NORTON ROSE FULBRIGHT

International Comparative Legal Guides

Practical cross-border insights into digital health law

Digital Health 2024

Fifth Edition

Contributing Editor

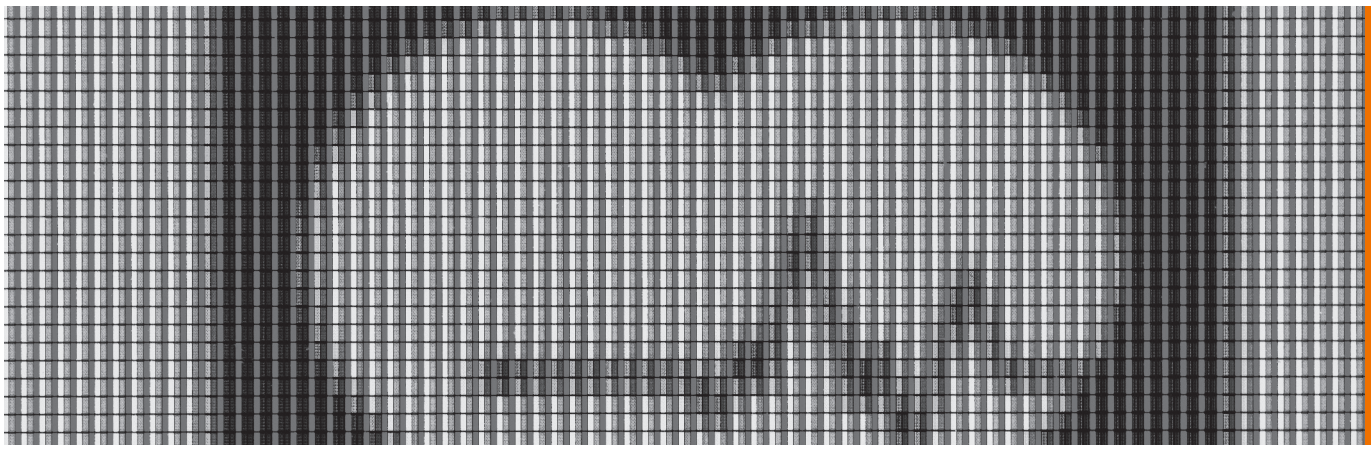
Roger Kuan

US Head of Digital Health and Precision Medicine Practice

Norton Rose Fulbright

ICLG.com

COMPARE & RESEARCH THE LAW, WORLDWIDE.



ISBN 978-1-83918-326-3
ISSN 2633-7533

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

Publisher
James Strode

Production Deputy Editor
Maya Tyrrell

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
Fraser Allan

Strategic Partners

International Comparative Legal Guides

Digital Health 2024

Fifth Edition

Contributing Editor:
Roger Kuan
Norton Rose Fulbright

Introductory Chapter

Expert Analysis Chapters

Q&A Chapters

From the Publisher

Dear Reader,

Welcome to the fifth edition of *ICLG – Digital Health*, published by Global Legal Group.

This publication provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to digital health laws and regulations around the world, and is also available at www.iclg.com.

This year, the *Guide* has an introductory chapter which provides an overview of digital health.

In addition, two expert analysis chapters cover investing and diligence in healthcare solutions, and emerging trends in the global regulation of digital health.

The question and answer chapters, which in this edition cover 22 jurisdictions, provide detailed answers to common questions raised by professionals dealing with digital health laws and regulations.

As always, this publication has been written by leading digital health lawyers and industry specialists, for whose invaluable contributions the editors and publishers are extremely grateful.

Global Legal Group would also like to extend special thanks to contributing editor Roger Kuan of Norton Rose Fulbright for his leadership, support and expertise in bringing this project to fruition.

James Strode
Publisher
Global Legal Group

International Comparative Legal Guides

Introduction

Norton Rose Fulbright
Johnson & Johnson

Roger Kuan

David Wallace

What is Digital Health?

The rapid convergence of digital technologies with healthcare over the past five years (even prior to the COVID-19 pandemic) has transformed how healthcare is delivered to the masses. The promise of digital technologies continues to transform the healthcare delivery model from a traditional model based on a "one size fits all" practice of medicine that was characterised by a provider-centric approach with information silos, to a new model that is focused on patient-centric treatment personalisation with high data accessibility and utilisation. The result is a highly personalised healthcare system that is focused on data-driven healthcare solutions and individualised delivery of therapeutics and treatments to patients using information technologies (IT) that enable seamless integration and communication between patients, providers, payors, researchers and health information depositories. A November 2020 report by Precedence Research published on *GlobeNewsWire* indicates that the global digital health market is poised to grow at a compound annual growth rate of around 27.9% over the next seven years to reach approximately US$833.44 billion by 2027.[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; Wyoming; and 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 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. https://www.globenewswire.com/news-release/2020/11/17/2128470/0/en/Digital-Health-Market-Size-to-Hit-Around-US-833-44-bn-by-2027.html#:~:text=The%20global%20digital%20health%20market,27.9%25%20from%202020%20to%202027
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
555 California Street
Suite 3300
San Francisco, 94104
California
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

A New Era of Investing and Diligence in Healthcare Solutions


Jason Novak


Dr. Milad Alucozai


Nathanael Green

Norton Rose Fulbright

Introduction

Investing in emerging biotech and healthcare companies is a unique venture that requires knowledge and understanding of both the technology and the team behind the science. Here, we address themes for what makes a startup-investor team productive and how these themes lead to valuable companies. These themes should be considered by investors and founders alike (and their legal counsel) to consider each role in the bigger picture. This helps both sides' understanding of what their counterpart considers and how they can shape their strategy to maximise the team's output.

A New Era of Investing

Invest in the team

Investing in the team, not necessarily the tech itself, is often a predictor of success. In healthcare, it can be hard to predict the value of something that may have a binary outcome – i.e., an approval of a drug, diagnostic, or device. So, investing in the team can drive success. Second-place teams are not exciting.

Entrepreneurs frequently undervalue the significance of storytelling. Good investors can dedicate days to hearing pitches. A large number of these pitches immediately delve into technical aspects, market, and product innovations, but they neglect the entrepreneur's background. It is more important, especially at an early stage, for the founders to articulate why they are the appropriate individuals for this venture at this moment, and how their unique experiences have brought them to this point. Successful entrepreneurs convey their journey to investors effectively. Consequently, it is worthwhile to invest time in creating a compelling narrative that will not be overlooked or forgotten.

Another key factor in finding a founder capable of going the distance is grit – the relentless determination that fuels a founder to persevere through challenges. It is a joy to work with exceptional founders who are achieving their visions in challenging conditions. Startups are tumultuous, and success is hard-earned. Grit is a key attribute that propels founders through these tumultuous obstacles, changes, and uncertainties. Gritty founders view hurdles as opportunities and setbacks as progress.

Non-dilutive funding

In the current funding environment, pursuing grants is a viable strategy that all founders should consider. Unfortunately, many founders and their investors overlook significant opportunities, failing to capitalise on these non-dilutive resources. A lack of commitment to non-dilutive funding can be a red flag for investors and, if it is not, it should be.

Applying for grants does more than just infuse much-needed capital into startups, extending their runway. It also serves as a testament to the resilience of the founders, as navigating the grant application process can be a challenging endeavor.

Moreover, securing a grant provides a form of market validation to all stakeholders. Grants are competitive. Receiving a grant implies that the startup has been evaluated and deemed worthy by a third-party organisation. This can enhance the credibility of the startup in the eyes of potential investors.

The use of active investors and board

Years ago, when speaking with a well-known venture capitalist (VC) about the scientific advancements of a local startup, the VC remarked that the technology was not scalable or interesting for his firm. Ironically, this was a company where he had led the investment and served on the board. His forgetfulness raised questions about the value of VCs sitting on numerous boards if they cannot recall the companies or their operations. Picking the wrong investor can be dead-weight to the company. However, the right investors can open doors, give advice, and help scale the company. Investors with real-world experience in the healthcare space can be invaluable resources to new companies that may not have the expertise or connections beyond their scientific sphere.

Thankfully, the healthcare sector is experiencing a healthy long-term correction. The departure of unfit VCs is beneficial, making room for new funds and allowing the good ones to shine. Despite a slight recession and the presence of a peculiar bubble filled with "zombie VCs" – those who take meetings without the intention to invest, those lacking dry powder to invest, or those intentionally slowing down to observe the situation – there are still great investments to be made. The emergence of specialist investors is driving this healthy transition. The

pools of capital and the finances are taking a little longer, but startups that prioritise getting validation data and a pathway to quality clinical data have been rewarded. Sticking to these fundamentals has been a blessing for this space.

Being an active investor

Productive investors are able to speak the language of their founders. It is not merely about understanding scientific jargon; it is about appreciating the journey of discovery, acknowledging the challenges, and articulating the transformative potential of biotech inventions. This ability is crucial in fostering collaborations and driving the commercial success of biotech innovations.

Productive investors also understand the underlying legal, regulatory, or commercial aspects needed for successful commercialisation. It is a common occurrence for large funds to seek outside input on common issues. The fact that these large, well-known funds reach out for outside advice indicates a lack of internal expertise. It suggests that they do not have someone within their organisation who can provide insights or make sense of these agreements.

This lack of in-house expertise is concerning, especially considering the size and reputation of these funds. It is alarming to think that these organisations, which manage substantial assets, do not have the necessary knowledge to fully comprehend the intricacies of these assets. This includes understanding the intellectual property (IP) and data associated with these assets.

It is important to note that this is not the case with all investing groups. Some organisations manage these aspects exceptionally well, demonstrating a deep understanding of the assets, the associated IP, and data. The experience of a founder can vary significantly depending on the investing group one is dealing with. It is a trade-off, and the level of expertise and understanding can fluctuate from one investor group to another. So, while some situations can be concerning, others can be quite reassuring.

A New Era of Diligence

Focus and understanding of IP

Founders must understand and appreciate two things: the IP behind their innovations; and the data (where relevant) that fuels innovation. A crucial lesson learned is the significant role that the technology transfer of IP and data from a university plays. An incorrect agreement can hinder future financing, obstruct the signing of commercial agreements, and gradually lead to the demise of a company. Furthermore, while private grants can be excellent sources of funding, understanding the IP policies governing these grants is crucial to avoid costly licence fees.

The advice consistently given is that for any transaction to occur, it is not only important for the founders to understand it, but they should also be very thoughtful about where the IP goes and how it is shared. This is even more important than the transactional value of the deal because if the IP is not fundamentally secured, it could set the company up for failure in future agreements or other types of arrangements. This approach extends to data as a property right. The lack of understanding of data (and associated trained models) can lead to bad arrangements that serve as a hurdle to further development.

In the biotech world, for instance, if an asset is not secured – if there is not a solid composition-of-matter patent, or if the company is attempting to repurpose someone else's invention without success – it can lead to numerous complications. These issues might not seem significant when the company is small, but any degree of success or financing can instantly jeopardise the company if the foundational elements are not solidified.

Often, these are the reasons why companies fail. It is not necessarily because the technology was not good or the team was not competent. More often than not, it is due to overlooked aspects like these that catch people off guard. Therefore, it is imperative to address these issues early on to ensure the long-term success of the company. Exclusivity is king, and IP and data are two sources of exclusivity, particularly when pre-revenue or pre-launch.

Data rights

An increasing amount of energy is being focused on data-related matters. Who owns the rights to use, transact, and commercialise data and data sources is an important matter to address. Currently, more often than not, neither side of a deal possess a sufficiently sophisticated understanding of data-related matters. How data rights can be partitioned in order to serve both parties requires sophisticated understanding of (1) what the data contains and how the data *could* be used, (2) what levers exist to partition data, and (3) what implications exist for these decisions. What can, and often does, occur in a data (or data-related) deal, particularly in the healthcare and biotech sectors, is that there is a set of circumstances that can satisfy both sides, but neither side knows how to articulate and memorialise the language necessary to achieve that satisfaction. Instead, each side fights over everything (including the mundane), primarily based on the fear of "missing something".

As with many negotiations, one side, often the larger entity, will lead off with very one-sided data agreements, as they should. This is a negotiation. The problem occurs when smaller entities (i.e., startups) assume that partnering with a large company would be a dream come true, and sign without giving it much thought. That is the worst case. A more standard case is when both sides dedicate a vast majority of time to the legacy concerns, including up-fronts, royalty structures, milestone payments, and IP ownership. That can often come at the expense of sufficient focus on data rights. This can also lead to problems, particularly for the startup, that often needs the data as part of their platform or business model, but are not sufficiently experienced in data transactions.

This highlights why IP due diligence on data rights is important. There cannot be an assumption of knowledge in the investor community or on both sides of a transaction. Often, there needs to be someone who acts as the adult in the room. There have been instances when outside counsel for one party must educate both sides before negotiation starts. Without this, the resulting imbalance can lead to issues in getting a deal done.

Differences between traditional tech IP and bio/pharma IP

The intersection of technology and biology, particularly with the advent of Machine Learning and Artificial Intelligence, presents unique challenges due to the differing business models. The importance of IP in biotech, given its long time-window from conception to ultimate approval, contrasts with traditional tech where IP becomes less relevant as newer versions emerge post-patent issuance.

To this, generally speaking, legacy technologies (tech, biotech, automotive, food, healthcare, etc.) are well comprehended within the legal community. However, when these technologies are merged, the ability to proactively address issues that have not yet surfaced is not a natural tendency for the legal community, which are typically reactive rather than proactive. This is especially evident when tech and biotech, with their distinct business models and philosophies, are brought together.

In biotech, IP is paramount as it could potentially be the only asset for a decade while waiting for a molecule to reach the market.

On the other hand, in tech, the transient nature of innovation means that by the time a patent is issued, the focus may have already shifted to the sixth version, rendering the first version, covered by the patent, less important or not important at all.

Further, when these ideologies are merged, whether led by tech or biology, there are inherent deficiencies due to the starkly different cultures. This is particularly true when meeting in the middle, where neither side fully understands the other. A common assumption is that larger companies, such as those that focus on traditional tech or biology spaces, possess more sophistication on a subject. However, this is often not the case when venturing into an emerging or converging space outside of the legacy space. In such situations, it is harder for a large company – an aircraft carrier – to maneuver compared to a small company – a speedboat. During negotiations about a technology unfamiliar to the big company, the small company often assumes a level of knowledge on the part of the big company. This creates a paradox where the large company must project confidence while simultaneously grappling with ignorance, making negotiations even more challenging.

Despite these challenges, numerous effective solutions have emerged. Looking ahead, key developments in biotech, digital health, precision medicine, and diagnostics over the next five years paint an interesting picture. Reflecting on the past few years, it is clear that regardless of how good a solution is, understanding regulatory policy, IP/data strategy, and care delivery is crucial. Recognising that startups cannot operate in isolation and that federal government decisions impact their operations has been an enlightening realisation. Consequently, more companies are becoming conscious of this reality, which was not a common consideration five or six years ago. Additionally, due to market trends, more pitches are being received where people are already contemplating exit strategies and transactions, adding another layer of complexity to the landscape.

It continues to be an interesting world. As more legacy technologies merge, we will all become more effective in proactively addressing issues on the horizon. However, we are currently in a nascent state of convergence technology. Issues are new. Strategies are evolving. In this uncertain time of innovation and economics, having the right team around you to address these futuristic issues will put you in great stead as your company or business grows.

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

Nathanael Green is an associate in Norton Rose Fulbright's Houston office. His practice focuses on developing IP portfolios mainly for universities and life science companies. Nathanael counsels clients on portfolio strategies, which include preparing and prosecuting patent applications and developing patent landscape opinions. Nathanael has experience with technologies across the life science space, including cellular therapies, gene therapies, small molecules, diagnostic assays, medical devices, organic chemistry and drug screening.

Norton Rose Fulbright
1301 McKinney, Suite 5100
Houston, Texas, 77010-3095
USA

Tel: +1 713 651 5422
Email: nathanael.green@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/nathanael-green-phd-05433757

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

Recent Updates on Emerging Trends in the Global Regulation of Digital Health: Fragmented Frameworks Continue Striving to Catch Up With Technological Advancement

Latham & Watkins


Eveline Van Keymeulen


Elizabeth Richards


Nicole Liffrig Molife


Oliver Mobasser

Introduction/Overview

Continued advances in healthcare technology create an enormous opportunity to enhance healthcare delivery and accessibility, reduce healthcare costs, and advance public health as a whole. Digital health technologies are becoming increasingly prevalent and are being utilised in innovative ways that benefit both patients and providers. For example, these technologies are changing the dynamics of care delivery through platforms like telehealth, transforming when, where, and how patients receive care. They also facilitate broader patient involvement in clinical research through "decentralisation" of clinical trials, allowing for remote patient monitoring ("RPM") to collect health-related data at home. Advancements in digital health have also established new ways or mechanisms to document and transfer electronic health records and facilitate correspondence between providers. These technologies have advanced the capability to detect early, sub-clinical signs of disease, aiding providers in offering preventive care or treatment sooner. Digital health technologies have also been used to promote general health and wellness, such as through mobile applications and wearables intended for everyday use. Therefore, the scope for digital health applications is vast and holds great potential, paving the way for innovative solutions in patient care, disease management, and health system efficiency that could revolutionise the medical field.

The proliferation and implementation of digital health tools, however, have been moderated by laws and regulations that predate these novel approaches to healthcare using digital technologies. Consequently, government and regulatory bodies are faced with the challenge of reconciling the rigid enforcement of their established legal structures with the evolving landscape of digital health, all while fostering ongoing progress in the sector. In this chapter, we discuss certain key legal constructs that digital health companies and investors must consider, and the emerging legal trends impacting applications of digital health in the United States ("US"), European Union ("EU"), and United Kingdom ("UK").

Key Legal Constructs for Digital Health Companies

Medical device considerations

One of the key legal constructs that companies and investors in the digital health industry must consider is the framework applicable to medical devices across jurisdictions.

US

In the US, the Food and Drug Administration ("FDA") has the legal authority to regulate medical devices. The law defines a device to mean "an instrument, apparatus, implement, machine, contrivance, implant, *in vitro* reagent, or similar or related article, including any component, part, or accessory, which is" among other things, either "intended for use in the diagnosis of disease or other conditions or in the cure, mitigation, treatment, or prevention of disease" or "intended to affect the structure or any function of the body" and "does not achieve its primary intended purposes through chemical action" and is "not dependent on being metabolized for the achievement of [those] purposes".[1] Certain software functions that might otherwise fall within the scope of this broad definition fall within an exemption under the law and will not be deemed a device. For example, in general, a software function intended for "maintaining or encouraging a healthy lifestyle and [that] is unrelated to the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition" will not be regulated as a device.[2]

With the exception of those software functions deemed to be shielded from the FDA's medical device oversight by statute, the law paints a broad brush; it sweeps many digital health technologies, including certain software – which may not traditionally be viewed as a "device" or "product" – within the FDA's reach. Because the medical device framework was established prior to the relatively recent explosion in the development and use of digital health technologies, it is not tailored to the unique features of digital health and is often a poor fit. Indeed, the FDA and industry alike have recognised that the existing regulatory framework for medical devices can present a barrier to innovation and stifle or slow the utility and hamper the promise digital health may present for improving the public health.

