e.g., to a different company in the federated network). Although federated learning, in theory, obviates the privacy concerns associated with sharing patient-specific healthcare data among different companies in a federated network, the sharing of federated learning data (e.g., the weights or parameters of a locally trained AI model) is not bullet-proof in eliminating all privacy and data security concerns, and may additionally lead to other issues to consider.

For example, since locally trained AI models are based on locally available healthcare data, locally trained AI models based on non-heterogeneous, non-diverse or small-sized healthcare data may potentially reveal private information about a set of patients that may not have provided consent. Thus, even in a federated learning environment, additional privacy-preserving measures may be implemented when exchanging the results of locally trained ML models across companies.

Secondly, since locally available healthcare datasets used to train the ML models in federated learning are characteristically smaller in comparison to healthcare data available to companies and entities across the healthcare landscape, the ML models thus trained may not necessarily have the best performance. Simply put, there may be a trade-off between the advantages of preserving data privacy conferred through federated learning, and the reduced performance of the ML models developed through federated learning.

Therefore, when entering federated learning healthcare data sharing agreements, a party should consider the trustworthiness of other members of the healthcare data sharing agreement to strike the right balance in this trade off. For example, when there are trusted parties, there is a reduced need for additional privacy-preserving countermeasures, and the parties may opt for ML models with optimal e-performance. On the other hand, for federated learning that occurs among parties that may not all be trustworthy, additional measures may be required to mitigate data security risks. Such additional measures may include, for example, advanced encryption of trained ML models, secure authentication and verification systems of all parties, differential privacy and protections against adversarial attacks.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Although generative AI has the potential to revolutionise the healthcare industry, parties seeking to use generative AI in the provisioning of digital health solutions should consider the following factors:

- Parties should be cautious of the overreliance of generative AI tools and products for digital health solutions. In particular, generative AI models are known to often produce false results (i.e., hallucinations). When treatment recommendations are based on such results, the effect on the user's health can be potentially catastrophic, and companies using the generative AI can be held liable.
- Generative AI models rely on large amounts of data for their development. Parties should determine whether such data includes PHI or any information that otherwise identifies known individuals. In particular, HIPAA requires Covered Entities to only use and disclose PHI for certain permitted purposes, which include (among other purposes) the use of such data for the patient's treatment, processing of payments and the organisation's healthcare operations purposes. Thus, the use of such data for the training of generative AI models would need to be justified under such permitted purposes. If a Covered Entity's use of PHI does not fall within a permitted purpose, the Covered Entity would need the patients' consent to use or disclose their identifiable data.
- As obtaining consent from each and every patient may be impractical considering the size of datasets typically used in generative AI models, parties may consider deidentifying the data in order to avoid falling under the purview of the HIPAA rules. However, parties should be aware of state privacy laws that have even more stringent data use requirements than HIPAA.
- Even after a generative AI is trained, a party using trained generative AI to provision a digital health solution to a user should be aware of any input received form the user. The input may itself be considered a PHI under HIPAA or other data worthy of privacy protection under more stringent state laws.

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

The FDA plays a primary role in regulating SaMD, which includes healthcare products that are AI/ML-enabled, as the FDA's purpose is to protect the public health by ensuring the safety, efficacy and security of drugs, biological products and medical devices.

The HHS OCR also enforces regulations related to healthcare data use and collection.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

For the FDA, issued guidance/discussion through, for example, the SaMD proposed regulatory framework (2019 paper), the SaMD action plan (2021 paper) and the marketing submission recommendations for PCCP for SaMD (2023 paper) all highlight an aggressive commitment to developing a regulatory framework around AI/ML-enabled medical devices (including software).

The OCR enforces HIPAA in order to protect against improper use and collection of patient healthcare data.

Details on HIPAA and FDA Guidance related to AL/ML-enabled SaMD are discussed at length above.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Current U.S. law requires that patents and copyrights can only be owned by human inventors and authors, respectively.

For patents, 35 U.S.C. §100, the Manual of Patent Examining Procedure and recent Federal Circuit cases (*Beech Aircraft Corp. v. EDO Corp.*, 990 F.3d 1237, 1248 (Fed. Cir. 1993); and *Univ. of Utah v. Max-Planck-Gessellschaft zur Forderung der Wissenschaften e.V.*, 743 F.3d 1315 (Fed. Cir. 2013)) have held that only natural persons can be inventors for patents.

For copyrights, §306 of the Compendium of U.S. Copyright Office Practice states that "(t)he U.S. Copyright Office will register an original work of authorship, provided that the work was created by a human being".