With this construct in mind, the FDA has issued a variety of guidance documents designed to apply flexibility to this new class of technologies that might otherwise fall within its regulatory crosshairs. For example, the FDA has issued guidance on its approach to regulating device software functions and mobile medical applications,[3] general wellness products,[4] and clinical decision support software[5] in an effort to establish a clearer line between certain digital health technologies that are subject to FDA oversight and those that are not. In some cases, the FDA has applied a policy of enforcement discretion, noting that although the technology may technically constitute a medical device subject to FDA oversight, the FDA has declined to assert its medical device authority and apply medical device requirements over such technologies. Consistent with its increased attention to digital health, in September 2020 the FDA

announced the launch of its Digital Health Center of Excellence to establish a "comprehensive approach to digital health technology" to "set[] the stage for advancing and realizing the potential of digital health".[6] In January 2024, the FDA elevated the Digital Health Center of Excellence to a full office within the Office of Strategic Partnerships and Technology Innovation as an ongoing expansion in digital health.[7] Continuing with this trend, in October 2023, the FDA announced that it is establishing a Digital Health Advisory Committee, which will include core voting members with expertise in several key areas in digital health,[8] as well as non-voting representatives of industry interests.[9] The committee's members will be called on to advise FDA on issues relating to digital health technologies and the approach the FDA should take to regulating them.

The FDA has also engaged in a number of actions in recent years to address certain novel digital health technologies, including artificial intelligence and machine learning ("AI/ML") in medical applications.[10] Specifically, the FDA has proposed the establishment of a new regulatory framework to enable a more flexible approach to regulating these technologies, which may be designed to iterate and improve after commercialisation. The FDA has continued to expand on this framework by publishing in 2023 a guidance document focused on enabling applicants to submit a marketing application that seeks authorisation for certain anticipated changes to the product after marketing, even prior to initial marketing authorisation (a "predetermined change control plan"),[11] and the agency announced that it plans to publish several new AI/ML-related guidance documents in 2024.[12] Finally, in December 2023 the FDA issued a final guidance governing the use of digital health technologies for remote data acquisition in clinical investigations, the use of which has the potential to allow for further decentralisation of clinical trials.[13] The FDA issued draft guidance in May 2023 to assist the industry in mapping the existing regulatory landscape governing clinical trials – with the assumption that clinical trials take place at a physical clinical trial "site" – to the new world of decentralised studies, where some or all of the trial-related activities take place at locations other than clinical trial sites.[14] While these efforts are commendable, regulatory uncertainty remains and opportunities abound for the industry to play a role in shaping the resulting framework.

EU

Similarly, in the EU, regulatory authorities may consider digital health technologies to be regulated as devices, pursuant to Regulation (EU) 2017/745 on medical devices ("MDR") or Regulation (EU) 2017/746 on *in vitro* diagnostic medical devices ("IVDR"). The MDR and IVDR clarify that software that is intended by the manufacturer to be used for one of the medical purposes listed in these regulations will be classified as a medical device or *in vitro* diagnostic medical device, respectively. These regulations could therefore capture many digital health solutions, including software incorporating AI when intended for use for medical purposes. As such, to be placed on the EU market, these solutions must be compliant with general safety and performance requirements as a prerequisite for European conformity, or "CE" marking, without which medical devices, including *in vitro* diagnostic medical devices, cannot be marketed or sold in the EU. To guide manufacturers, the Medical Device Coordination Group has issued guidance on the qualification and classification of software under the MDR and IVDR,[15] and on Medical Device Software intended to work in combination with hardware or hardware components,[16] and the Manual on borderline and classification in the EU regulatory framework for medical devices contains many examples related to qualification of software and mobile applications.[17]

Today, more than 25% of medicines assessed by the European Medicines Agency ("EMA") incorporate a medical device component, which increasingly include digital technologies (such as "digital pills"). In its 2021 guideline, the EMA addressed the challenges related to the development of these combination products that use emerging technologies by recommending that developers engage with the relevant medicines authorities and notified bodies in a timely manner, e.g., by requesting formal scientific advice, or through an Innovation Office.[18]

As related to AI, on December 8, 2023, the European Parliament and Council reached political consensus on the world's first regulatory framework on AI ("AI Act") after protracted negotiations following the AI Act's initial publication of the initial proposal for the AI Act in April 2021. The AI Act is expected to enter into force in 2024, and the majority of the substantive requirements will apply two years later. The AI Act will apply to AI in all sectors, including the health sector. Under the AI Act, it is expected that most AI systems that are part of medical devices and *in vitro* diagnostic medical devices, or are themselves such products, will be classified as high risk and require a conformity assessment by a notified body (e.g., a device, such as a pacemaker, that uses an AI system to identify the user's normal cardiological parameters and thus monitor the proper functioning of the patient's heart). As most software-based medical devices and *in vitro* diagnostic medical devices are already subject to conformity assessment by MDR- or IVDR-notified bodies, there is a possibility they would have to undergo a second conformity assessment procedure under the proposed AI Act, which could lead to increased cost, resources, documentation and regulatory scrutiny. In addition, such a requirement could create additional constraints for those notified bodies designated under the MDR and IVDR, which are already experiencing enormous backlogs. While the agreed text has not yet been published or formally approved, given the overlap between the medical device and AI frameworks, it remains to be seen whether the AI Act will advance innovation in the digital health space, or ultimately stifle it. The EMA has recently published a draft reflection paper outlining the current thinking on the use of AI to support the safe and effective development, regulation and use of medicines, the consultation process on which ended on December 31, 2023.[19] The reflection paper primarily focuses on providing regulatory strategy guidance for pharmaceutical companies on the use of AI/ML in the lifecycle of medicinal products (including R&D, authorisation, and post-authorisation) but also covers the interplay between medical devices and medicines. Acknowledging the rapid development in this field, the reflection paper discusses the scientific principles relevant for regulatory evaluation when these emerging technologies are applied to support safe and effective development and use of medicine. It emphasises that further reflections are needed regarding advice on risk management as the impact of system malfunction or degradation of model performance can range from minimal to critical or even life-threatening.

UK

As a result of Brexit, the MDR and IVDR do not apply in Great Britain, though they are applicable in Northern Ireland pursuant to the Northern Ireland Protocol. On June 26, 2022, the UK Medicines and Healthcare products Regulatory Agency ("MHRA") published its response to a 10-week consultation[20] on the future regulation of medical devices in the UK. The aims of the consultation included exploring amendments to the current Medical Devices Regulations 2002 with a view to creating an innovative framework for regulating software and AI as medical devices. The new regime was originally scheduled to come into force in July 2023, but has recently been postponed

to July 2025. For the most part, the proposed changes in many of these areas align with the new EU regime under the MDR and IVDR.

With respect to AI, in contrast with the approach taken by the EU, on March 29, 2023, the UK government published a white paper entitled "A pro-innovation approach to AI regulation", which sets out the UK's proposal to not introduce new legislation, but instead to leverage existing regulatory frameworks and empower regulators to apply a principles-based approach to supervising AI applications within their remit (rather than introducing new legislation or a new AI regulatory body). The government is expected to publish its full response to the white paper consultation in early 2024, further detailing its proposed approach to AI regulation.

On October 17, 2022, the MHRA published guidance on "Software and AI as a Medical Device Change Programme – Roadmap",[21] a programme aiming to reform the regulation of these technologies and ensure that the regulatory requirements for software and AI are clear, and that patients are protected. The programme consists of proposals to make key reforms across the lifecycle of these products, including qualification, classification, pre- and post-market requirements, and cybersecurity.

As regulators in the US, EU and UK continue to refine their approaches to digital health technologies, including when and how such technologies should be regulated as medical devices, the legal and regulatory frameworks are likely to shift. This changing landscape can present difficulties for companies in the digital health industry when assessing the regulatory burdens that may apply across the lifecycle of their products and services. Furthermore, despite regulators' attempts to adapt to technological innovation in a flexible manner, future advancements in digital health may continue to outpace the legal frameworks, with regulators seemingly playing a constant game of catch-up.

Telehealth considerations

Digital health technologies that pertain to the delivery and use of telehealth to deliver care require a thorough evaluation of another set of healthcare regulatory laws outside of the FDA and comparable medical device regulations globally.

US

No uniform federal law governs the delivery of telehealth services. Instead, telehealth is regulated at state level, and digital health companies must evaluate a patchwork of state laws to understand the restrictions that impact how healthcare providers and healthcare entities use technology, and how each step in the care delivery model can be structured to comply with varying state laws. Because state standards were developed when care was predominantly provided through in-person encounters, state laws lag behind innovation and do not fully contemplate the range of available technology that is changing the healthcare delivery model.

Each state has developed its own licensing requirements and standards governing: (i) the general practice of telehealth and the ability for remote delegation, supervision, and prescription; (ii) whether the delivery of care can be synchronous or asynchronous; and (iii) the scope of clinical care, coordination and management that can be delivered digitally. Specialty societies are stepping in to shape the standards of practice and spur policy discussion relating to digital health and use of AI. For example, the American Medical Association ("AMA") has developed a Digital Health Implementation Playbook[22] and has defined the concept of "augmented intelligence", focusing on AI's assistive functions.[23] The AMA has also issued principles for augmented intelligence development, deployment and use, with the goal of advancing high-quality, clinically validated augmented intelligence in patient care.[24] A presidential executive order was issued in October 2023 designed to establish guidelines on the safe, secure and trustworthy development and use of AI in the healthcare sector, and recently a number of healthcare providers and payors organisations made voluntary commitments to advance AI technology safely and equitably.[25]

In addition, state licensing laws limit the geographic reach of licensed healthcare professionals ("HCPs") by requiring them to be licensed where the patient resides, unless the care was provided, for example, directly to another HCP (rather than to the patient) or in an emergency situation. The onset of the COVID-19 pandemic prompted states to temporarily loosen licensure restrictions on the practice of telehealth and apply waivers from these requirements, accelerating the use and acceptance of telehealth services and allowing HCPs to provide services to patients across state lines. However, many of the state waivers that were implemented during the pandemic expired and have not been extended, resulting in a setback in the advancements in telehealth that were gained over the past few years. Efforts to reduce these licensure barriers continue, including allowing for out-of-state licensure exemptions, providing for telehealth licensure pathways under certain circumstances, and continued expansion of state licensure compacts, such as the Interstate Medical Licensure[26] and Psychology Interjurisdictional Compact,[27] which are designed to streamline the licensing process for HCPs who wish to be licensed in multiple jurisdictions.

Lastly, leveraging technology to deliver remote care or augment an HCP's ability to diagnose and treat patients through AI implicates another set of laws, called state corporate practice laws. These laws generally prohibit lay, unlicensed entities from delivering healthcare or exercising undue influence or control over the delivery of healthcare services. These laws may require companies to implement certain corporate structures, operational models or other safeguards to ensure that HCPs maintain unfettered control over clinical decision-making.

EU

The European Commission defines telehealth as "the provision of healthcare services, through the use of [information and communications technology], in situations where the health professional and the patient (or two health professionals) are not in the same location" and involves "secure transmission of medical data and information, through text, sound, images or other forms needed for the prevention, diagnosis, treatment and follow-up of patients".[28] As in the US, the regulation of telehealth services in the EU remains fragmented, as such services are essentially regulated at a national level. The most relevant effort to regulate health services across the EU is Directive 2011/24/EU on patients' rights in cross-border healthcare (the "Cross Border Healthcare Directive"), which ensures continuity of care for European citizens across borders (e.g., e-prescribing) and dates back many years.

A 2018 European Commission market study on telemedicine concluded that "most telemedicine solutions are deployed at the national or regional level" and that "this is due to the significant differences in national regulations and social security schemes".[29] The study recommended that "EU countries… harmonize their legal frameworks in order to make solutions compatible and to enable cross-border telemedicine practices".[30] The recent European Commission proposal for a Regulation on the European Health Data Space included provisions seeking to harmonise and encourage cross-border telemedicine,[31] but

these provisions were removed by the European Council during the ongoing legislative process. Trilogue negotiations on the European Health Data Space commenced in December 2023, so it remains to be seen what position is ultimately reached on the proposals regarding telehealth. While recent developments at the EU level in this space remain limited, it is worth noting that in November 2022, the World Health Organization ("WHO") issued a consolidated telemedicine implementation guide, which provides an overview of the key considerations for implementing telemedicine globally.[32]

UK

No specific laws govern telehealth in the UK. However, the provision of health or social care (including by remote means) in England is primarily governed by the Health and Social Care Act 2008 and the Health and Care Act 2022. Similar legislation covers Northern Ireland, Scotland, and Wales. The Electronic Commerce (EC Directive) Regulations 2002 (the "eCommerce Regulations"), which impose certain requirements for the provision of online services, may also apply to the provision of telemedicine services.

The provision of health and social care is regulated on a regional basis by different agencies. For example, in England, the Care Quality Commission ("CQC") regulates telehealth providers under the regulated activity of "transport services, triage and medical advice provided remotely". Telemedicine service providers (including individuals or corporate entities) are required to register with CQC or the equivalent body in Northern Ireland, Scotland, and Wales.

While these regulators have authority over healthcare service providers (i.e., the individual or the entity), individual providers are also subject to licensing and enforcement by their professional bodies. In particular, the General Medical Council has licensing and enforcement authority in respect of doctors, and the General Pharmaceutical Council has such authority in respect of pharmacists. The obligation to be appropriately qualified and registered with a professional governing body applies regardless of whether the service is provided remotely or in person. As a result of Brexit, the "country-of-origin" principle under the eCommerce Regulations – which allow European Economic Area ("EEA") online service providers to operate in any EEA country, while only following relevant rules in the country in which they are established – and the rules on cross-border care from the Cross Border Healthcare Directive no longer apply. This means that professionals providing telemedicine services from the UK to patients in the EEA may also need to be licensed in the country where the patient is located.

Coverage and reimbursement considerations

Beyond the legal considerations applicable to compliance of digital health technologies with the medical devices framework and telehealth restrictions and requirements, companies must consider the laws and regulations applicable to coverage and reimbursement for their digital health technologies, or coverage and reimbursement of healthcare services provided using digital health technologies.

US

Coverage and reimbursement for health services that use digital health technologies (like telehealth) are often determined on a payor-by-payor basis, which can make it difficult for companies to navigate the payor landscape and achieve certainty with respect to payor adoption of their technologies. While the US does not have a single payor system that establishes uniform reimbursement and coverage for healthcare services that use digital health technologies, policies established by the Centers for Medicare & Medicaid Services ("CMS") – which administers Medicare, the nation's single-largest public insurance programme – are particularly important because they often influence coverage and payment policies adopted by other payors.

In recent years, CMS has expanded coding and payment policies for remote monitoring services and payment for certain software-based diagnostic tools. However, as a recent fraud alert issued by the Office of Inspector General signals,[33] RPM is under increased scrutiny by federal regulators and payors as utilisation of these services have grown. RPM and digital health companies should monitor these enforcement developments and coverage and utilisation restrictions that may be issued by payors this year, as well as monitor their operations and billing practices for compliance with Medicare, Medicaid and other payor requirements.

In addition, Congress and various federal and state agencies have continued to provide expanded flexibilities to enable coverage and reimbursement for telehealth services, including policies allowing certain telehealth services to be reimbursed at the same rate as equivalent in-person services. While some of these flexibilities have been extended through the end of 2024, pay and coverage parity for telehealth services is under review. The explosion of telehealth and digital health offerings in the US healthcare system because of these policies has been paralleled by an increasing number of enforcement actions, scrutiny by federal regulators, and the issuance of a special fraud alert around the use of telehealth services.[34] It is important that digital health companies stay abreast of this increased regulatory scrutiny, and the evolving regulatory scheme, as they structure their operations.

EU

The reimbursement landscape for digital health tools is fragmented across the EU, given that reimbursement decisions are made at a national or even regional level, and not by EU authorities. This poses particular challenges to both the manufacturers that are developing digital health technologies and the health authorities that are evaluating them. In particular, these authorities' traditional methods to evaluate products for coverage and reimbursement do not focus on aspects that are relevant to digital health technologies (e.g., interoperability, privacy, data security, and ethical considerations). Moreover, because these technologies are often updated more quickly than traditional devices (especially when incorporating AI/ML), they require similarly speedy evaluation decisions. As a consequence, national reimbursement schemes for digital health technologies are inconsistent across the EU, including with respect to the type of evidence that is accepted as sufficient, and little guidance is available to assist manufacturers in navigating the requirements. Certain countries have implemented specific frameworks for reimbursement decisions with respect to digital health technologies. Germany, for instance, is the first EU country to have recently implemented a "fast track" reimbursement for certain digital medical products, such as wearable devices or mobile applications.

The EU Health Technology Assessment ("HTA") Regulation (2021/2282) ("HTAR"), which for the first time introduces a permanent legal framework for joint HTA work (i.e., joint clinical assessments and scientific consultations) by EU Member States, is an important step toward a more uniform assessment of innovative high-risk medical devices, including digital health technologies. In preparing for the regulation's phased implementation from 2025 onwards, several national HTA bodies in Europe have recently joined forces with EU-level

organisations, such as the European Network for HTA, to develop recommendations on harmonised evaluation guidelines for digital medical devices. For instance, in October 2022, a European taskforce was launched by nine EU Member States with the objective to reach a mutual understanding between national HTA agencies for digital medical devices in order to harmonise assessment criteria and clinical evidence requirements and improve access to digital health technologies in the EU.[35]

UK

The National Health Service ("NHS") funds the majority of digital health products and services provided to patients in the UK. In addition, there exists a smaller, but growing, private healthcare sector, which is funded through private insurance or directly by patients. There are a number of routes for products to be made available for reimbursement by the NHS, including selling directly to NHS trusts or primary care organisations, or procurement through the NHS supply chain or public tenders. In addition, digital health products can undergo a technology appraisal from the National Institute for Health and Care Excellence ("NICE"), and the NHS is obligated to fund and resource treatments recommended by NICE.

The NHS has published a "guide to good practice for digital and data-driven health technologies",[36] which is designed to help innovators understand the NHS requirements when the NHS buys digital and data-driven technology. NICE has published the "Evidence standards framework for digital health technologies",[37] which describes the standards for digital health technologies to demonstrate their value in the UK healthcare system.

Data privacy and data use

Data and digital health go hand-in-hand, whether they involve the analysis of large and complex datasets by an AI/ML tool or the collection of an individual's health and lifestyle data through a wearable device. As such, navigating the complex and continually evolving web of privacy and cybersecurity laws is critical to the deployment of any digital health solution.

US

The Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009, and regulations implemented thereunder (collectively, "HIPAA") imposes privacy, security, and breach notification obligations on certain healthcare providers, health plans, and healthcare clearinghouses, known as "covered entities", as well as their "business associates" that perform certain services that involve creating, receiving, maintaining or transmitting individually identifiable health information referred to as "protected health information" ("PHI") for or on behalf of such covered entities, and their covered subcontractors. HIPAA requires covered entities and business associates to develop and maintain policies with respect to the protection of, use and disclosure of PHI, including the adoption of administrative, physical, and technical safeguards to protect such information, and certain notification requirements in the event of a breach of unsecured PHI.

The data protection landscape is rapidly growing and evolving on a state level. For example, the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act, and regulations promulgated thereunder (collectively, "CCPA"), requires companies that process information on California residents to make certain disclosures to consumers about their data collection, use, and sharing practices. CCPA also allows consumers to opt out of certain data sharing with third parties and exercise certain individual rights regarding their personal information, providing a private right of action for data breaches and penalties for noncompliance. Similar laws have been passed in other states and are continuing to be proposed at the state and federal level, reflecting a trend toward more stringent privacy legislation in the US.

The Federal Trade Commission ("FTC") and many state Attorneys General continue to enforce federal and state consumer protection laws against companies for online collection, use, dissemination, and security practices that appear to be unfair or deceptive. Recent FTC guidance on AI/ML has focused on the potential risks to fair and transparent consumer transactions represented by opaqueness in automated decision-making and predictive analytics. The FTC is also concerned about misleading representations to consumers regarding a company's data collection and handling practices that underwrite the datasets on which algorithms are trained. The FTC has highlighted the particular risks to healthcare consumers in unfair or deceptive data practices leveraging AI as an area of developing regulatory concern. Of particular relevance to the digital health sector are potential harms to patients introduced as a result of improper oversight when AI tools are used for automated decision-making, leading to discriminatory clinical or treatment outcomes.

Further, on December 13, 2023, the U.S. Department of Health and Human Services through the Office of the National Coordinator for Health Information Technology issued its final Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing rule ("HTI-1 Rule") that establishes transparency requirements for the use of AI/ML in certified health IT. The HTI-1 Rule is focused on mitigating bias and inaccuracy in healthcare AI/ML tools and will require healthcare AI developers of certified health IT to provide more information about their AI/ML products to users, including information about funding sources, data used to train the model, intended use cases, external validation processes and description of approaches to manage, reduce, or eliminate bias.

EU

In the EU, the processing of personal data is primarily governed by Regulation (EU) 2016/679 ("GDPR"). The GDPR imposes comprehensive data-privacy compliance obligations in relation to the use or "processing" of information relating to an identifiable living individual or "personal data". The GDPR applies not only to entities established in the EU, but also to entities established outside the EU if they offer goods or services to EU individuals or monitor their behaviour. Organisations deploying digital health solutions to individuals across the EU and the UK may therefore need to comply with both the GDPR and the UK data protection regime. While the GDPR was intended to harmonise data protection laws across the EU, national implementing laws diverge in certain areas, such as the processing of personal data for public health or scientific research purposes. Therefore, companies must navigate not only the GDPR, but also national implementing and supplementary legislation, as well as legal, ethical and professional rules designed to protect patient confidentiality.

Although the GDPR was enacted to be technology-neutral, the advent of the digital health industry has led to challenges in the interpretation and application of the GDPR. For example, some digital health applications, such as wearables, have led to questions on the distinction between health data (which is considered "special-category data" under the GDPR and subject to enhanced protections) and other non-health "lifestyle"

data. This distinction, in turn, leads to potential compliance challenges, such as identifying appropriate legal bases for processing such health data and other personal data under the GDPR and ensuring that individuals are adequately informed of the processing of their data.

Other applications of digital health, such as AI/ML algorithms, have raised difficult questions regarding transparency and how data subjects can be informed in easy-to-understand terms of how the algorithm processes their data. Where personal data has been used to train an algorithm, withdrawal of a subject's consent (where consent has been used as the legal basis for such processing) to limit further use of their data may not be practical or possible and could affect the integrity of the algorithm. In such cases, the developer will need to consider whether it can continue to legitimately use that data, such as whether it has been effectively anonymised or aggregated. Ensuring data accuracy and the absence of bias are also key considerations for these types of tools.

Another increasingly tricky area for digital health operators is in relation to international data transfers. Where personal data are transferred from the EU to a country that is not considered to provide an "adequate" level of protection for the data, such transfer is prohibited unless a relevant derogation applies or certain safeguards are implemented. As a result of EU caselaw, complexity and uncertainty remain regarding such transfers, particularly in relation to transfers to the US.[38] The shifting sands of data transfers can be difficult to navigate and companies must pay close attention to the complex data flows that are often involved in digital health solutions in light of the legal developments governing such transfers.

Many digital health solutions, such as wearables and apps, may use cookies or other tracking technologies. While cookies that are strictly necessary for the device, site, or app to function correctly can be used without opt-in consent, others such as analytics or advertising trackers will require specific opt-in consent under EU Directive 2002/58/EC and national implementing laws, which may not be straightforward depending on the nature of the device. User data collected from devices is also subject to the GDPR. The use of cookies, tracking technologies, and user profiling is subject to increasing regulatory scrutiny and enforcement, particularly around the use of individuals' data for marketing and advertising.

Beyond the general requirements to ensure the security of personal data in the GDPR, there is a trend toward increasing regulation of cybersecurity through sector-specific or device-specific rules. For example, the MDR requires the manufacturing of certain devices to take into account information security principles. In addition, on November 28, 2022, the EU adopted Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the EU ("NIS-2 Directive"). The NIS-2 Directive establishes cybersecurity risk-management measures and reporting requirements for critical sectors, including manufacturers of medical devices. The draft EU Cyber Resilience Act, for which the European Parliament and Council reached provisional agreement on November 30, 2023, also proposes a framework of consistent security standards for digital products, applicable through the whole product lifecycle.

In parallel with the trend toward increased regulation and scrutiny, there is a trend toward enabling greater sharing and reuse of data, particularly for research and innovation. For example, on May 3, 2022, the European Commission launched its proposal for a Regulation for the European Health Data Space to "unleash the full potential of health data", facilitating the systematic digitisation of health records and secondary use of clinical data for research purposes. In addition, the EU Data Act, which was adopted by the European Parliament and Council in November 2023, regulates the sharing and use of data generated by connected devices, includes new rights for users of connected services, introduces data portability obligations, imposes restrictions on the use of user data, and regulates data sharing contracting.

Across the EU, there is a trend toward increasing enforcement of data protection laws and ever-larger fines. There is also increasing scrutiny and enforcement from a broader range of regulators – including data protection regulators, consumer protection authorities, and competition regulators – and increasing coordination efforts around data and digital platforms. At the same time, there is increasing momentum for policies and proposals designed to unlock data for research purposes, including for the development of AI and other digital health tools with the potential to advance healthcare.

UK

Following Brexit, the GDPR has been mirrored in UK law as the "UK GDPR", which together with the Data Protection Act 2018 form the UK's data protection regime. The UK Information Commissioner's Office has introduced specific data-transfer mechanisms to safeguard transfers of data out of the UK, namely the International Data Transfer Agreement and the International Data Transfer Addendum to the EU's standard contractual clauses.

The UK government has proposed wide-ranging reforms to UK data protection laws, set out in the UK Data Protection and Digital Information Bill (which was introduced to the House of Commons in March 2023 and at the time of writing is being reviewed by the House of Lords). The bill largely maintains the GDPR framework in UK law, albeit with modifications reflecting the government's intention to move away from prescriptive requirements and toward a more risk-based approach. While the UK has signalled a more business-friendly and flexible approach, which would be welcomed by operators in the digital health sector, it remains uncertain where the post-Brexit UK privacy landscape will land.

On June 29, 2022, the UK government published a policy paper titled "A plan for digital health and social care",[39] which sets out its far-reaching plans for the digital transformation of health and social care in England. The plan includes proposals for the systematic digitisation of health and social care records, and the creation of a life-long health and social care record. The proposal also aims to equip the NHS with the capacity to develop image-sharing and other technical capabilities based on AI, to enable "digitally supported diagnoses" and to establish a network of trusted research environments to support research and development.

Conclusion

Digital health companies must stay attuned to the emerging trends in the global regulation of these technologies, with the recognition that the frameworks are continuing to evolve. As demonstrated in the US, EU, and UK, a myriad of legal requirements create a spider's web for companies and investors to carefully navigate in order to avoid compliance issues and maintain momentum in a competitive marketplace. By remaining aware of the key legal constructs and staying abreast of proposed changes in these frameworks, stakeholders can play a part in shaping the legal regimes applicable to their digital health solutions. Moreover, they can reduce the risk of a compliance misstep, which may be more likely in an industry in which technological advancements outpace the legal frameworks and innovators, in many cases, operate in uncharted territory under the law.

Endnotes

1. 21 U.S.C. § 321(h)(1) (2022).
2. Id. § 360j(o).
3. U.S. Food & Drug Admin. (FDA), Policy for Device Software Functions and Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff (2022), https://www.fda.gov/media/80958/download
4. U.S. FDA, General Wellness: Policy for Low Risk Devices: Guidance for Industry and Food and Drug Administration Staff (2019), https://www.fda.gov/media/90652/download
5. U.S. FDA, Clinical Decision Support Software: Guidance for Industry and Food and Drug Administration Staff (2022), https://www.fda.gov/media/109618/download
6. U.S. FDA, *Digital Health Center of Excellence*, https://www.fda.gov/medical-devices/digital-health-center-excellence (last visited Jan. 21, 2023); U.S. FDA, *About the Digital Health Center of Excellence*, https://www.fda.gov/medical-devices/digital-health-center-excellence/about-digital-health-center-excellence (last visited Feb. 12, 2024).
7. U.S. FDA, FDA Elevates Office of Strategic Partnerships and Technology Innovation to Super Office in CDRH (Jan. 24, 2024), https://www.fda.gov/medical-devices/medical-devices-news-and-events/fda-elevates-office-strategic-partnerships-and-technology-innovation-super-office-cdrh
8. Request for Nominations for Voting Members for the Digital Health Advisory Committee, 88 Fed. Reg. 70672 (Oct. 12, 2023).
9. Request for Nominations of Individuals and Industry Organizations for the Digital Health Advisory Committee, 88 Fed. Reg. 70675 (Oct. 12, 2023).
10. See, *e.g.*, U.S. FDA, *Artificial Intelligence and Machine Learning in Software as a Medical Device*, https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device (last visited Feb. 12, 2024).
11. U.S. FDA, Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine Learning (AI/ML)-Enabled Device Software Functions (April 2023), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial
12. U.S. FDA, CDRH Proposed Guidances for Fiscal Year 2024 (FY2024), https://www.fda.gov/medical-devices/guidance-documents-medical-devices-and-radiation-emitting-products/cdrh-proposed-guidances-fiscal-year-2024fy2024 (last visited Feb. 12, 2024).
13. U.S. FDA, Digital Health Technologies for Remote Data Acquisition in Clinical Investigations (Dec. 2023), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/digital-health-technologies-remote-data-acquisition-clinical-investigations
14. U.S. FDA, Decentralized Clinical Trials for Drugs, Biological Products, and Devices (May 2023), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/decentralized-clinical-trials-drugs-biological-products-and-devices
15. Med. Device Coordination Group (MDCG), Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR (2019), https://health.ec.europa.eu/system/files/2020-09/md_mdcg_2019_11_guidance_qualification_classification_software_en_0.pdf
16. Med. Device Coordination Group (MDCG), Guidance on MDSW intended to work in combination with hardware or hardware components (2023), https://health.ec.europa.eu/system/files/2023-10/md_mdcg_2023-4_software_en.pdf
17. Eur. Comm'n, Manual on Borderline and Classification in the EU Regulatory Framework for Medical Devices (2022), https://health.ec.europa.eu/latest-updates/manual-borderline-and-classification-community-regulatory-framework-medical-devices-september-2022-2022-09-07_en
18. European Medicines Agency (EMA), Guideline on Quality Documentation for Medicinal Products When Used with a Medical Device (2021), https://www.ema.europa.eu/en/documents/scientific-guideline/guideline-quality-documentation-medicinal-products-when-used-medical-device-first-version_en.pdf
19. EMA, Draft reflection paper on the use of artificial intelligence in the lifecycle of medicines (2023), https://www.ema.europa.eu/en/documents/scientific-guideline/draft-reflection-paper-use-artificial-intelligence-ai-medicinal-product-lifecycle_en.pdf
20. Medicines and Healthcare Regulatory Products Regulatory Agency (MHRA), Consultation on the Future Regulation of Medical Devices in the United Kingdom (2021), https://www.gov.uk/government/consultations/consultation-on-the-future-regulation-of-medical-devices-in-the-united-kingdom
21. MHRA, Software and AI as a Medical Device Change Programme – Roadmap (2022), https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme/software-and-ai-as-a-medical-device-change-programme-roadmap
22. American Medical Association (AMA), *Digital Health Implementation Playbook Series*, https://www.ama-assn.org/practice-management/digital/digital-health-implementation-playbook-series (last visited Jan. 8, 2024).
23. AMA, *Augmented Intelligence in Medicine*, https://www.ama-assn.org/practice-management/digital/augmented-intelligence-medicine#:~:text=The%20AMA%20House%20of%20Delegates%20uses%20the%20term%20augmented%20intelligence,intelligence%20rather%20than%20replaces%20it (last visited Jan. 8, 2024).
24. AMA, Policy: *Augmented Intelligence in Health Care*, https://www.ama-assn.org/system/files/2019-08/ai-2018-board-policy-summary.pdf (last visited Jan. 8, 2024); AMA, *Principles for Augmented Intelligence, Deployment, and Use*, https://www.ama-assn.org/system/files/ama-ai-principles.pdf (last visited Jan. 8, 2024).
25. Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence (October 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ Delivering on the Promise of AI to Improve Health Outcomes (December 2023), https://www.whitehouse.gov/briefing-room/blog/2023/12/14/delivering-on-the-promise-of-ai-to-improve-health-outcomes
26. Interstate Medical Licensure Compact, https://www.imlcc.org/ (last visited Jan. 8, 2024).
27. Psychology Interjurisdictional Compact (PSYPACT), https://psypact.org/page/About (last visited Jan. 8, 2024).

28. Eur. Comm'n, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Telemedicine for the Benefit of Patients, Healthcare Systems and Society (2008), COM(2008)0689 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52008DC0689
29. Eur. Comm'n, Market Study on Telemedicine (2018), https://health.ec.europa.eu/system/files/2019-08/2018_provision_marketstudy_telemedicine_en_0.pdf
30. *Id.*
31. Eur. Comm'n, Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space (2022), COM(2022) 197 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197 (The original Article 8 set out that: "If a Member State accepts the provision of telemedicine services, it shall, under the same conditions, accept the provision of similar services by healthcare providers located in other Member States.").
32. World Health Org. (WHO), Consolidated Telemedicine Implementation Guide (2022), https://www.who.int/publications/i/item/9789240059184 (last visited Jan. 26, 2023).
33. Office of Inspector General, U.S. Dept. of Health and Human Services (HHS), Consumer Fraud Alert: Remote Patient Monitoring (November, 2023), https://oig.hhs.gov/fraud/consumer-alerts/consumer-alert-remote-monitoring/
34. HHS, Special Fraud Alert: OIG Alerts Practitioners To Exercise Caution When Entering Into Arrangements With Purported Telemedicine Companies (2022), https://oig.hhs.gov/documents/root/1045/sfa-telefraud.pdf
35. Haute Autorité de Santé (HAS), Towards a European Evaluation Framework for Digital Medical Devices (DMDs) in the European Union — Launch of a European Taskforce (2022), https://www.has-sante.fr/jcms/p_3382241/en/towards-a-european-evaluation-framework-for-digital-medical-devices-dmds-in-the-european-union-launch-of-a-european-taskforce (last visited Jan. 26, 2023).
36. Dept. of Health and Social Care (DHSC), U.K. Nat'l Health Serv., A Guide to Good Practice for Digital and Data-Driven Health Technologies (2021), https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology (last visited Jan. 30, 2023).
37. Nat'l Inst. for Health and Care Excellence (NICE), Evidence Standards Framework for Digital Health Technologies (2022), https://www.nice.org.uk/about/what-we-do/our-programmes/evidence-standards-framework-for-digital-health-technologies (last visited Jan. 30, 2023).
38. On October 7, 2022, President Biden signed an Executive Order on 'Enhancing Safeguards for United States Intelligence Activities,' which introduced new redress mechanisms and binding safeguards to address the concerns raised by the Court of Justice of the EU in relation to data transfers from the EEA to the US and which formed the basis of the new EU-US Data Privacy Framework ("DPF"), as released on December 13, 2022. The European Commission adopted its Adequacy Decision in relation to the DPF on July 10, 2023, rendering the DPF effective as an EU GDPR transfer mechanism to U.S. entities self-certified under the DPF. On October 12, 2023, the UK Extension to the DPF came into effect (as approved by the UK Government), as a UK GDPR data transfer mechanism to U.S. entities self-certified under the UK Extension to the DPF.
39. DHSC, U.K. Nat'l Health Serv., A Plan for Digital Health and Social Care (2022), https://www.gov.uk/government/publications/a-plan-for-digital-health-and-social-care/a-plan-for-digital-health-and-social-care (last visited Jan. 30, 2023).

Eveline Van Keymeulen advises multinational companies and start-ups in the pharmaceutical, biotech, medical devices and digital health sectors on a broad variety of complex European, domestic and cross-border regulatory matters, including clinical trials, product approvals, regulatory incentives, market access, promotion and advertising, post-market obligations and general compliance matters. Eveline is widely recognised for her regulatory life sciences expertise by *Chambers* (2020–2022), *The Legal 500* (2018–2022) and *Who's Who Legal Life Sciences* (2016–2022). She was voted European "Advisory Lawyer of the Year" by *LMG Life Sciences* (2021) and won their "Impact Case of the Year" award (2021–2022) for her work in the groundbreaking CJEU Kanavape case, for which she equally received the *Financial Times* European Innovative Lawyer Award (2022).

Latham & Watkins
Boulevard du Régent, 43–44
Brussels, B-1000
Belgium

Tel: +32 2 788 6000 / +33 1 4062 2060
Email: eveline.vankeymeulen@lw.com
LinkedIn: www.linkedin.com/in/evelinevankeymeulen

Elizabeth Richards advises clients in all facets of oversight and regulation by the FDA, helping clients navigate regulatory frameworks governing the digital health and medical device, pharmaceutical, biotechnology, food, dietary supplement and cosmetic industries. She is attuned to her clients' business objectives while guiding them through compliance, enforcement, transactional and legislative matters, traversing the legal labyrinth required to bring new products to market and maintain compliance once commercialised. Her practice spans all stages of the product life cycle, and she has been recognised as a leading industry lawyer by multiple publications, including *Chambers USA*, *The Legal 500 US*, *LMG Life Sciences* and *The Diversity Journal*.

Latham & Watkins
555 Eleventh Street, NW, Suite 1000
Washington, D.C., 20004
United States

Tel: +1 202 637 2130
Email: elizabeth.richards@lw.com
LinkedIn: www.linkedin.com/in/elizabeth-richards-94972271

Nicole Liffrig Molife advises emerging companies as well as commercial companies in the digital health, pharmaceutical, medical device and technology sector. She leverages her deep knowledge of fraud and abuse laws, as well as telehealth and other healthcare regulatory laws to guide companies as they develop their product development and launch strategies and business models, providing solutions that mitigate regulatory risk while fostering innovation. Nicole's practice includes counselling on sales and marketing activities and relationships with referral sources, evaluating industry collaborations, structuring key commercial agreements at all stages of development and advising on life sciences transactions.

Latham & Watkins
555 Eleventh Street, NW, Suite 1000
Washington, D.C., 20004
United States

Tel: +1 202 637 2121
Email: nicole.liffrig@lw.com
LinkedIn: www.linkedin.com/in/nicole-liffrig-molife

Oliver Mobasser advises multinational pharmaceutical, biotechnology, medical technology and digital health companies and their investors on complex licences, collaborations, acquisitions, divestments, commercial contracts, and other IP and data-focused matters and transactions.

Latham & Watkins
99 Bishopsgate
London, EC2M 3XF
United Kingdom

Tel: +44 20 7710 4738
Email: oliver.mobasser@lw.com
LinkedIn: www.linkedin.com/in/oliver-mobasser

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.

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 Therapeutic Goods Administration ('TGA'), regulates some digital health technologies as medical devices.