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

A variety of considerations must be addressed when licensing data for use in ML for digital health solutions, including, for example:

- Data Set Definition:
  - The contents of the data (e.g., genomic, proteomic, EHRs, etc.) being shared.
  - The type of data (e.g., PHI, deidentified, anonymised, etc.) that is being shared.
  - The file format of the data being shared.
- Data Use Case:
  - Data used to train ML algorithm of digital health solution.
  - Geographic location(s) for data use.
  - Fields (e.g., oncology, ophthalmology, etc.) that the data can be used in.
- Data Rights:
  - Ownership of the data and subsequent data generated from the data.
  - Amount of time that the data can be used for.
  - Sub-licensing rights.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Standard AI (e.g., traditional or predictive AI) uses structured data and predefined algorithms to analyse information and make predictions. Examples of digital health technologies and products using standard AI include ML models for disease prediction or anomaly detection in medical images. Generative AI uses deep learning models (e.g., large language models) to generate new content, such as new text, new images or synthetic data. Examples of generative AI applications in digital health include the use of generative AI to draft patient notes, engage patients in telemedicine (e.g., via chat bots), generate explanations of medical conditions, and generate potential molecular structures for new treatments.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

The first major issue is accuracy and reliability. Generative AI can potentially create false or misleading medical information (e.g., via hallucinations), which is particularly concerning for healthcare. A second issue is the reliability of data used to train the generative AI model. If the generative AI relies on biased or incomplete data, the resulting digital health products may potentially reinforce health disparities. Related to both the first and second issue is the lack of clarity on who would be responsible if a digital health technology employing the generative AI is found to be defective (e.g., the technology leads to an unfavourable medical outcome). Would liability fall on the AI developer, the healthcare provider using the technology, or an institution employing the healthcare provider? A third issue relates to the risk of compromising sensitive or proprietary information in the process of the digital health product generating new content via its generative AI model. For example, it is likely that digital health technologies applying generative AI models are trained on the PHI of patients, and must therefore be compliant with relevant privacy laws (e.g., HIPAA, GDPR, etc.). However, there is a risk that the new content generated by the AI model may inadvertently reveal sensitive information about the patient. Similarly, there is a risk that the new content may be too similar to a copyrighted or other IP-protected work based on the training data including such work. The use of the new content may result in IP infringement.

Various legal considerations may help mitigate the aforementioned issues. For example, it may be useful to rely on de-identified, encrypted and/or synthetic data instead of PHI to train AI models, in order to reduce privacy risks. To the extent PHI is used, it is important to obtain patient consent in accordance with HIPAA, the HITECH Act and state privacy laws. To the extent the dataset includes any proprietary or IP-protected data, it is crucial to obtain the necessary licences to use the dataset. Additionally, it may be useful to train generative AI models on datasets that are diverse and representative to reduce bias and create a more effective product. Furthermore, human oversight in AI-generated medical recommendations may be critical in preventing harm to a user, averting hallucinations, reducing tort and other legal risks, and gaining the public's trust and acceptance of the generative AI-enabled digital health product.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

The FTC is starting to employ a penalty referred to as algorithm disgorgement to punish companies who use improperly sourced data in algorithm development and training. This penalty requires companies to delete or destroy algorithms and models that were developed using illegally obtained data. This essentially means that the company must remove any products built on data it should not have used, effectively taking away the benefits gained from improper data collection practices.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Theories of liability include: contract breach (e.g., data agreements, data transaction, consent agreements); violation of U.S. federal, U.S. state, and ex-U.S. laws related to the protection of PHI and personal data generally; negligence (e.g., by the product provider, the health provider, or the payer); product liability and Consumer Protection Law in the U.S. and abroad; Corporate Practice of Medicine; and Anti-Kickback laws (even with recent legislation increasing safe harbour).

9.2 What cross-border considerations are there?

Please see question 9.1 above as many of these liability categories are analogues in ex-U.S. territories. Jurisdictional issues may arise due to the digital nature of the industry, but other more established liability categories (e.g., tort laws) will generally be applicable in various countries for which business is conducted.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

As previously discussed, data used in the training and development of generative AI for digital health solutions may include PHI and other sensitive data protected under various state privacy laws. When obtaining authorisation from the respective patients or individuals is impractical or impossible, it is advisable to deidentify such data to the extent possible, or otherwise make sure that the use of such data in generative AI model training complies under various privacy laws (e.g., HIPAA, state privacy laws, etc.). For example, HIPAA requires that PHI can only be used for various permitted purposes. Such data should also be handled with extreme care, for example, by strengthening cybersecurity and implementing measures to prevent reidentification.

Companies should safeguard against the overreliance of data output from generative AI models. For example, to protect users from and minimise liability risks associated with false data (i.e., hallucinations), companies should provide disclaimers that the generative AI models are merely recommendations and the recommendations may change based on the dataset in which the models are being trained.

Furthermore, if a company relies on another partner for the use or implementation of a generative AI tool, the company should ensure that there are privacy policies and data security procedures in place to clarify data ownership and specify how the partner is to use the generative AI tool.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

The FTC can utilise algorithm disgorgement, discussed above. The HHS OCR can require corrective action plans under HIPAA, where Covered Entities would be required to adopt plans to address compliance deficiencies. There are also civil monetary

penalties under HIPAA, with a wide range of money damages per violation. In fact, state attorneys can bring civil actions themselves. Under HIPAA, there can be criminal violations, and corresponding criminal penalties, carried out by the Department of Justice. These penalties can include both fines and imprisonment.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

As discussed herein and above, digital health (regardless of whether it is cloud-based), bring several potential legal issues related to, for example, data use, data rights, data security/cybersecurity (e.g., hacking, loss, breaches), data loss and PHI. These issues can arise in the U.S., in several U.S. states, and internationally as well. Cloud use can also bring forth issues depending on data location, which can be in various places around the world depending on entity location, customer location, and so on.

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

As discussed above, digital health is a convergence of typically disparate industries: tech; and healthcare. Each industry encounters unique issues. The extremely highly regulated and appropriately risk-averse nature of healthcare can lead non-healthcare companies to have strategic (often legal) "blind spots" based on their experience leading up to the digital health endeavour. For example, non-healthcare companies, unlike healthcare companies, have not typically had to contemplate various legal issues. These can include, for example, FDA, HIPAA/HITECH Act, state health data laws, international health data laws, reimbursement, corporate practice of medicine and anti-kickback considerations.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

As a continuation of question 10.2, not only are there various legal and strategic issues commensurate with converging two typically disparate industries, each having their own unique issues, these issues and their corresponding strategy should be sophisticatedly addressed and dealt with concurrently by a digital health venture. These issues include, primarily, IP, FDA/regulatory, data use/privacy/security (including HIPAA), reimbursement and healthcare transactions. These issues are interrelated and unless a cohesive strategy, from the off, addresses a plan for each of these issues, a potential investment target may have a "blind spot" that can significantly delay launch, diminish revenue, or slow or reduce adoption. It must be noted that each of these issues cannot always be "handled" by early-stage companies immediately at once. Rather, these issues should be considered, and a strategy developed that will be tested, executed and regularly reassessed so that each issue can be moved forward to resolution concurrently with the other issues.

Moreover, given the converging nature of digital health, investors should not assume that founders are broadly educated on all these subjects. Early diligence as to strategy is essential as there are not many serial digital health entrepreneurs given the youth of the digital health industry. This can rear its head, not only with understanding how to address the issues above, but also how to transact with partner entities (e.g., health systems and large pharmaceutical companies of typically greater experience and leverage), which can saddle new ventures with contract terms that affect future growth potential.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

There are two spectrums to the hurdles affecting widespread clinical adoption. On the one hand, the industry of digital health is young from an adoption standpoint. Many patients, particularly the elderly, have extensive experience and likely comfort with in-person treatment. Moreover, the parties involved in deciding on a digital health solution are very likely new to the industry as well, making robust diligence difficult to achieve on potential digital health solutions. On the other hand, due in part to COVID-19, digital health entrants have increased dramatically in the last few years. As a result, digital health consumers, already ramping up their knowledge in this space, now have to deal with a wealth of options. Which to choose? How do I navigate all these potential solutions?

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

With the dramatic increase in digital health solutions entering the market, and the aforementioned diligence shortfalls that can accompany customers, formal endorsements are one way of differentiating your solution from your competitors. Add to that the difficult financial situation in the U.S., one that may continue for a substantial period of time, and customers will be even more circumspect in analysing solutions, and may look for any designation that can mitigate the risk of purchasing a subpar solution.