1.2 What are the key emerging digital health technologies 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.
- Big Data Analytics: use of historic data to provide consumers with tailored healthcare pathways and a better understanding of medication use.
- Predictive technology: the use of algorithmic or data-driven software to guide further preventive or diagnostic testing for patients.
- Telehealth: delivery of support by healthcare practitioners without the need for face-to-face appointments. In December 2021, the Federal Government announced that it would allocate A$106 million over four years to support permanent telehealth services. Additionally, since 1 January 2022, patient access to telehealth services has been supported by ongoing Medicare Benefits Schedule ('MBS') arrangements.
- My Health Records: digitisation of health records to improve the quality and availability of health information.
- 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.
- Secure Messaging: facilitating the secure, encrypted exchange of information between health professionals.

1.3 What are the core legal issues in digital health for your jurisdiction?

The core legal issues in digital health in Australia are applicability of and compliance with the regulatory framework and issues regarding privacy and data security. As digital health technologies develop and become more prominent, the means by which sensitive health data is collected, stored and shared must reflect this development. Following a recent high-profile privacy breach at a major health insurer, there is a heightened focus on ensuring digital health data is stored securely so as to prevent unauthorised access.

While the Australian digital health market is certainly growing post-COVID, the legislative and regulatory schemes are not yet sophisticated enough to deal with the nuanced issues arising in this market. To address this nuance from a privacy perspective, the Australian Government has undertaken a thorough review of Australia's principal privacy legislation, the *Privacy Act 1988* (Cth) ('Privacy Act'). Amendments to the Privacy Act are still awaited, with the earliest amendments expected in mid-2024.

1.4 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).

More generally, it has been estimated that AI could contribute more than A$20 trillion to the global economy by 2030.

1.5 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 Telstra Health, Medical Director, Best Practice, Genius Solutions and Alcidion.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

There is a lack of sophistication in Australia's digital health regulatory framework. The current legislation that is broad enough to apply to digital health includes the *Therapeutic Goods Act 1989* (Cth) ('TG Act'), the *Therapeutic Goods (Medical Devices) Regulations 2002* (Cth) ('TG Regulations') and the *My Health Records Act 2012* (Cth) ('My Health Records Act').

The TG Act establishes the national controls which relate to the quality, safety, efficacy and availability of therapeutic goods that are used in Australia. It provides a uniform approach for all states and territories to adopt. The term therapeutic goods is given a broad definition and includes software-based medical devices and other digital health technologies. The level of regulation for these devices is dependent upon the disease they are designed to assist with, its 'risk rating' and severity of the consequences if the device were to fail. A number of items of software, such as those designed to assist in healthcare practice management, or clinical workflow management, are excluded from regulation in Australia. However, the system continues to suffer from a lack of refinement to cover emerging technologies. This creates difficulties in confirming which products need to be registered and to what standard, and what restrictions might be placed on their marketing, promotion and supply. The Australian regulatory framework continues to take steps to better align with the EU Medical Devices Regulation. It also suggests that, in certain cases, dialogue with the TGA may be a prudent option.

The My Health Record Act enables the operation of a national public health patient information system, by which health practitioners can access health records of individuals through a digital sharing platform. It is a singular platform, and is the only one of its kind. It relates solely to the processes pertaining to the My Health Record, which is a secure digital record of an individual's healthcare information. Operation of the My Health Records Act is supported by the *My Health Records Regulation 2012* (Cth) and the *Healthcare Identifiers Act 2010* (Cth).

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Despite its general application, the Privacy Act applies 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, 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 Records scheme must be stored in Australia and under no circumstances is to be disclosed to cross-border entities.

Australia's consumer regulatory scheme, the *Competition and Consumer Act 2010* (Cth) ('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 which 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 which 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 regulatory schemes apply to consumer healthcare devices or software in particular?

To the extent that a consumer healthcare device or software is a medical device, it will need to conform to the TG Act and the TG Regulations. The specific nature of the compliance requirements differs based on the 'class' of the device. Medical devices are classified with regard to their intended purpose. In particular, the classification rules take into account the degree of invasiveness in the human body, the duration and location of use, and whether the device relies on a source of energy, which applies to virtually all digital health technologies.

There remains some tension between the definitions used in the TG Act and the actual intended use of technology. This is particularly acute in relation to wearables, as well as products aiming to provide guidance to doctors in the exercise of their professional judgment. In many cases, it is necessary to contemplate exactly what the supplier has said about the product as to whether it will be regulated or not. As noted above, the regulatory framework has not been updated to specifically cover the myriad of digital health technologies now in use. The TGA does use its existing framework to declare certain goods to be, and not to be, medical devices, and therefore within or outside the regulatory framework. In relation to software-based devices, the TGA has declared a number of types of technology to be excluded from the regulatory framework.

Additionally, all consumer products are regulated by the CCA. This regulation includes, amongst other matters, consumer protections, provisions applying to warranty disclosure, misleading advertising and fitness for any disclosed purpose.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

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.

Under the TG Act and the 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.

The Office of the Australian Information Commissioner is responsible for the administration of the privacy provisions contained in the My Health Records Act and the *Healthcare Identifiers Act 2010* (Cth).

Additionally, the Australian Competition and Consumer Commission ('ACCC') is responsible for enforcing the 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.

2.5 What are the key areas of enforcement when it comes to digital health?

The primary areas that regulatory authorities are targeting are:

- Classification of devices, both to bring devices within the regulatory framework or to up-classify devices.
- Ensuring digital health products conform to consumer product standards.
- 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.
- The digital economy, including consumer data issues in digital health, is an area of priority for the ACCC.
- Consumer product safety issues for young children, with a focus on compliance, enforcement and education initiatives.

2.6 What regulations 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.

2.7 What regulations apply to artificial intelligence/machine learning 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.

3 Digital Health Technologies

3.1 What are the core legal or 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.

- **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.
  There may also be issues of tort liability where the robotic technology causes harm to a patient. Additionally, data privacy issues arise where the robotic device collects personal information, though this can typically be mitigated by only allowing access to de-identified patient data.
- **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. 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.
- **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**
  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 which merely provides information for consideration by a healthcare professional, to software which provides a warning or recommendation, to software involved in clinical decisions. This is a key area where the regulatory framework has ambiguities.
- **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, 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 which 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, and the appropriate treatment of software updates, and the applicable regulatory oversight of these.

- **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 issues for digital platform providers?

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). While disclosure can be legitimised by obtaining informed consent from the individual to which the information relates, it is important that digital platform providers also remain vigilant in complying with the APPs.

Digital platform providers must also ensure that they have appropriate data management systems and security measures in place, so as to protect against unauthorised access and misuse of personal information it collects. For companies, compliance is becoming even more important, following significant privacy breaches to a number of entities in recent times, and very significant increases in fines.

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

The use of personal data is subject to the APPs. The key issue in relation to 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. The de-identification of patient data is also important, particularly where the information has served its purpose. However, there are often issues in terms of de-identification, particularly where other sources of information can provide sufficient information to re-identify the individual. Withdrawal of consent can also be problematic, particularly since the express right to be forgotten does not exist under Australian law. As such, the right to withdraw consent, or have information deleted, is typically imposed as a matter of voluntary obligation by way of a privacy policy. This creates issues as to how the information is deleted, particularly if it has been passed to third parties or otherwise linked to other data sources.

Given the sensitive nature of health data and identifiers, another important consideration is whether personal information has been adequately de-identified or anonymised prior to disclosure or use, particularly for digital health technologies. Providers also need to contemplate the extent to which some personal information, such as genetic information, can truly be de-identified, especially in a healthcare environment.

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.

4.2 How do such considerations change depending on the nature of the entities 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.

Generally, an APP entity will not include a small business operator, registered political party, State or Territory authority or a prescribed instrumentality of a State, though small businesses which hold or collect health information are fully subject to the Privacy Act.

4.3 Which key regulatory requirements apply?

The Privacy Act is the primary federal law related to protecting patient health information. It is important to note that Australia's Privacy Act has recently undergone a significant review and broad reforms are expected. The Privacy Act limits the use of key identifiers, such as a Medicare number (the key primary identifier used throughout the health systems), being used by private enterprises to identify a patient.

Additionally, the Commonwealth has recently passed the *Security of Critical Infrastructure Act 2018* (Cth) ('SOCI Act'). The SOCI Act applies to regulate Australia's critical infrastructure sectors and assets. Notably, the SOCI Act applies to the healthcare and medical sectors.

The SOCI Act requires the responsible entity for a critical infrastructure asset to have a critical infrastructure risk-management programme. Where a cyber-security incident occurs which has a relevant impact on a critical infrastructure asset, the responsible entity is required to notify Australia's Cyber and Infrastructure Security Centre.

The implications of this legislation are still being played out, and will likely be driven by the larger private, rather than public, hospitals pushing down a range of cyber-security-related requirements on to their providers of relevant digital healthcare

solutions. A high-profile example of this is patient information systems, the failure of which can virtually render a hospital non-functional.

4.4 Do the regulations define the scope of 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 What are the key contractual considerations?

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.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

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 which 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.

4.7 How are issues with 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.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

Australia has been slow to regulate generative AI, and no meaningful steps are currently being taken in this regard. The use of generative AI in the digital health space is not currently subject to specific regulation, such that the sole source of regulation remains the TG Act.

The Privacy Act Review suggested the introduction of several measures for enhancement of the Act, with specific proposals aiming to enhance transparency and individual self-management where AI systems and algorithms are used.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

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 which 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 regards 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.

5.2 How do such considerations change depending on the nature of the entities 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

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.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and 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).

Further, the Victorian Parliament recently 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.

5.5 What are the key issues 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 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 What is 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 What is 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 What is 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 What is 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 are the core rules or laws related to government-funded inventions in your jurisdiction?

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.

7 Commercial Agreements

7.1 What 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 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 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 machine learning 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 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 is the role of machine learning in digital health?

In Australia, ML is used in a variety of ways and in a variety of clinical settings. ML is commonly used to design and conduct medical research, including clinical trials. The functionality of ML has been used to identify molecular targets and drug-target pairs to assist with drug discovery.

ML is commonly used to expedite computation and data management. Use of ML in this context can reduce costs. ML has been used to analyse molecular structures to correlate them with certain properties, such as the ability to kill bacteria.

ML has been used for direct-for-patient usage through mobile apps. ML has also been used to integrate genomic information into Australia's healthcare systems. There are also potential uses in radiology and pathology to provide assistance in the evaluation of test results. Various companies are seeking to develop algorithms based on data sets, to be used in the context of diagnostic tests.

The arrival of public databases supported by AI which might feed into certain digital pathways has the potential to throw up some complex regulatory and liability issues.

8.2 How is training data licensed?

There are no special rules applying to training data. The licensing of training data depends on the relevant licensee and the terms of each licence agreement. The provenance of such data can be critical to understand, especially if it has been generated in a clinical trial setting. There is clearly a demand for good normal data sets, noting that so many of the data sets around relate to treated persons that are not necessarily representative of the broader community.

However, issues we are seeing emerge are liability/warranty regarding training data, financial return models which seek to lock onto derived data sets and the ownership/entitlement to 'insights' that may be garnered from the use or analysis of such data.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning 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 considerations apply to licensing data for use in machine learning?

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.

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 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 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.

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 Records 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 which 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.

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 Australian Digital Health Agency ('ADHA'), which is a Commonwealth entity which 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 is typically taking 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. MSAC is responsible for undertaking a health technology assessment 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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with 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 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 which 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, and presently in a state of flux. This is an acute issue where the product or service is patient focused, as opposed to, for example, something more directed to the health ecosystem.
- Australia has, to date, been particularly protective around the sovereignty of its genetic data and health data more generally. There is some specific awareness around data from indigenous persons. It remains to be seen whether this becomes a focus of attention, noting that there is an increasing level of awareness of this issue arising out of various interactions with China.
- The continuing ratcheting up of standards, and penalties for breach of the same, in both the privacy and cyber-security space. This is being driven by both Federal and State reforms, and also increasingly prescriptive contractual terms.
- The TGA response, if any, to the importer–sponsor issue, and the implications for overseas bodies delivering technology into Australia.
- 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.

Bernard O'Shea is the Head of Norton Rose Fulbright Australia's Life Science sector focus, and has been working in the sector for over 20 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 bring novel products to market, and is actively involved in assisting multiple digital health companies 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 lawyer 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

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

Austria

Herbst Kinsky Rechtsanwälte GmbH

Dr. Sonja Hebenstreit

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 Austrian law. The Austrian Federal Ministry of Health's definition (see https://www.sozialministerium.at/Themen/Gesundheit/eHealth.html) uses the term "e-health" as the general term, comprising the use of information and communication technologies in health-related products, services (including telemedicine) and processes. The Ministry uses the term "telemedicine" as referring to the provision or support of healthcare services using information and communication technologies, where the patient and the healthcare provider are not present in the same place. This is in line with the definition used by the European Commission, who suggested using the term "telehealth" as referring to health-related procedures and "telemedicine" as referring to treating people from a distance (see https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf , page 25).

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

Key emerging technologies are, in particular, artificial intelligence (AI) applications including machine learning (ML), which can contribute, for example, to earlier disease detection and more accurate diagnosis.

1.3 What are the core legal issues in digital health for your jurisdiction?

The core legal issues in digital health are: compliance with data protection laws (see sections 4 and 5); compliance with the requirement that only a licensed physician may give medical advice (see question 2.1); the technical requirements (see *GTelG 2012* in question 2.2); and the determination of whether a product qualifies as a medical device (see questions 2.1 and 3.1).

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

There is no reliable data available regarding the digital health market size for Austria, as the available statistics either do not refer to Austria in particular, or only consider specific segments of the total digital health market.

According to a market outlook as published by Statista (see https://de.statista.com/outlook/hmo/digital-health/oesterreich), the overall revenue for 2023 in Austria in the e-health sector amounts to approximately 649.1 million euros. According to the forecast, a market volume of 922.7 million euros will be reached in 2028, corresponding to an expected annual sales growth of 7.29%. However, this survey does not take into account the public e-health sector in Austria (which is the most relevant sector) as it only includes non-prescription e-health devices and apps.

In another study published by Roland Berger (see https://de.statista.com/statistik/daten/studie/1178751/umfrage/umsatz-auf-dem-markt-fuer-digital-health-weltweit/), the volume of the digital health market in 2026 in Germany is estimated to reach 59 billion euros. Consequently, one tenth of this (5.9 billion euros) could be assumed for Austria's digital health market volume in 2026 as a tentative estimate (due to the size ratio between Austria and Germany).

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

As pointed out in question 1.4, there are no reliable figures available on the Austrian digital health market size. Therefore, we cannot provide an overview of the five largest digital health companies by revenue.

Further, please note that a major part of digital health solutions applied in Austria are organised by the Austrian state and implemented by the Umbrella Association of Austrian Social Insurance Institutions.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The Austrian Physicians Act 1998, Federal Law Gazette I 169/1998, as last amended by the Federal Law Gazette I 108/2023 (*Ärztegesetz* 1998 (*ÄrzteG*)) contains, in principle, regulations on training and admission as a physician, regulations on the exercise of the profession (e.g. group practices), prohibitions of discrimination and regulations on the organisation of the self-administration of physicians (Medical Association). Section 3 of the *ÄrzteG* stipulates that medical advice may only be given by licensed physicians. Section 49 paragraph 2 of the *ÄrzteG* further stipulates that physicians shall practice their profession "personally and directly". This provision is regarded as not generally prohibiting telemedicine, i.e. the individual diagnosis

and treatment from a distance, without direct human contact. The Austrian Medical Association has stated that telemedicine might support the relationship between physician and patient and the treatment process; and that digital monitoring and online contact might be helpful for the diagnosis as well as for the therapy, but has emphasised that a clear legal framework is required for telemedicine services. Currently, no such specific legal framework is in place. In any case, physicians are obliged to comprehensively inform the patient and get the patient's informed consent (likewise), whereas in the case of telemedicine, they need to be in full control of the patient's situation and the telehealth treatment must be for the patient's benefit.

In the context of the referral of patients through online platform operators, the prohibition of commissions according to Section 53 paragraph 2 of the *ÄrzteG* must be observed, according to which the physician may not promise, give, take or have promised to himself or another person any remuneration for the referral of patients to him or through him. According to paragraph 3 *leg cit*, activities prohibited under paragraph 2 are also prohibited for group practices (Section 52a) and other physical and legal persons. This means that the collection of commissions from patients is prohibited not only for doctors but also for other third party (natural or legal) persons.

The Austrian Medicinal Products Act, Federal Law Gazette 185/1983, as last amended by Federal Law Gazette I 72/2023, (*Arzneimittelgesetz* (*AMG*)) implements a large number of European Union (EU) directives concerning regulations on medicinal products, in particular Directive 2001/83/EC – Community code relating to medicinal products for human use. The *AMG* contains regulations on the authorisation of medicinal products, regulations regarding marketing, advertising and distribution of medicinal products as well as quality assurance requirements.

The Austrian Medical Devices Act, Federal Law Gazette 657/1996, as last amended by Federal Law Gazette I 27/2023, (*Medizinproduktegesetz* (*MPG*)) as well as the Medical Device Regulation 2017/745 on medical devices (MDR), which entered into force on May 26, 2021, after having been postponed for a year due to the COVID-19 pandemic, constitutes the major regulatory framework for medical devices. The MDR lays down rules concerning the placing on the market, making available on the market or putting into service of medical devices for human use and accessories for such devices in the EU. The MDR also applies to clinical investigations concerning such medical devices and accessories conducted in the EU.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The General Data Protection Regulation, Regulation 2016/679 (GDPR) contains central provisions on data protection. Although the GDPR as a regulation applies uniformly and directly throughout the EU, a large number of opening clauses allow national deviations by Member States. Providers of digital health in particular must take into account the provisions on the lawfulness of the processing of health data pursuant to Article 9 of the GDPR, as well as the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, pursuant to Article 32 of the GDPR.

The Austrian Data Protection Act, Federal Law Gazette I 165/1999, as last amended by Federal Law Gazette I 148/2021, (*Datenschutzgesetz* (*DSG*)) specifies the provisions of the GDPR and, in particular, contains provisions on proceedings before the Austrian data protection authority. For the private sector, the *DSG* does not provide any provisions for the processing of health data that deviate from the GDPR.

The Austrian Health Telematics Act 2012, Federal Law Gazette I 111/2012 as last amended by Federal Law Gazette I 82/2023, (*Gesundheits-Telematikgesetz* 2012 (*GTelG 2012*)) contains special regulations for the electronic processing of health data and genetic data (please refer to Article 4 Nos 13 and 15 of the GDPR) by healthcare providers. A healthcare provider in the meaning of health telematics is a professional who, as a controller or processor (in the meaning of Article 4 Nos 7 and 8 of the GDPR), regularly processes health data or genetic data in electronic form for the following purposes:

- medical treatment or care;
- nursing care;
- invoicing of health services;
- insurance of health risks; or
- exercise of patient rights.

The *GTelG 2012* also contains detailed regulations on the operation of *ELGA* by ELGA GmbH, which is owned by the Republic of Austria, the Umbrella Association of Austrian Social Insurance Institutions and the federal provinces or their health funds. *ELGA*, known as *Elektronische Gesundheitsakte*, means Electronic Health Records and is available to all persons receiving care in the Austrian healthcare system (see https://www.gesundheit.gv.at/gesundheitsleistungen/elga.html). In the context of *ELGA*, other e-health services have also been introduced, such as the electronic medication prescription (e-medication), the electronic vaccination pass (e-vaccination pass; see section 24b *et seq*. *GTelG 2012*, as well as eHealth Regulation, Federal Law Gazette II 449/2020, last amended by Federal Law Gazette II 53/2023) or recently the electronic Parent-Child-Pass (E-Parent-Child-Pass Act, Federal Law Gazette I 82/2023).