Key digital health-related certification bodies in the U.S. include: the American College of Radiology; the American Board of Medical Specialties; the American Medical Association; and the American Board of Professional Psychology.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

From a U.S. industry standpoint, payors continue to observe inconsistency in regard to the reimbursement of digital health-related therapies and treatments. Further, from a government payor programme perspective, government review of proposed regulations continues in an effort to ascertain how best to determine whether a particular digital health-related device is clinically beneficial to or reasonable and necessary for a government healthcare programme beneficiary. The result is healthcare providers seeking reimbursement for digital health-based care must utilise the coverage, coding and billing requirements of the respective payor programmes (whether

government or private based) that are currently available and that vary by payor programme. Providers seeking reimbursement must also comply with the respective enrolment, registration and licensing requirements of such payors as they would with any healthcare treatment reimbursement submission.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Innovations in digital health often involve the use of multiple entities. For example, personalised medicine may involve the use of organisations that collect data to be used for the training of AI/ML models, computing systems performing the development and training of the AI/ML models, computing systems deploying and utilising the trained AI/ML models to discover insights for drug development, and labs developing the drugs. The presence of multiple entities, even for a single innovation, raises unique challenges for enforcing or protecting against legal claims, whether it is data privacy violation, IP infringement or product liability. For example: patent claims may need to be prepared with an eye toward the different entities practising various aspects of the innovation; data maps would need to be developed for each entity, to uncover the myriad areas in which breaches could occur; and product liability would need to be investigated through each entity's vantage point.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

This is not applicable.

Roger Kuan is a Partner at Norton Rose Fulbright and US head of the Digital Health and Precision Medicine Practice, where he counsels companies that are uniquely positioned in the convergence of the life/medical sciences and technology industries on how to successfully navigate the complexities of the IP, data rights and regulatory challenges they encounter.
Roger has extensive experience in IP strategy and portfolio management (utility/design patents, trademarks, copyrights, and trade dress), data rights strategy, licensing and technology transactions, freedom-to-operate clearances, enforcement, monetisation, IP due diligence, and dispute resolution. His practice is focused in the life sciences sector (e.g., research tools, analytical instrumentation/software, digital therapeutics, medical devices, diagnostics, biomanufacturing equipment, etc.) with an emphasis in emerging technologies such as precision medicine (e.g., genomic sequencing platforms, AI/ML, computational genomics/bioinformatics, molecular diagnostics, companion diagnostics, etc.), digital health (e.g., mobile apps, clinical decision support, software, AI/ML imaging diagnostics, wearables, etc.) and 3D printing/bioprinting.

Norton Rose Fulbright
1 Embarcadero Center, Suite 1050
San Francisco, California 94111-3698
USA

Tel: +1 628 231 6810
Email: roger.kuan@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/roger-kuan-1b5b824

Jason Novak's practice was specifically created to focus on advising entities, both large and small, on the various legal issues that can arise with emerging technologies in the healthcare, food and life sciences industries, with a particular and targeted focus on "convergence" technologies (e.g., digital health, personalised/precision medicine, alternative protein) that operate at the intersection of multiple industries.
Jason has extensive experience in IP and data rights strategy. For data rights, Jason advises clients on transactions, protection and general strategy. On the IP front, Jason's experience extends to patent portfolio management, preparation and prosecution, oppositions, counselling, licensing and technology transactions, in- and out-licensing, freedom-to-operate, various types of due diligence, IP training, risk recognition and management and dispute resolution.

Norton Rose Fulbright
1 Embarcadero Center, Suite 1050
San Francisco, California 94111-3698
USA

Tel: +1 628 231 6811
Email: jason.novak@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/jason-novak-002102b

Apurv Gaurav is a USPTO-registered lawyer and a senior counsel in the IP Transactions and Patent Prosecution group at Norton Rose Fulbright. Apurv is passionate about helping his clients form, protect, enforce and utilise patents and other IP assets in a manner that advances his clients' long-term business strategy. Leveraging his technical background in electrical engineering and molecular and cell biology, and his advanced coursework and certification in machine learning, Apurv has worked on various legal matters spanning a wide spectrum of technologies, but is uniquely well-positioned to advise in digital health, precision medicine and other areas at the convergence of software and life sciences.

Norton Rose Fulbright
1045 W. Fulton Market, Suite 1200
Chicago, Illinois, 60607
USA

Tel: +1 312 964 7775
Email: apurv.gaurav@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/apurv-gaurav-39611454

Norton Rose Fulbright provides a full scope of legal services to the world's preeminent corporations and financial institutions. The global law firm has more than 3,000 lawyers advising clients across more than 50 locations worldwide, including London, Houston, New York, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg, covering Europe, the United States, Canada, Latin America, Asia, Australia, Africa and the Middle East. With its global business principles of quality, unity and integrity, Norton Rose Fulbright is recognised for its client service in key industries, including: financial institutions; energy, infrastructure and resources; technology; transport; life sciences and healthcare; and consumer markets.

www.nortonrosefulbright.com

NORTON ROSE FULBRIGHT

NORTON ROSE FULBRIGHT

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3,000 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa.

nortonrosefulbright.com