To meet the challenges of the COVID-19 pandemic, (temporary) simplifications to the conditions of transmitting health data via email and fax for healthcare providers were implemented to the *GTelG 2012* as well.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The *MPG* and the *MDR* (see question 2.1) likewise apply to consumer devices.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

In connection with the *GTelG 2012* and Health Telematics Regulation 2013, as last amended by Federal Law Gazette II 506/2013 (*Gesundheitstelematikverordnung (GTelV 2013)*) the Federal Minister for Health is competent for notifications and for the operation of the eHealth directory service according to paragraphs 9 and 10 of the *GTelG 2012*.

In connection with the *ÄrzteG*, the competent authorities are the Austrian Medical Chamber, the respective state governor (*Landeshauptmann*) and the Federal Minister for Health.

The Federal Office for Safety in Health Care (*Bundesamt für Sicherheit im Gesundheitswesen* (*BASG*)) is the central regulatory authority for the medicinal products and medical devices industry. The BASG is responsible, among other things, for the approval of medicinal products, market surveillance and pharmacovigilance, notifications in connection with clinical trials, the control of advertising restrictions and the granting and review of operating licences.

Investigations and assessments are typically carried out by the Austrian Agency for Health and Food Safety (*Österreichische Agentur für Gesundheit und Ernährung* (*AGES*)) on behalf of the BASG.

The Austrian Data Protection Authority (*Datenschutzbehörde* (*DSB*)) is the supervisory authority, as defined in Article 4 Section 21 of the GDPR, for the monitoring of data protection law and the assertion of data subjects' rights under the GDPR.

2.5 What are the key areas of enforcement when it comes to digital health?

As far as can be seen, neither the Austrian Medical Chamber nor the *BASG* or the Federal Minister of Health recently took relevant enforcement measures in the regulatory area of digital health and healthcare IT.

In 2018, the *DSB* rendered a major decision regarding the communication between physicians and patients (DSB-D213.692/0001-DSB/2018): according to the *DSB*, patients cannot consent to the (unencrypted) transmission of health data (e.g. medical reports) by physicians. The *DSB* reasoned that the choice of the communication method is a technical/organisational measure according to Article 32 of the GDPR, and that no consent can be provided to insufficient technical/organisational measures.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

According to Recital 19 of the MDR, software qualifies as a medical device when it is specifically intended by the manufacturer to be used for one or more medical purposes, while software for general purposes, even when used in a healthcare setting, or software intended for lifestyle and well-being purposes is not a medical device. The qualification of software, as either a device or an accessory, is independent of the software's location or the type of interconnection between the software and a device. Therefore, as a general rule, software for general purposes, even if used in the healthcare sector, is not a medical device. The manufacturer determines the intended use, which is essential for software for general purposes to be differentiated from a medical device.

According to the MDR, manufacturers of medical devices are obliged to carry out a clinical evaluation for all their products – regardless of the risk class – which also includes a post-market clinical follow-up. Such clinical evaluation is an essential task of the manufacturer and an integral part of a manufacturer's quality-management system (Article 10 paragraphs 3 and 9f of the MDR). The clinical evaluation is a systematic and planned process for the continuous generation, collection, analysis and evaluation of clinical data for a device. Through the clinical evaluation, the manufacturer verifies the safety and performance of his device, including the clinical benefit.

Furthermore, Regulation No. 207/2012 on electronic instructions for use of medical devices must be observed when providing electronic instructions for use.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

The terms "AI" or "ML" are generic and rather technology-neutral terms, as they represent a wide range of different kinds of technologies. To date, there is no definitive legal definition available in the Austrian or European jurisdiction and the European legislator is aiming to issue its AI Regulation (COM 2021/206) based on a rather technology-neutral level. *De lege lata*, the same regulations apply to AI and ML as to all other technologies, which means that for the healthcare sector, in particular, the MDR as well as the GDPR are relevant.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  According to Section 3 of the *ÄrzteG*, medical advice may only be given by licensed physicians. Furthermore, the physician must decide in each individual case of such telehealth consultation, if he can sufficiently control possible dangers despite the lack of physical contact with the patient and whether he has a sufficient information basis for his decisions. In case the physician fears that he does not have a sufficient basis for his medical decision due to lack of physical patient contact, he must advise the patient to physically see a physician.
  Austrian law does not contain rules for the provision of telemedicine or virtual care services in general, but a specific regulation has been issued regarding the provision of teleradiology services: the Medical Radiation Protection Regulation, Federal Law Gazette II 375/2017, last amended by Federal Law Gazette II 353/2020 (*Medizinische Strahlenschutzverordnung*) provides that teleradiology is permitted within the framework of basic and special trauma care, as well as in dispersed outpatient primary care facilities of acute hospitals and otherwise only in order to maintain night, weekend and holiday operations for urgent cases.
  According to paragraphs 3 and 4 of the *GTelG 2012*, health service providers may transfer health data and genetic data only if:
  - the transmission is permitted under Article 9 of the GDPR;
  - the identity of those persons whose health data or genetic data is to be transmitted is proven;
  - the identity of the healthcare providers involved in the transmission is proven;
  - the roles of the healthcare providers involved in the transmission are demonstrated;
  - the confidentiality of the transmitted health data and genetic data is guaranteed; and
  - the integrity of the transmitted health data and genetic data is guaranteed.

  In addition, the *GTelG 2012* and *GTelV 2013*, issued by the Federal Minister of Health on the basis of the *GTelG 2012*, contain detailed regulations on encryption and technical implementation of communication.
  The COVID-19 pandemic has led to a massive increase regarding the use and offer of telemedicine services.
  As outlined above in question 2.2, due to the COVID-19 pandemic, (temporary) simplifications to the conditions of transmitting health data (via email and fax) for healthcare providers have been implemented to the *GTelG 2012*.
- **Robotics**
  According to Section 3 of the *ÄrzteG*, medical advice may only be given by licensed physicians. Furthermore, robotics may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes (e.g. robotics for surgical purposes).
- **Wearables**
  Wearables may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes.

- **Virtual Assistants (e.g. Alexa)**
  According to Section 3 of the *ÄrzteG*, medical advice may only be given by licensed physicians. Virtual Assistants in general would not qualify as a medical device. However, natural language processing may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes.
- **Mobile Apps**
  See question 2.6 (Software as a Medical Device).
- **Software as a Medical Device**
  See question 2.6.
- **Clinical Decision Support Software**
  See question 2.6. Further, the GDPR, in particular its provisions on automated individual decision-making (Article 22 of the GDPR), must be considered in case personal data is processed.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  See question 2.6 (Software as a Medical Device) and section 8 (AI and ML).
- **IoT (Internet of Things) and Connected Devices**
  IoT and connected devices may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes (e.g. blood pressure measurement using cloud recording); furthermore, the GDPR must be considered in case personal data is processed.
- **3D Printing/Bioprinting**
  Bioprinting raises a wide range of legal and ethical questions. Currently, no *sui generis* regulatory regime governing the entire bioprinting process is in place in Austria. According to the European Commission and the European Medicines Agency, tissue-engineered products might fall under the definition of advanced therapy medicinal products (ATMPs). Additionally, IP and, in particular, patent rights questions might arise.
- **Digital Therapeutics**
  Digital therapeutics is a rather broad term used for device-controlled therapy measures. In particular, digital therapeutics may be subject to the MDR as well as provisions of the GDPR. In view of its high-risk potential, digital therapeutic software shall, according to Annex VIII; Rule 11 of the MDR, be classified as a medical device of at least risk class IIa.
- **Digital Diagnostics**
  Digital diagnostics in the sense of device-controlled diagnostic measures may be subject to the MDR as well as the GDPR.
- **Electronic Medical Record Management Solutions**
  See questions 2.2 and 10.6 for detailed information on the *ELGA*, the Austrian central digital health solution, which also serves as an electronic medical record management solution. A very recent solution that is currently being implemented is the Parent-Child-Pass (see question 2.2).
- **Big Data Analytics**
  In particular, the GDPR must be observed when applying big data analytics. The *Data Governance Act (DGA)*, which entered into force in September 2023, intends to facilitate the re-use of protected data held by the public sector (e.g. personal data and/or commercially confidential data) which could be re-used under specific EU or national legislation.
- **Blockchain-based Healthcare Data Sharing Solutions**
  The GDPR must be observed, as well as the *GTelG 2012*; no legislation is in place specifically governing blockchain technology.
- **Natural Language Processing**
  Natural language processing generally does not qualify as a medical product (e.g. speech recognition in dictation software). However, natural language processing may be subject to the MDR when specifically intended by the manufacturer to be used for one or more medical purposes; furthermore, the GDPR must be observed.

3.2 What are the key issues for digital platform providers?

One of the main restrictions on digital platforms for individual healthcare is that medical advice may only be given by licensed physicians (Section 3 of the *ÄrzteG*; see question 2.1).

Furthermore, online platform operators should keep in mind the prohibition of commissions in Section 53 paragraph 2 of the *ÄrzteG*, according to which the physician may not promise, give, take or have promised to himself or another person any remuneration for the referral of patients to him or through him. Moreover, these activities are also prohibited for group practices (Section 52a) and other physical and legal persons. This means that the collection of commissions from patients is prohibited not only for doctors, but also for other third party (natural or legal) persons.

Digital platforms must take appropriate (high) technical/organisational measures for data security when processing health data (Article 32 of the GDPR) and the *GTelG 2012* must be considered in case personal health data is processed.

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

The processing of personal data must comply with the GDPR. When processing health data, Article 9 of the GDPR applies; according to that provision, the processing of health data in connection with healthcare providers is lawful only if (only the most relevant legal grounds have been included in the following):

- the data subject has given explicit consent to the processing of their personal data for one or more specified purposes (Article 9 Section 2 letter a of the GDPR);
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent (Article 9 Section 2 letter c of the GDPR);
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health, social care, treatment or the management of health or social care systems (Article 9 Section 2 letter h of the GDPR);
- pursuant to a contract with a health professional, when the personal data is processed by or under the responsibility of a professional subject to the obligation of professional secrecy (Article 9 Section 2 letter h in connection with Section 3 of the GDPR); and
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices (Article 9 Section 2 letter i of the GDPR).

4.2 How do such considerations change depending on the nature of the entities involved?

In principle, the provisions of the GDPR apply equally to all entities. However, the legal grounds in Article 9 Section 2 letter h only apply to data processing, when the personal data is

processed by or under the responsibility of a professional subject to the obligation of professional secrecy. Therefore, entities not subject to professional secrecy cannot rely on this legal ground.

4.3 Which key regulatory requirements apply?

The general regulatory provisions of the GDPR apply, namely the principles of transparency, lawfulness, purpose limitation, data minimisation, proportionality, accuracy, data security and accountability. As in the context of digital health services, large-scale processing of sensitive personal data will be involved, the entity providing such services is required to designate a Data Protection Officer in accordance with Article 37 para 1 lit c of the GDPR. Furthermore, a data protection impact assessment might be required (e.g. according to Article 35 para 3 lit b of the GDPR) before processing is started.

4.4 Do the regulations define the scope of data use?

Yes, please refer to question 4.1. Some legal grounds of Article 9 of the GDPR impose limitations on the purpose of the processing (e.g. preventive or occupational medicine; see question 4.1). Neither the GDPR nor the *DSG* contain regulations defining the scope of data use in the context of digital health.

4.5 What are the key contractual considerations?

If the processing is based on explicit consent of the data subject, such valid and fully informed consent must be given by the patient/data subject. Furthermore, according to Article 28 of the GDPR, any data controller must conclude a written data processing agreement with processors, which must contain the minimum contents specified therein. In the event where more than one controller jointly decides on the respective processing, an agreement on joint controllership must be concluded between these controllers.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The key legal issues and therefore greatest challenge with regard to securing comprehensive rights to personal data is that the personal data must be collected in accordance with the principles pursuant to Article 5 of the GDPR and that a corresponding legal basis must be guaranteed for each processing at all times. Successfully facing those legal issues is not only important because of the severe penalties for the unlawful processing of personal data provided for in the GDPR (Article 83 of the GDPR); it is also vital for any digital (health) application using personal data to safeguard that such use is lawful as otherwise the application risks being shut down by the data protection authority at any time.

However, the GDPR is only applicable to personal data. Therefore, if no personal data according to Article 6 or Article 9 of the GDPR is processed, a specific right to process the data is not necessary from a data protection point of view.

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

A data subject may request the respective data controller to correct any inaccurate or incomplete personal data. If the data is not corrected by the processor or if the data subject is of the opinion that the processing of the personal data violates the GDPR, the data subject may file a complaint with the data protection authority and/or a (civil) lawsuit against the controller requiring the correction of the inaccuracy.

The Federal Act on Equal Treatment, Federal Law Gazette I 66/2004, as last amended by Federal Law Gazette I 115/2023 (*Gleichbehandlungsgesetz* (*GlBG*)) focuses on equal treatment in the world of work and in other areas. No one shall be discriminated because of his gender, age, ethnical affinity, religion or belief or sexual orientation. A person who is subject to discrimination can claim the establishment of the non-discriminatory condition and compensation for the pecuniary loss and for the personal impairment suffered.

The Federal Act on the Equality of Persons with Disabilities, Federal Law Gazette I 82/2005, as last amended by Federal Law Gazette I 32/2018 (*Bundes-Behindertengleichstellungsgesetz* (*BGStG*)) aims to eliminate or prevent discrimination against persons with disabilities. This is to ensure equal participation of persons with disabilities in society and to enable them to lead a self-determined life.

No one may be discriminated against on the basis of a disability. In the event of a violation of this prohibition, the person concerned is in any case entitled to compensation for the pecuniary loss and for the personal impairment suffered.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

The normal legal framework applies to data usage (i.e. GDPR, *GTelG 2012*, the Copyright Act with the text and data mining exception being implemented in section 42h Copyright Act) since, so far, no specific AI legal framework has been implemented.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Sharing health data between healthcare professionals is subject to the *GTelG 2012* (see question 3.1 for the conditions of sharing under the *GTelG 2012*), sharing of data between individuals other than healthcare professionals is solely subject to the GDPR; see question 4.1 for sharing within the EU. For sharing with an individual located outside the EU/EEA, the GDPR provisions on the transfers of personal data to third countries or international organisations apply.

5.2 How do such considerations change depending on the nature of the entities involved?

Sharing of data between individuals other than healthcare professionals is solely subject to the GDPR (see question 4.1). In this case, the *GTelG 2012* does not apply.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Please refer to questions 4.3 and 5.1.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

One of the aims of the DGA, which entered into force in September 2023, is facilitating the re-use of protected data held by the public sector (e.g. personal data and/or commercially confidential data) which could be re-used under specific EU or national legislation. The DGA provides for rules and safeguards to enable such re-use of data whenever it is possible under other legislation.

Another European initiative, which builds upon the DGA, is the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, which intends to address health-specific challenges to electronic health data access and sharing by providing a framework for the secondary use of electronic health data.

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

Federated models follow a relatively new ML approach, where each federated device shares its local model parameters instead of sharing the whole dataset used to train it (see https://edps.europa.eu/press-publications/publications/techsonar/federated-learning_en). As a consequence of the federated structure, key issues to consider are whether the local model parameters constitute personal data and if so, how data security, data accuracy, data integrity and confidentiality are handled. Please refer also to questions 4.3 and 5.1.

6 Intellectual Property

6.1 What is the scope of patent protection for digital health technologies?

Technical inventions that are novel, that, considering the state of the art, are not obvious to a person skilled in the art, and that can be applied in the industry, can be subject to patent protection under the Austrian Patent Act 1970, Federal Law Gazette I 259/1970, as last amended by Federal Law Gazette I 51/2023 (*Patentgesetz 1970 (PatG 1970)*). If and insofar as a digital health technology meets the above-mentioned requirements, it can be subject to patent protection. Only a natural person can qualify as an inventor.

The inventor can either file a patent himself or transfer his right to a third party. The patent owner has the exclusive right to manufacture, put into circulation, offer for sale and use the patented invention for the duration of the patent, namely up to 20 years. A "prolongation" of the patent protection can only be achieved by virtue of a Supplementary Protection Certificate, a *sui generis* IP right available for specific medicines and plant protection products.

Software programs as such cannot be subject to patent protection.

6.2 What is the scope of copyright protection for digital health technologies?

Under Austrian law (the Austrian Federal Law on Copyright in Works of Literature and Art and on Neighbouring Rights, Federal Law Gazette I 111/1936, as last amended by Federal Law Gazette I 244/2021 (*Urheberrechtsgesetz (UrhG)*)), a work is defined as an "original intellectual creation" (Section 1 paragraph 1 of the *UrhG*). The author has the exclusive right to use his work in the way defined by the law (in particular: reproduction right; distribution right; rental and lending right; broadcasting right; right of public performance; and of communication to the public of a performance, making available right). Protection starts in the very moment of creation, which means that no registration with any authority is required for protection under the Copyright Act. According to Section 1 paragraph 1 of the *UrhG*, works can be original intellectual creations in the area of literature (including computer programs), musical arts, visual arts and cinematography. Digital health technologies can especially fall under the category "computer programs". In principle, only creations of human beings are regarded as works and protected by copyright; and the legislator has so far not provided for specific rules for "computer-generated works". According to current doctrine, computer-generated works may still be subject to copyright protection. The programmer as the author, although not directly involved in the creation of the work, has created the creative framework for it by programming the appropriate autonomy.

The Copyright Act further grants exclusive rights to performers (such as singers, dancers and actors) as well as phonogram producers, photographers, broadcasters and the producers of a database (*sui generis* right).

6.3 What is the scope of trade secret protection for digital health technologies?

The Unfair Competition Act, Federal Law Gazette I 448/1984, as last amended by Federal Law Gazette I 99/2023 (*Bundesgesetz gegen unlauteren Wettbewerb,* (*UWG*)) contains in its Sections 26a *et seq.* civil law and civil procedural law rules for the protection of trade secrets. According to the legal definition in Section 26b of the *UWG*, information that is:

- secret, namely not known or readily accessible by persons that normally deal with the respective information;
- of commercial value because of its secrecy; and
- subject to reasonable measures to be kept secret,

qualifies as a trade secret.

It must be proven that reasonable measures have been taken; these may include specific IT security measures and the restricted accessibility of secret information (e.g. only accessible to particularly trustworthy employees).

A variety of information may be regarded as a trade secret, for example, inventions and designs (if not protected as a patent or design) as well as not otherwise protected information such as production processes, customer information, business models or the like.

The owner of a trade secret is particularly entitled to claims of forbearance, removal and damages against anyone who unlawfully acquires, uses or discloses his trade secrets.

Section 26h of the *UWG* contains specific rules to ensure the protection of trade secrets in civil proceedings.

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

Universities may claim any service invention made by one of its employees within three months of notification of the invention (see Section 106 paragraph 2 of the University Act 2002, Federal Law Gazette I 120/2002, as last amended by Federal Law Gazette I 52/2023, (*Universitätsgesetz 2002* (*UG 2002*)) in connection with the Patent Act's rules on service inventions); the employee is generally entitled to a special remuneration if the university makes use of that right. If the university does not claim the

invention, the general rule applies, namely, the inventor is entitled to the invention. Regarding the commercialisation of technology developed by its researchers, Austrian universities pursue different strategies – from outlicensing to transferring IP and increasingly, additionally acquiring shares in its spin-out companies.

6.5 What is the scope of intellectual property protection for software as a medical device?

There are no specific rules for Software as a Medical Device from an IP protection point of view, i.e. the software as such will be protected by copyright law; whether patent protection can be sought must be assessed individually.

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

Exclusively natural persons can be named and registered as an inventor for patents, as the legal institution of an "e-person" is not recognised in Austrian law. If an AI device should "invent" a patentable product, this goes back to the actual inventor (natural person) of the AI device. According to the Patent Act, only human beings can qualify as inventors.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

In principle, the rules of the Patent Act regarding service inventions (section 7 *et seq.* Patent Act) apply to inventions made within academic (see question 6.4), or other public-funded institutions (see e.g. the Federal Act on General Matters Pursuant to Article 89 of the GDPR and the Research Organization (*Forschungsorganisationsgesetz*, (*FOG*)), Federal Law Gazette I 341/1981, as amended by Federal Law Gazette I 52/2023, and Federal Act on the Institute of Science and Technology Austria (*IST-Austria-Gesetz* (*ISTAG*)), Federal Law Gazette I 69/2006, as amended by Federal Law Gazette I 75/2020).

7 Commercial Agreements

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

If not otherwise regulated, collaborative improvements belong to the respective inventors of such improvement, whereas the ownership of the basis technology will not change following such improvements. The ownership, and eventually licences regarding the use of such collaborative improvements, is therefore usually regulated precisely and meticulously in the respective agreements containing the regularities for the collaboration.

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

Besides regulatory considerations (see question 2.1), the general principles apply, namely Austrian law's (federal) rules on commercial contracts, providing regulations on the general principles and specific contract types.

The general principles of contracts, as well as a large number of specific contracts, are regulated in the Civil Code (*Allgemeines Bürgerliches Gesetzbuch*) and in the Commercial Code (*Unternehmensgesetzbuch*).

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

Parties should in general consider data governance. Please refer to questions 4.3, 5.1 and 5.5. In terms of data licensing, see question 8.2.

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

Parties will need to consider that, according to Section 3 of the *ÄrzteG*, medical advice may only be given by licensed physicians. See also above question 3.1 (in particular regarding *Telemedicine/ Virtual Care* and *Virtual Assistance*).

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Many digital health devices use ML (such as, e.g. in the field of radiology, and generally in diagnosing). ML is substantial for developing smart digital health solutions and is said to have the potential to substantially transform healthcare both for patients and medical professionals.

8.2 How is training data licensed?

The protection and licensing of training data does not differ from any other protection of information, creations and data. If the training data were created in a specific way by a human being (e.g. texts for speech recognition) they may be subject to copyright protection (see question 6.2). In addition, training data may also be subject to trade secrecy protection (see question 6.3). For using such data, a licence agreement must be concluded with the respective right holder.

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

Software may, in principle, be protected by copyright (see question 6.2). However, copyright protection requires an "intellectual creation" which, according to Austrian law, can only originate from the thoughts of a human being. Assuming that the improvement could have only been achieved because the programmer has "instructed" the algorithms correspondingly, it could be argued that the programmer is the author of the work (in other words, the improvement, which continues to depend on the basis work). In case the improvement was indeed created without active human involvement, it does not qualify for copyright protection.

8.4 What commercial considerations apply to licensing data for use in machine learning?

For the provision of data for use in ML, the licensor is often commercially interested not only in remuneration, but will often have an interest in technical cooperation, under which the licensor

acquires rights to the results of the ML. Therefore, the provision of data for use in ML is often based on a broad cooperation.

9 Liability

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

No specific liability schemes for adverse outcomes in digital health solutions exist under Austrian law. Austrian tort law generally stipulates that the tortfeasor is obliged to compensate for those damages which he has culpably and unlawfully caused. In addition to material damages, the injured party is also entitled to receive compensation for pain and suffering in case of injuries to the body and/or health. Punitive damages are not paid in Austria. Unlawfulness in the context of the provision of health services typically results from the violation of contractual obligations (e.g. duties of care, non-valid consent to the treatment because of incorrect or insufficient information). The liability for personal injury cannot be excluded and/or limited by contract.

The Austrian Product Liability Act, Federal Law Gazette 99/1988, last amended by Federal Law Gazette I 98/2001, (*Produkthaftungsgesetz* (*PHG*)) transposes in particular Directive 1999/34/EC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. If a defect in a product kills a person, causes bodily injury or damage to health, or damages a physical object other than the product, the manufacturer, distributor and the importer shall be liable for damages under Section 1 of the *PHG*. Liability is subject to the product being defective and therefore not offering the safety that can be expected under consideration of all circumstances (Section 5 paragraph 1 of the *PHG*). However, liability shall be excluded if the manufacturer, distributor or importer proves that: (i) the defect is due to a legal provision or official order with which the product had to comply; (ii) the characteristics of the product are in accordance with the state of the art in science and technology at the time when the person making the claim put it into circulation; or (iii) where the person making the claim has manufactured only one basic material or part of a product, the defect was caused by the design of the product into which the basic material or part has been incorporated or by the instructions of the manufacturer of that product.

9.2 What cross-border considerations are there?

In case of any cross-border provision of digital health services, the respectively applicable law and the applicability of regulatory requirements must be determined.

In case it is intended that foreign doctors provide telemedical treatment to Austrian patients, these require an Austrian professional licence if their activity does not fall under Section 37 of the *ÄrzteG* (freedom to provide services). According to Section 37 of the *ÄrzteG*, nationals of EU/EEA Member States or Switzerland who lawfully exercise the medical profession in another EU/EEA Member State or Switzerland may, from their foreign professional domicile or place of employment, practice medicine in Austria only if the medical activity is temporary and occasional, which must be assessed on a case-by-case basis, in particular on the basis of the duration, frequency, regular return and continuity of the activity.

Further considerations refer to the law applicable in a cross-border scenario: the provision of health services is typically based on a contract concluded by a natural person for a purpose which can be regarded as being outside his trade or profession (the patient) with another person acting in the exercise of his trade or profession (the medical professional). According to Article 6 Regulation 593/2008 on the law applicable to contractual obligations (Rome I) the contract as well as the contractual liability derived therefrom shall therefore be governed by the law of the country where the consumer has his habitual residence, provided that the professional: (i) pursues his commercial or professional activities in the country where the consumer has his habitual residence; or (ii) by any means, directs such activities to that country or to several countries including that country. Cross-border healthcare providers therefore typically have to comply with the laws of a large number of countries in which they offer their services.

For claims arising from product liability under the *PHG*, pursuant to Article 5 Regulation 864/2007 on the law applicable to non-contractual obligations (Rome II), the law applicable shall be: (i) the law of the country in which the person sustaining the damage had his habitual residence when the damage occurred, if the product was marketed in that country; or, failing that; (ii) the law of the country in which the product was acquired, if the product was marketed in that country; or, failing that (iii) the law of the country in which the damage occurred, if the product was marketed in that country. As a result, providers of medical devices must therefore also comply with a large number of legal systems in the area of product liability.

9.3 What are best practices to minimise liability risks posed by the use of generative AI in the provisioning of digital health solutions?

As, according to Section 3 of the *ÄrzteG*, medical advice may only be given by licensed physicians, it must be safeguarded that any medical advice or diagnosis is only given by such licensed physician.

10 General

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

Like for healthcare IT in general (see question 1.3), the main legal issues for Cloud-based services for digital health are the compliance with data protection law (see sections 4 and 5), the technical requirements for telehealth (see *GTelG 2012* in question 2.1) as well as determining whether a product qualifies as a medical device (see questions 2.1 and 3.1).

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

The intended business model and the actual product or service that shall be offered must be carefully examined from a legal perspective, in particular from a regulatory (e.g. the Physicians Act and limitations of telemedicine, MDR) and from a data protection point of view; in addition, the applicability and requirements of the *GTelG 2012* need to be considered. Furthermore, if such is relevant, depending on the business model, it should be assessed whether reimbursement of the services in question by the state sick funds is at all possible.

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

A comprehensive regulatory (including data protection) due

diligence is advisable in order to safeguard that the business, which the digital healthcare venture intends to undertake or already undertakes, complies with all applicable legal requirements.

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

One key barrier is Section 3 of the *ÄrzteG*, according to which medical advice may only be given by licensed physicians. Furthermore, the funding and/or (non-)reimbursement of digital health solutions by the state sick funds is a major issue; non-reimbursement would be a barrier to the widespread use of digital health solutions. Since the COVID-19 pandemic, the sick funds have expanded reimbursement of telemedicine treatment.

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?

From a formal/legal point of view, under Austrian law, clinician certification bodies might not be of specific relevance, even though acceptance or endorsement of a specific digital health solution by such body might prove compliance with specific quality standards or recommendations issued by such body. However, within a possible legislative process, these bodies might typically be consulted. The introduction of digital health solutions is in principle exclusively governed by law.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

The Austrian state provides for a central digital health solution, namely *ELGA* (see question 2.2), which is owned by the Republic of Austria, the Umbrella Association of Austrian Social Insurance Institutions, as well as the federal provinces or their health funds. The services that are provided within *ELGA* (e.g. e-medication) do not have to be paid separately by patients and are covered by the general health insurance. The legal requirements of *ELGA* are set forth in the *GTelG 2012*.

Any other digital health solution an individual might want to use would need to be prescribed by a physician and be appropriate in order to be reimbursable by the Umbrella Association of Austrian Social Insurance Institutions.

10.7 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 COVID-19 pandemic has led to a massive increase regarding the use and offer of telemedicine services in Austria, including non-contact medication prescriptions and the COVID-specific symptom check and triaging via app. With the help of these telemedicine applications, it was possible to find rapid solutions for patient care during the pandemic.

In addition, reimbursement by sick funds for telemedicine treatments was expanded and the use of video consultations mostly for initial consultations, therapeutic discussions and review of findings increased.

These developments have proven useful and will therefore be kept and be further expanded in fields where telemedicine can be reasonably used, as telemedicine offers enormous potential for the high-quality and cost-effective provision and support of healthcare services and ensures access to high-quality healthcare throughout the country.

Furthermore, the Austrian federation has emphasised that it intends to increase the use of and is in the process of creating a legal framework for specific digital health applications, namely of evidence-based, software-driven therapeutic applications for the prevention, management or treatment of a medical disorder or disease, which shall be reimbursed by the state sick funds if prescribed by a physician (see more at https://www.digitalaustria.gv.at/Strategien/Digital-Austria-Act---das-digitale-Arbeitsprogramm-der-Bundesregierung/Einblicke-in-den-Digital-Austria-Act/Digitales-Gesundheitswesen.html).

Dr. Sonja Hebenstreit is a partner at Herbst Kinsky Rechtsanwälte GmbH, which she joined in 2005. She specialises in the fields of intellectual and industrial property law, unfair competition, life sciences and data protection. Sonja Hebenstreit represents Austrian and international clients, including biotech and tech start-ups, as well as numerous pharmaceutical and medical devices companies, in a variety of regulatory issues, licensing and other contractual matters, as well as in data protection, unfair competition and reimbursement matters.

Herbst Kinsky Rechtsanwälte GmbH
Dr. Karl Lueger-Platz 5
A-1010 Vienna
Austria

Tel: +43 1 904 2180
Email: sonja.hebenstreit@herbstkinsky.at
LinkedIn: www.linkedin.com/in/sonja-hebenstreit-76b72864

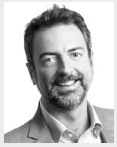
The Firm
Since its establishment in 2005, Herbst Kinsky Rechtsanwälte GmbH has become one of Austria's leading commercial law firms. Its specialised and highly committed lawyers combine many years of experience gained abroad and in reputable Austrian law firms. The Firm's practice covers a full range of services in all areas of commercial, corporate, civil and public law, including banking, insurance and capital markets, corporate and M&A, IP, IT and life sciences, merger control, antitrust and competition, data protection, real estate, dispute resolution and arbitration. The Firm has established a particularly strong presence in the field of life sciences and healthcare.

Our Clients
The Firm's clients range from large international privately held and publicly listed companies, banks, insurance companies and private equity investors to small and mid-size business entities, as well as start-ups. Clients cut across many different industries, including life sciences, energy, information technology, financial institutions and insurance.

www.herbstkinsky.at

HERBST KINSKY
RECHTSANWÄLTE GMBH

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 technologies in your jurisdiction?

In recent years, Belgium has seen a rise in the development and implementation of a number of 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.

1.3 What are the core legal issues in digital health for your jurisdiction?

The emergence of new health technologies results in changing roles for healthcare actors and challenges the boundaries of the current legal framework. With an increasingly consumer-centric approach to healthcare, patients are empowered to take an active role in the co-maintenance of their own health. In response, the role of the hospital is gradually shifting from a focus on inpatient to outpatient treatment, while the medical (tech) industry more often comes into direct contact with patients, leading to data protection and compliance concerns. The reality of an ever-increasing digitalisation of healthcare is often at odds with existing laws and regulations (concerning, for example, intellectual property protection, data protection, liability and compliance) and will continue to require swift and agile action by the legislator.

1.4 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 estimations project that the digital health market in Belgium could reach up to 800 million euros in 2024.

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

In line with question 1.4, 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.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The core healthcare regulatory schemes related to digital health are:

- the Act on the Performance of the Healthcare Professions of 10 May 2015;
- the Act on Hospitals and Other Care Facilities of 10 July 2008;
- the Health Care Quality of Practice Act of 22 April 2019;
- the Patients' Rights Act of 22 August 2002;
- the Law on Medicines of 25 March 1964;
- the 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; *In Vitro* Diagnostic Medical Devices Act of 15 June 2022;
- the 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; and
- a number of legislative initiatives and already adopted instruments in light of the EU's digital strategy, such as the Digital Services Act (EU Regulation 2022/2065), the EU proposal for an AI Act, and general data strategy, such as the Data Governance Act (DGA) (EU Regulation 2022/868) and the recently adopted Data Act (EU Regulation 2023/2854).

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

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). Lastly, a number of substantial legislative initiatives in light of the EU's digital strategy (i.e. regarding digital services, markets, content, AI, cybersecurity, etc.) will significantly impact the offering of digital health goods and services in the future.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The legislation on medical devices (see question 2.6), product liability (see question 9.1), e-commerce and the consumer protections set forth in the Code of Economic Law (CEL), Book VI are relevant to consumer healthcare devices. Intellectual property rights of software are protected by Book XI, Title 6 of the CEL.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

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) supervises the quality, safety and efficacy of medicines and health products. 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. Lastly, the Belgian Data Protection Authority (DPA) enforces compliance with data protection and the recently established Health Data Authority oversees the sharing and use of healthcare data.

2.5 What are the key areas of enforcement when it comes to digital health?

The DPA and the Market Court in Brussels ensure enforcement of 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 offenses that are criminally curbed.

2.6 What regulations 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. In addition, medical devices must 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.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

Software that is powered by AI/Machine Learning (ML) is currently governed by the same regime as other software (see questions 2.3 and 2.6). 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. It can, however, be expected that AI/ML-powered devices or software will in the future be regulated by specific instruments. In this regard, the European Parliament and the Council have just reached political agreement on the new draft regulation on AI (the AIA), which will be officially adopted shortly. 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.

3 Digital Health Technologies

3.1 What are the core legal or 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 are mainly related to the quality and credibility of online healthcare providers, and the privacy and security of patient data. There has, however, been a switch in mindset. As of 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 must 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.
- **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 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 General Data Protection Regulation (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 recent introduction of the Digital Services Package by the European Commission 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 can be reimbursed if they fulfil all criteria of the mHealth Belgium validation pyramid. In the first instance, they must be CE-certified as a medical device and meet the requirements of the GDPR. Secondly, they must 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. The procedure has recently been changed to allow more stakeholders to submit a reimbursement application and to improve the process of assessing such apps. 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 must 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. Interesting to note is that an EU-funded initiative (Label2Enable) aimed at promoting the development and implementation of an EU quality label for wellness apps is currently running.
- **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 proposed AIA and the MDR suggests that AI-powered medical devices will in the future be regulated by stringent requirements in both instruments. 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**
  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 transfer 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 which 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. This obligation has already become effective for certain healthcare practitioners, such as general practitioners, but not for all. 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) must 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).
- **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.
- **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 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 expected rules on AI will also need to be considered.

3.2 What are the key issues for digital platform providers?

Under the current regime, liability of digital platform providers for copyright breaches and other infringements has been limited (Book XII of the Code of Economic Law). Hosting providers cannot be held liable for infringements committed through their services insofar as the service provided merely consists of the storage of information provided by a recipient of the service. In addition, the platform provider may not have (had) knowledge of the illegal activity or information. Once the provider has actual knowledge of the infringement, it must act expeditiously to remove or to disable access to the information concerned and it must inform the public prosecutor of such infringement. While the "notice and take down" principle is upheld under the new EU Digital Services Act, more stringent obligations are imposed on intermediary service providers, including extensive transparency obligations. 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).

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

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 must 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 healthcare providers. 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.

4.2 How do such considerations change depending on the nature of the entities involved?

As a consequence of the introduction of e-health, the personal data of patients are no longer solely processed by physicians and other healthcare providers, 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))).

4.3 Which key regulatory requirements apply?

In the physician–patient relationship, patients have the right to consult their medical record, which should be updated and stored carefully (art. 10 of the Act on Patients' Rights, arts 22–24 of the Code of Medical Ethics of the NCOP, arts 33–40 of the Health Care Quality of Practice Act of 22 April 2019). Only healthcare providers having a therapeutic relation with the patient may access the electronic health records of a patient, excluding, for example, medical advisors from insurance companies. In the broader context of (e-)health services, one must take account of the GDPR and the Belgian Law on the Protection of Natural Persons with regard to the Processing of Personal Data.

4.4 Do the regulations define the scope of 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.)

4.5 What are the key contractual considerations?

When more than one party is involved in the processing of (health-related) personal information, both territorial aspects and the relationship between the parties must 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) must 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).

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The GDPR maintains 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.

4.7 How are issues with 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.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

Generative AI works optimally when fed with substantial amounts of high-quality training data, but it can be quite a challenge for generative AI companies to secure adequate rights to such data. On the one hand, comprehensive licence rights must be acquired if the training data used is protected by copyright or other intellectual property rights (see also question 6.2). On the other hand, if the training data contains information that can directly or indirectly identify an individual, the principles of the GDPR must be respected (including the principles of purpose limitation and data minimisation, which run counter to the idea that as much data as possible should be collected). Considering that generative AI companies do not always have a connection to the data subject whose personal data is processed by their AI system (and the source of the data is not always clear), such companies sometimes struggle to find an appropriate legal basis and inform data subjects about the processing of their personal data. Similarly, it can be difficult for data subjects to exercise their rights (i.e. the right of access, the right to rectification and the right to object) as personal data is collected, processed and produced at different stages of the AI system's deployment.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

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 European Commission's proposal of a European Health Data Space, intended to facilitate the use and sharing of European health records both for the purpose of providing healthcare services and for "secondary purposes" such as research.

5.2 How do such considerations change depending on the nature of the entities 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The sharing of data is considered to be another aspect of the processing of data under Belgian law. Correspondingly, the same regulatory requirements apply (see question 4.3). Notably, a data subject must be informed about the third parties with whom its personal data will be shared. Further, if the third party is situated outside the scope of the GDPR, adequate safeguards must be taken to protect the personal data when transferred. In addition, from 24 September 2023 onwards, the DGA has been in force in the EU, providing a framework to strengthen trust in voluntary data sharing for the benefit of businesses and citizens.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

Since 2008, a national e-Health platform has been established, where healthcare providers upload electronic health records of a patient to allow all other healthcare providers 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 Belgian Integrated Health Record (BIHR), a more advanced model of data exchange via a central digital platform which 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 Authority has recently 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.

5.5 What are the key issues 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 What is the scope of patent protection for digital health technologies?

Since there are no specific intellectual property 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 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 which 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. Patents are valid for 20 years.

6.2 What is 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 Code of Economic Law). 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 though, provided that the acquisition, verification and presentation thereof constitute a substantial investment by the author (art. XI.306 of the Code of Economic Law). Interestingly, there seems to be a legislative trend to limit the scope of copyright protection in an attempt 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, 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. Article 43 of the recently adopted 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 What is 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 Code of Economic Law). 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 intellectual property 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 What is 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 Code of Economic Law). 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 are the core rules or laws related to government-funded inventions in your jurisdiction?

The core rules and laws applicable to government-funded inventions in Belgium are noted down in the Belgian Code of Economic Law, Book XI, Title 1, Chapter 2. Irrespective of any governmental funding, the inventor is considered the person who developed the invention.

7 Commercial Agreements

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

The allocation of intellectual property rights must be carefully assessed before concluding collaborative agreements. Both the ownership of results and the intellectual property 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 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 must 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 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 must 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 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 4.8), several data protection-related challenges must 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 is the role of machine learning in digital health?

ML is valuable for a broad array of applications in digital health which can lead to more holistic care strategies that could improve patient outcomes. In this context, ML can help healthcare organisations meet growing medical demands, improve operations and lower costs, which is especially valuable for a sector characterised by limited resources. Besides, ML can help practitioners detect and treat diseases efficiently, with more precision and personalised care.

8.2 How is training data licensed?

The Database Directive laid some of the groundwork in facilitating the license of vast amounts of data. Databases may be protected either through copyright protection, if the structure of the database is sufficiently original, or through the *Sui Generis* Database Right (SGDR) for the substantial investment in obtaining, verifying or presenting the content of the database (or through both) (Title 7 of Book XI of the Code

of Economic Law). Under the SGDR, the extraction and reuse of substantial parts of a database can be commercialised for a period of 15 years from the creation date of the database or from the moment the database first became publicly available. The right of a producer of a database can either be transferred or licensed (exclusive or not).

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning 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 ML, cannot be protected by copyright if it is created without creative human involvement and does not meet the requirement of originality. As 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 considerations apply to licensing data for use in machine learning?

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. On the other hand, Belgian data protection regulation principally prohibits the processing of health-related data, unless an exception, such as consent of the data subject, applies. Moreover, the principle of data minimisation and the restrictions on data processing for a purpose other than for which it was initially collected, may directly clash with the commercial interests of tech companies.

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 and the new proposals for an updated product liability directive and an AI liability directive, for example, with the aim of more equally sharing the burden of proof for complex digital solutions between the claimant and manufacturer.

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. 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 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 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 healthcare provider). This can be challenging as it may not always be clear how the software has reached a certain conclusion. The EU legislative proposals on liability in relation to AI (i.e. the Proposal for a Directive on liability for defective products revising the existing Product Liability Directive; and the Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence) provide for the combined application of a strict (product) liability and a fault-based liability regime for AI technologies.

While 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, concrete measures to reduce the risks relating to the complexity and lack of transparency involved in AI systems are still lacking. 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.

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 requires implementation in Belgian law by 17 October 2024. NIS2 extends the scope of entities to which the NIS requirements apply to also cover hospitals and other healthcare providers. 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 must 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 must be determined and one must 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 must 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?

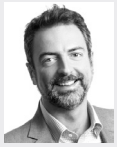
The NIHDI is responsible for the accreditation of physicians and pharmacists, while organisations such as the Joint Commission International accredits hospitals in Belgium. As the NIHDI is also the institution responsible for reimbursement decisions (see question 10.6), naturally, its endorsement of 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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with 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 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. Lastly, shortages in, for example, the chip industry have important consequences for the costs and availability of medical devices.



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
1800 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
1800 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
1800 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
1800 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 and cGMP) and compliance matters (including transfers of value, promotion of life sciences products, antitrust compliance questions, patient-directed programmes and GDPR). Its Life Sciences department is headed by Pieter Wyckmans and Olivier Van Obberghen.

www.quinz.be

Canada


Vanessa Grant


Véronique Barry


Brian Chau


Sarah Pennington

Norton Rose Fulbright

1 Digital Health

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

"Digital health" is generally 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 technologies 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 are the core legal issues in digital health for your jurisdiction?

The core legal issues in digital health in Canada include:

- regulatory compliance;
- intellectual property rights;
- data protection;
- cybersecurity; and
- practice of medicine laws.

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

According to Statista, a global data and business intelligence platform (https://www.statista.com):

- Revenue in the Canadian digital health market was projected to reach US$3.14b in 2023.
- Revenue is expected to show an annual growth rate (2023–2028) of 7.61%, resulting in a projected market volume of US$4.53b by 2028.
- The average revenue per user is expected to amount to US$109,500.
- Canada's largest market will be digital treatment and care with a total revenue value of US$1.46b expected for 2023.

1.5 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, Babylon Holdings Limited, WELL Health Technologies Corp., Cloud MD Software and Services Inc., and ThinkResearch Corp.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

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 healthcare to certain federal groups (for example, the military); while 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 provision of digital health, including:

- The *Food and Drugs Act* (Canada) (**FDA**).
- The *Medical Devices Regulations* (Canada) (**MDR**).
- Provincial laws, including professional and ethical standards.

From a regulatory perspective, the FDA, MDR and HC guidelines govern the import, sale and advertisement of devices and SaMD in Canada.

In addition, other federal statutes apply with respect to the sale and advertisement of digital health services, including, for

example: federal privacy legislation; the *Competition Act* (Canada) 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 legislation also governs the provision of digital health services, including, for example:

- legislation specifically applicable to digital health services, e.g., medical billing process and medical/privacy standards;
- legislation generally applicable to the provision of products and services (which would include digital health), e.g., consumer laws, privacy, cybersecurity and procurement rules; and
- legislation and professional standards, codes and guidelines for healthcare professionals (**HCPs**) and pharmaceutical companies, established by the legislature, industry associations, professional colleges and other self-regulatory groups.

This core health regulatory scheme is completed by emerging standards and rules adopted, such as:

- non-binding standards adopted by non-profit organisations such as the Canadian Agency for Drugs and Technologies in Health funding;
- 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; and
- 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 federal laws, such as Bill C-27, known as the *Digital Charter and Implementation Act*, which, among other things, introduces a draft *Consumer Privacy Protection Act*, draft *Personal Information and Data Protection Tribunal Act* and a draft *Artificial Intelligence and Data Act*.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

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 Quebec have their own private-sector privacy laws, which replace 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.
- Many laws impose various restrictions and requirements on access and processing of PI. Generally, informed consent must be obtained from individuals before processing their PI. Requirements for consent to be valid vary by province, but generally 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 generally must also be informed of this beforehand.
- Most laws generally 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. In Quebec, five reforms took place in less than two years after introducing a new law governing PHI, reviewing the regulatory landscape to emulate the GDPR and adopting a new law to create a Minister of Cybersecurity.

Anti-kickback and competition laws are also in force in Canada:

- The *Competition Act* (Canada) governs how businesses must deal with their competitors. Under that Act, any action viewed as promoting an anti-competitive business strategy can lead to severe penalties, ranging from injunctive actions and pecuniary penalties, to prison sentences for serious offences. Advertising by HCPs is regulated under the general advertising rules of the Act, which is administered by the Competition Bureau.
- 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 may 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 Quebec, anti-corruption compliance is enforced by a multi-sector agency under the *Anti-Corruption Act* (Quebec).

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

At a federal level:

- The FDA, MDR and other laws referred to in question 2.1 will apply, as the *Consumer Product Safety Act* does not apply to MDs, including SaMD.
- The signatories of the Canadian Product Safety Pledge will need to comply with the series of voluntary commitments imposed by the pledge, which aims to strengthen the safety of consumer products and cosmetics sold online through preventative and corrective actions.

At a provincial and territorial level, companies will need:

- To determine whether consumer protection laws are applicable and, if so, comply with their requirements. The applicability of these laws may, however, not be applicable when the person providing the relevant digital health products and services does not qualify as a "merchant" under these acts.
- To take into account product liability law.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

HC is the primary regulatory authority responsible for the

administration of federal legislation. HC launched the "Regulatory Review of Drugs and Devices" (https://www.canada.ca/en/health-canada/corporate/transparency/regulatory-transparency-and-openness/improving-review-drugs-devices.html) initiative and established the Digital Health Review Division (**DHRD**) (https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/announcements/notice-digital-health-technologies.html) within the HC Medical Device Bureau (https://www.canada.ca/en/health-canada/corporate/about-health-canada/branches-agencies/health-products-food-branch/medical-devices-directorate.html) to facilitate pre-market review of digital health technologies and to adapt to the everchanging technologies in digital health.

HC can take enforcement actions 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.
- Seizure and detention, forfeiture and destruction.

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.

HC 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.

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 HCPs.

2.5 What are the key areas of enforcement when it comes to digital health?

At a federal level, DHRD's key areas of focus include:

- Wireless MDs.
- Mobile medical apps.
- Telemedicine.
- SaMD.
- AI.
- Cybersecurity (https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/announcements/notice-cybersecurity.html).
- 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.
- Provincial and territorial 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.

2.6 What regulations 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 classified as a MD and subject to the MDR and how a software is classified as a Class I, II or III device, depending on the potential risks.

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 stated to be involved are non-serious, it 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 MDs are 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 generally show the MDs are designed and manufactured in compliance with ISO 13485 and other MD-related good manufacturing practices.

Manufacturers of Class II, III and IV MDs must also 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. Information on the licensing process is on the HC website.

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.

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.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

HC's Draft Guidance Document (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) provides that a MD that uses machine learning 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 a MD to be approved for clinical use, it will have to comply with the steps described above in order to obtain a MDEL from HC. HC highlights that when considering a machine learning MD, it will take into consideration its safety and effectiveness.

Bill C-27, known as the *Digital Charter and Implementation Act*, among other things, introduces a draft *Consumer Privacy Protection Act*, draft *Personal Information and Data Protection Tribunal Act* and a draft *AI and Data Act*.

As noted above, digital health devices that are classified as MDs will also have to comply with federal, provincial and territorial privacy laws, and with the health and other core regulatory schemes detailed elsewhere in this chapter.

3 Digital Health Technologies

3.1 What are the core legal or 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* (https://fmrac.ca/wp-content/uploads/2022/07/FMRAC-Framework-on-Virtual-Care.pdf), 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 practice, 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 have an MDEL 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 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 issues for digital platform providers?

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 to consider for use of personal data?

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 (https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/). Similarly, the federal government also has an office of the privacy commissioner that 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 do such considerations change depending on the nature of the entities involved?

All businesses that operate in Canada and handle PI that crosses provincial or national borders are subject to PIPEDA, regardless of which province or territory they are based in. PIPEDA generally applies to PI held by private-sector organisations that are not federally regulated. The following provinces have implemented health-related privacy laws that have been declared substantially similar to PIPEDA (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/) with respect to health information:
- Ontario (https://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm).
- New Brunswick (https://laws.gnb.ca/en/showfulldoc/cs/P-7.05/20121030).
- Newfoundland and Labrador (https://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm).
- Nova Scotia (https://novascotia.ca/dhw/phia/PHIA-legislation.asp).

These regulatory requirements supplement the common law and the civil law.

Where organisations collect or process PI or PHI, they are generally required to obtain an individual's consent when they collect, use or disclose that individual's PI. Individuals have the right to access their PI held by an organisation and to challenge its accuracy.

4.3 Which key regulatory requirements apply?

Federal

PIPEDA applies to private-sector organisations across Canada that collect, use or disclose PI in the course of a commercial activity (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_03_ca/).

Provincial privacy laws

Alberta (https://pipa.alberta.ca/index.cfm?page=legislation/act/index.html), British Columbia (https://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01) and Quebec (https://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1_A.html) have their own private-sector privacy laws (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/) that have been deemed substantially similar to PIPEDA. Organisations subject to a substantially similar provincial privacy law are generally exempt from PIPEDA with respect to the collection, use or disclosure of PI that occurs within that province.

As noted above, certain provinces have adopted legislation regarding PHI.

4.4 Do the regulations define the scope of data use?

Generally, data must be used for the primary purpose for which it was collected.

Under PIPEDA, the Alberta, British Columbia and Quebec Acts, an organisation is generally required to obtain consent for any collection, use or disclosure of personal data, subject to limited prescribed exceptions, which may be summarised as follows:
- appropriate notice has been provided to or made available to the data subject;
- the data subject has provided consent to the processing for the identified purposes;
- the personal data is necessary to perform a contract with the data subject;
- the personal data is necessary to comply with a legal obligation;
- the personal data is necessary to protect the vital interests of a natural person; or
- the personal data is necessary for the public interest.

4.5 What are the key contractual considerations?

The key contractual considerations include the following:
- ensuring appropriate consent for the collection of PI or PHI (and the regime for withdrawal of consent);
- ensuring compliance with privacy laws;
- restrictions on disclosure of PI or PHI and cross-border transfer of data; and
- establishing a liability regime for failure to comply with privacy laws.

A common issue in these types of agreements includes who takes the lead where there has been a data breach.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The key legal issues in Canada with securing comprehensive rights to data that is used or collected is ensuring that the appropriate consents are obtained from individuals and that organisations comply with the relevant legal requirements for the collection, use and disclosure of PI or PHI.

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

Canadian law on data inaccuracy, bias and/or discrimination is evolving. Canadian laws already address privacy, security, intellectual property and human rights. In September of 2023, for example, the federal government issued preliminary 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.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

Data-usage laws for generative AI companies are evolving in Canada. The federal government has promulgated the federal *Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems* (https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems), identifying measures that organisations are encouraged to apply to their operations when developing and managing AI systems. The federal government has also proposed federal laws, such as Bill C-27, known as the *Digital Charter and Implementation Act*, which, among other things, introduces a draft *Consumer Privacy Protection Act*, draft *Personal Information and Data Protection Tribunal Act* and a draft *Artificial Intelligence and Data Act*.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Key issues 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 do such considerations change depending on the nature of the entities involved?

The nature of the entities does not change the issues relating to the sharing of PI.

5.3 Which key regulatory requirements apply when it comes to sharing data?

As noted above, 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:

- **PIPEDA** is the general statute governing private-sector privacy considerations. Alberta, British Columbia and Quebec have their own private-sector privacy laws, which replace PIPEDA with provincial PI considerations, since they have been deemed substantially similar. The same applies to the PHI protection laws of New Brunswick, Nova Scotia, Ontario, and Newfoundland and Labrador. Other provinces have adopted PHI privacy legislation.
- Many laws impose various restrictions and requirements on the accessing and processing of PI. Generally, informed consent must be obtained from individuals before processing their PI. Requirements for consent to be valid vary by province, but generally 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 generally must also be informed of this beforehand.
- Most laws generally 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. For instance, in Quebec, five reforms took place in less than two years introducing a new law governing PHI, reviewing the regulatory landscape to emulate the GDPR and adopting a new law to create a Minister of Cybersecurity.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

There are some initiatives to establish standards in Canada. PHAC established an Expert Advisory Group (**EAG**) to advise on a pan-Canadian Health Data Strategy. In its final report, released in May of 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 will 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 incented 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 to consider with respect to federated models of healthcare data sharing?

See answer above.

6 Intellectual Property

6.1 What is 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 US patent-eligible subject matter).

The most recent guidance is the practice notice PN2020-04, providing guidance on the current understanding by the Patent Office 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.

While a simplified three-step test was proposed by an intervener in a decision relating to a computer-implemented technology and accepted in a Federal Court decision, the Federal Court of Appeal reversed this decision and struck the three-part test from the Federal Court's order, in light of the most current version of the Manual of Patent Office Practice. The current test has an "actual invention" determination conducted by the patent examiner.

6.2 What is 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.

Copyright can be protected both in a non-registered and registered form, with the benefits for registration generally 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.

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". Relative to "fair use" in the United States, in Canada, "fair dealing" is limited to specific enumerated grounds of protection. An "informational" analysis fair-dealing exception has been proposed by academics in 2019, along with a non-exhaustive approach for "fair dealing".

6.3 What is 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, machine learning models and/or trained machine learning 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 What is 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, 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 currently being tested in Canada.

In November 2021, the Canadian Intellectual Property Office (**CIPO**) issued a non-compliance notice for the Canadian patent application number CA3137161 (https://www.ic.gc.ca/opic-cipo/cpd/eng/patent/3137161/summary.html) identifying DABUS as the inventor along with a statement that "[t]he invention was autonomously generated by an AI" (the DABUS Application).

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, 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.

The current status of this patent application is "PCT Non-Compliant".

It is not clear at this point in time 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 are the core rules or laws related to government-funded inventions in your jurisdiction?

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.

7 Commercial Agreements

7.1 What 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 liability will be divided by the parties.
- Limitations of liability between the parties.
- Confidentiality obligations.
- Financial considerations: how will any resulting intellectual property be commercialised?

7.2 What 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 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 considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

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 be aware that the use of generative AI is merely an aid and not a substitute for clinical judgment.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning approaches are playing an increasing role in digital health, providing useful tools to improve the efficiency of healthcare delivery, both in respect to patient-facing technologies, automating backend infrastructure and foundational research.

Machine learning is being investigated for usage for personalising medicine delivery, improving the accuracy and consistency of health records and pattern recognition based on health informatics, among others. Machine learning is a particularly effective tool in view of population-level data availability that can be used to build increasingly accurate and robust statistical models.

Once trained, for example, a machine learning architecture can be deployed to deliver personalised outputs for a particular individual, or used to optimise process parameters for delivery of a particular digital health service or product.

8.2 How is training data licensed?

Machine learning uses training data to optimise an initial machine learning model. The training data include input/output pairs that are used to reward or penalise a particular desired outcome iteratively across a large number of iterations. In a simplified example, parameters of the machine learning model can be updated with each iteration such that over time,

the machine learning model is capable of generating a nuanced output based on the combination of parameters.

Training data often includes "labels" or "annotations", which are provided in the form of metadata that are used as additional inputs or target outputs. These labels or annotations are sometimes readily available, but in certain scenarios, the labels or annotations must be appended to raw data before the data is usable for machine learning. For example, training data can include information extracted from electronic health records, or raw images, which are then appended with additional information for providing additional inputs (or training input/output pairs) for machine learning. Labels can be licensed separately from the raw data.

Training data can have certain associated intellectual property rights (confidential information, trade secret, copyright) and privacy rights (especially those containing personal identifiable information) relating to the underlying data sets.

Training data is licensed using a variety of different types of proprietary and open-source licences. Different usage scenarios can have different licensing regimes (research/non-commercial and commercial licences). These licences impart obligations (e.g., payment, attribution, share-alike), restrictions (e.g., non-commercial, research only) or establish disclaimers (e.g., provided "as-is"). A growing area of consideration is the licensing of publicly funded or governmental data, whereby there may be additional obligations in respect of downstream benefits in exchange for data access.

Popular data-set licences can include data-set specific licences. The most common of these are the Creative Commons licences, Open Data Commons licences (**ODbL**) and the Community Data License Agreement (**CDLA**). There are different types of CDLA similar to Creative Commons licences, and these licences include useful database-specific language, which could provide more clarity when they are enforced.

There have been examples of open-source software licence terms being applied to data sets, but there are certain provisions in the open-source software licences that may not be directly applicable. Other licences include bespoke licences, and it is important to note that some bespoke licences have not been drafted by lawyers and impart a level of ambiguity.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning 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.

Specifically, for an algorithm that is improved by machine learning *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, 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 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 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 considerations apply to licensing data for use in machine learning?

From a commercial perspective, it is important to identify licence terms before deciding which data set to be used, and to monitor compliance with these licence terms.

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.

Another important commercial 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 machine learning outputs.

Similarly, a data set may inadvertently include unauthorised third-party data. These issues have been flagged in data sets such as EleutherAI's "The Pile" data set (unauthorised copies of books). A number of well-known and widely available AI tools appear to have been trained using "The Pile", as alleged in recent complaints.

It is important to note that many data sets have different licensing options that are available.

Finally, it is important to note that 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 machine learning 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.

Similarly, if a trained machine learning 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 machine learning model or the user, or both.

9 Liability

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

Unlike the European Union and other 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, a software licence), to whom the product or service is marketed and sold

(for example, is the sale to a consumer, a HCP or a business for incorporation into other devices?), and what is incorporated in the product or service (for example, AI algorithms).

Sources of product liability law in Canada include the common law (in each of the provinces and territories other than Quebec) and the civil law in Quebec. 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.

Generally speaking, 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, or failure to meet specifications. Consumer protection laws (federal, provincial and territorial) may also apply to the digital product or service. The *Canada Consumer Product Safety Act* (**CPSA**), for example, prohibits the manufacture, import and sale of products that pose a danger to human health or safety. The prohibition also extends to any advertising, packaging or labelling that may mislead consumers as to the safety of the product. 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 Quebec, consumers have similar protections under the *Civil Code of Quebec*.

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.

9.3 What are best practices to minimise liability risks posed by the use of generative AI in the provisioning of digital health solutions?

Best practices include:

- understanding the limits of the training data used to generate the information;
- 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 be aware that the use of generative AI is merely an aid and not a substitute for clinical judgment.

10 General

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

Cloud-based services raise:

- 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.: Quebec 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?

The 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 associations, colleges and orders for HCPs determine which types of products and services can be used by HCPs in order to comply with 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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with 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 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.

Vanessa Grant practises business law in our Toronto office. Her practice focuses on mergers and acquisitions, corporate finance and corporate governance for public and private corporations, including private equity and venture capital. She also provides ongoing general corporate and commercial legal advice to a number of clients.
She has worked with several national and international clients in various industries, with a particular focus on companies in the life sciences and technology sectors.

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, artificial intelligence 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 Laurier Boulevard, Suite 1500
Quebec, Quebec G1V 0B9
Canada

Tel: +1 418 640 5170
Email: veronique.barry@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/veronique-barry

Brian Chau is a patent lawyer with a background in Electrical Engineering and his work focuses heavily on intellectual property rights relating to AI and machine learning technologies. Brian has drafted a large number of granted AI and machine learning patents, both relating to foundational technologies (e.g., architectures, training approaches, optimisation) and more specific applied technologies (e.g., advanced manufacturing, autonomous vehicle/warehouse control, cybersecurity). Several AI-related granted patents drafted by Brian were highly ranked in the 2023 Evident AI Innovation report.

Norton Rose Fulbright
222 Bay Street, Suite 3000, P.O. Box 53
Toronto, Ontario M5K 1E7
Canada

Tel: +1 416 216 4831
Email: brian.chau@nortonrosefulbright.com
LinkedIn: www.linkedin.com/in/bgchau

Sarah Pennington provides strategic legal counsel across a range of industries, including the life sciences, pharmaceutical, technology and consumer product sectors. Her practice touches on all facets of intellectual property, including patents, trademarks, copyright and regulatory advice. In her litigation practice, Sarah provides strategic advice and representation to businesses and individuals faced with litigation or potential litigation. She has acted for clients in patent, trademark and copyright disputes before the Federal Court. Sarah also provides regulatory counsel to companies regulated by Health Canada, including advising on regulatory approval pathways, Patent Register listings, advertising matters and access to information requests.

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: financial institutions; energy, infrastructure and resources; technology; transport; life sciences and healthcare; and consumer markets.

www.nortonrosefulbright.com

NORTON ROSE FULBRIGHT

China


Cindy Hu


Jason Gong


Jiaxin Yang

East & Concord Partners

1 Digital Health

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

Digital health is not a legal term defined under the laws and regulations of the People's Republic of China ("PRC"), but is frequently referred to in commercial contexts and industry policies.

Digital health usually refers to the development and use of digital technologies to popularise health knowledge and its implementation to related fields, covering the application of digital technologies such as the Internet of Things ("IoT"), artificial intelligence ("AI") and big data in medical services and health management. Digital health usually utilises technologies such as big data and AI to provide solutions for medical treatment, clinical research, drug development, imaging diagnosis, health management and other medical and healthcare needs.

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

The key emerging digital health technologies include AI, mHealth, wearable devices, robotics, 3D printing, blockchain, global positioning system technology and 5G technology.

1.3 What are the core legal issues in digital health for your jurisdiction?

Personal privacy protection and data security are the core legal issues in digital health. In addition, the monopoly of healthcare data, the liability for medical damage caused by medical AI, and the ethical risks brought by the application of AI diagnosis and treatment technology are also common legal issues in digital health.

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

Influenced by COVID-19, China's online medical advantages have been highlighted, and the market share of digital health has increased continuously. According to the digital health report "2023 (I) China Digital Health Market Data Report", as of June 2023, the market size of China's Internet medical industry had reached CNY 173.43 billion and the transaction size of the pharmaceutical e-commerce industry had reached CNY 135.84 billion. It is estimated that the scale of China's digital health market will increase to CNY 4,222.8 billion in 2030, with a compound annual growth rate of 30.9%.

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

According to the relevant industry data, as of June 30, 2023, the top five digital health companies are JD Health, Alibaba Health, Ping An HealthKonnect, YSB Inc. and MedSci Healthcare.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The core healthcare regulatory schemes related to digital health include the following:

- Law of the PRC on the Promotion of Basic Medical and Health Care.
- Regulation on the Administration of Medical Institutions.
- Administrative Regulations on Application of Electronic Medical Records (for Trial Implementation).
- Administrative Measures on Standards, Security and Services of National Healthcare Big Data (for Trial Implementation).
- Administrative Measures for Internet-based Diagnosis (for Trial Implementation).
- Administrative Measures for Internet Hospitals (for Trial Implementation).
- Administrative Regulations on Telemedicine Services (for Trial Implementation) ("Administrative Regulations on Telemedicine Services").
- Detailed Rules for the Supervision of Internet Diagnosis and Treatment (for Trial Implementation).
- The Measures Regarding the Administration of Drug Information Service over the Internet.

- National Public Health Informatisation Construction Standards and Norms (for Trial).
- Guiding Opinions of the State Council on Vigorously Advancing the "Internet Plus" Action.
- Opinions of the General Office of the State Council on Promoting the Development of "Internet Plus Health Care".
- Notice of the National Health Commission's office on the Pilot Work of "Internet Plus Nursing Service".
- Guiding Opinions of the National Healthcare Security Administration on Improving the "Internet Plus" Medical Service Price and Medical Insurance Payment Policy.
- Guiding Opinions of the National Healthcare Security Administration on Actively Promoting the Medical Insurance Payment Work of "Internet Plus" Medical Services ("Guiding Opinions of "Internet Plus" Medical Services").
- Information Security Technology –Guide for Health Data Security (GB/T 39725-2020).

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The other core regulatory schemes include the following:

- Civil Code of the PRC ("Civil Code").
- Anti-Unfair Competition Law of the PRC ("Anti-Unfair Competition Law").
- Cybersecurity Law of the PRC ("Cybersecurity Law").
- Data Security Law of the PRC ("Data Security Law").
- Personal Information Protection Law of the PRC ("Personal Information Protection Law").
- Administrative Regulations on Human Genetic Resources of the PRC.
- Measures for Cybersecurity Review.
- Measures for Administration of Cybersecurity of Medical and Health Institutions.
- Interim Provisions on Banning Commercial Bribery.
- Measures for the Administration of Population Health Information (for Trial Implementation).
- Measures for the Management of Scientific Data.
- Information Security Technology – Personal Information Security Specification (GB/T 35273-2020).
- Information Security Technology – Security Requirements of Genetic Recognition Data (GB/T 41806-2022).
- Information Security Technology – Guide for Health Data Security (GB/T 39725-2020).

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The regulatory schemes that apply to consumer healthcare devices or software in particular include the following:

- Law of the PRC on the Protection of Consumer Rights and Interests.
- Product Quality Law of the PRC ("Product Quality Law").
- E-Commerce Law of the PRC.
- Regulations on the Supervision and Administration of Medical Devices ("Medical Devices Regulations").
- Rules for the Classification of Medical Devices.
- Administrative Measures on the Registration and Recordation of Medical Devices.
- Measures for the Supervision and Administration of Medical Device Production.
- Measures for the Supervision and Administration of Business Operations of Medical Devices.
- Measures for the Supervision and Administration of Online Sale of Medical Devices.
- Guiding Principles for Technical Review of Mobile Medical Device Registration.
- Guiding Principles for Registration Review of Medical Device Software Registration.
- Guiding Principles for Registration Review of Network Security Registration of Medical Devices.
- Guiding Principles for Registration Review of Artificial Intelligence Medical Device.
- Guiding Principles for Classification and Definition of Artificial Intelligence Medical Software Products ("Guiding Principles for AI Medical Software Products").
- Interim Measures for the Administration of Generative Artificial Intelligence Services.
- Classification Catalogue of Medical Devices.
- Norms on the Quality Management for the Clinical Trials of Medical Devices.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The principal regulatory authorities include the following:

- The National Health Commission ("NHC"): The NHC primarily formulates and enforces national health policies and regulations pertaining to healthcare services, healthcare institutions and healthcare professionals. Internet-based diagnosis and treatment and remote consultations between healthcare institutions are both regulated by the NHC.
- The National Medical Products Administration ("NMPA"): The NMPA regulates drugs, medical devices and cosmetics, and is responsible for the safety, supervision and management of standard formulation, registration and manufacturing to post-market risk management.
- The National Healthcare Security Administration ("NHSA"): The NHSA is primarily responsible for formulating and implementing policies related to basic medical insurance ("BMI"), such as reimbursement, pricing and the procurement of drugs, medical consumables and healthcare services.
- The Ministry of Industry and Information Technology ("MIIT"): The MIIT is responsible for the management of the Internet industry, the access management of the information and communication industry, and the construction of a network and information security guarantee system in the information and communication field. In terms of digital health, the MIIT is responsible for supervising relevant technology development, personal data protection, etc.
- The Cyberspace Administration of China ("CAC"): The CAC is responsible for the overall planning and coordination of network security and relevant supervision and administration, including regulating the cross-border transfer of healthcare data, cybersecurity review of internet hospitals, network personal privacy and information protection.
- The State Administration for Market Regulation ("SAMR"): The SAMR is responsible for supervising the market order in market transactions, online commodity transactions and related services, and organising the investigation and punishment of illegal medical advertisements, anti-commercial bribery and other acts against unfair competition.

- The National Data Bureau ("NDB"): The NDB is responsible for coordinating and advancing the construction of the basic system of data, coordinating the integration, sharing, development and utilisation of data resources, and advancing the planning and construction of digital China, digital economy and digital society in an overall manner.
- The Ministry of Public Security ("MPS"): The MPS is responsible for enforcing the Cybersecurity Classified Protection System and investigating cybercrimes, including conducting inspections and recording filings for the related system completed by healthcare institutions (internet hospitals are included), and investigating crimes related to infringement of personal data and illegal access to information systems.

2.5 What are the key areas of enforcement when it comes to digital health?

Personal information protection, data security and cybersecurity are the key areas of enforcement in relation to digital health. China has established the Personal Information Protection Law (effective from November 1, 2021), the Data Security Law and the Cybersecurity Law. The Multi-Level Protection Scheme implemented in the field of cybersecurity, as a compulsory legal obligation stipulated by the Cybersecurity Law and relevant regulations, has become a main focus in enforcement in most industries, including digital health.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

The main applicable laws and regulations include: Medical Devices Regulations; Rules for the Classification of Medical Devices; Administrative Measures on the Registration and Recordation of Medical Devices; Measures for the Administration of the Clinical Use of Medical Devices; and Guiding Principles for AI Medical Software Products.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

In addition to the relevant regulatory provisions applicable to medical devices, AI/Machine Learning ("ML") powered digital health devices or software solutions shall also comply with the Management Specification of AI-Aided Diagnosis Technology and Management Specification of AI-Aided Therapy Technology in terms of special requirements for medical institutions to carry out AI-aided diagnosis technology and AI-aided treatment technology in relation to department setting, staffing, technical management, etc.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Medical institutions shall comply with the Administrative Regulations on Telemedicine Services in terms of personnel setting, equipment and facilities, telemedicine service process, responsibility sharing and management.
- **Robotics**
  The liability arising out of medical accidents caused by robots is difficult to identify, and the division of responsibilities among producers, operators and users of intelligent robots is more complex.
- **Wearables**
  In accordance with Medical Devices Regulations and Rules for the Classification of Medical Devices, some wearables (such as hearing aids or pain relief therapeutic instruments) are regarded as medical devices, and are subject to the relevant regulatory requirements on medical devices.
- **Virtual Assistants (e.g. Alexa)**
  For virtual assistants like Siri and Alexa, problems such as eavesdropping, leakage of personal privacy and information may occur.
- **Mobile Apps**
  Mobile medical apps involve patients' electronic medical records, health records, consultation information and image data, and are highly dependent on the network and information technology. When cybersecurity or technical security is attacked or threatened, privacy and information leakage may occur.
- **Software as a Medical Device**
  In accordance with Medical Devices Regulations, Rules for the Classification of Medical Devices, and Guiding Principles for AI Medical Software Products, Software as a Medical Device ("SaMD") will be subject to the relevant regulatory requirements on medical devices.
- **Clinical Decision Support Software**
  The main application scenarios of Clinical Decision Support Software ("CDSS") include drug allergy warning, clinical guidelines, drug dose support, remote patient monitoring service, etc. CDSS systems have been applied in Chinese medical institutions; however, there are problems such as the lack of CDSS product access standards and industry regulation.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  Please refer to question 2.7.
- **IoT (Internet of Things) and Connected Devices**
  Most of the data stored or collected by the IoT terminal belongs to sensitive medical information. Once important information is leaked or maliciously modified by hackers, it will lead to cybersecurity, data and information leakage problems.
- **3D Printing/Bioprinting**
  The application of 3D bioprinting in medical treatment is still in the early stage of exploration, and no specific provisions for 3D bioprinting have been issued in China.
- **Digital Therapeutics**
  At present, digital therapy products are generally supervised as a medical device and are subject to relevant regulatory requirements on medical devices.
- **Digital Diagnostics**
  At present, digital diagnostics products are generally supervised as medical devices and are subject to relevant regulatory requirements on medical devices.
- **Electronic Medical Record Management Solutions**
  Electronic medical record management solutions systems shall comply with the provisions of Administrative Regulations on Application of Electronic Medical Records (for Trial), the Administration of Medical Records in Medical Institutions, the Notice of the National Health Commission on Further Promoting the Construction for the Informationisation of Medical Institutions with Electronic Medical Records as the Core and other relevant laws and regulations.

- **Big Data Analytics**
  The application of big data analytics in the medical field must strictly comply with the provisions of the Personal Information Protection Law, the Data Security Law, the Cybersecurity Law and other relevant laws and regulations.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Blockchain-based healthcare data sharing involves data security and medical record management, which is regulated by regulations on medical data protection and cybersecurity.
- **Natural Language Processing**
  Natural language processing involves a large number of personal oral languages which are fed back to the natural language processing system for identification and processing and, therefore, may lead to the problem of leakage of personal information and data.

3.2 What are the key issues for digital platform providers?

In terms of the healthcare sector, digital platform providers are highly regulated. In terms of industry access, digital platform providers must apply for different business licences according to their business types, for example, where the business involves online data processing, voice and image communication and other business forms, the digital platform providers are required to obtain value-added telecom service qualification; where the digital platform providers provide users with drug and medical device information through the Internet, they shall obtain the qualification of an Internet drug information service. In addition, in the process of business operation, it is also necessary to comply with the above regulatory requirements on personal information protection, data security and cybersecurity.

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

Some of the key issues for the use of personal data include how to standardise the code of conduct in such different links as collection, storage, use, processing, transmission, provision, disclosure and deletion of personal information so as to ensure the rational use of personal information without infringement.

4.2 How do such considerations change depending on the nature of the entities involved?

In addition to meeting the general provisions on the use of personal data, entities of different natures shall also comply with other relevant provisions, for example:

If the entity involved is a third party that obtains relevant personal information through sharing or joint processing in accordance with the terms of the relevant agreement, it shall process the personal information in accordance with the relevant agreement and shall not process personal information beyond the agreed processing purpose and method. If it infringes on individuals' rights and interests in terms of personal information and causes damage, it shall bear joint and several liability in accordance with the law.

If the entity involved is located overseas and has one of the following circumstances: 1) providing products or services to domestic natural persons; 2) analysing and evaluating the behaviour of domestic natural persons; or 3) under other circumstances stipulated by laws and administrative regulations, the said entity shall establish a special institution or designated representative within the territory of the PRC to handle matters related to personal information protection, and submit the name of the relevant institution or the name and contact information of the representative to the relevant department responsible for personal information protection.

If the entity involved falls within the definition of the critical information infrastructure operator ("CIIO"), it shall also abide by the Regulations on Security Protection of Critical Information Infrastructure.

4.3 Which key regulatory requirements apply?

The Personal Information Protection Law and other relevant laws and regulations stipulate the general rules on the collection and use of personal information. The use of personal information shall follow the principles of legality, legitimacy, necessity and integrity, and shall be open and transparent, and ensure the security and accuracy of personal information.

For example: 1) the data collection channel shall be legal, an advanced personal consent shall be obtained in accordance with the law. There must be an acknowledgment of the processing purpose, processing method, type of personal information processed, storage period, etc.; 2) the processing of personal information shall have legal basis and shall not excessively collect personal information; and 3) personal information collectors shall formulate corresponding internal systems for information protection.

In addition, it should be noted that: 1) certain activities performed outside the PRC related to processing personal information of natural persons residing in the PRC will also be regulated by Chinese laws; and 2) when providing the personal information of those located outside of the PRC, one shall also comply with the following requirements: a) passing the security assessment organised by the national network information department; b) obtaining a personal information protection certification from professional institutions; c) signing a contract with the overseas recipient according to the standard contract formulated by the national network information department to specify the rights and obligations of both parties; and d) special regulatory requirements of laws, administrative regulations or other conditions stipulated by the national network information department.

4.4 Do the regulations define the scope of data use?

According to the Personal Information Protection Law and other relevant provisions, the purpose, method and scope of processing personal information shall be clearly stated, and the processing shall be limited to the minimum scope to achieve the purpose of processing, and personal information shall not be excessively collected. The third party shall process personal information within the scope agreed by the individual on the processing purpose, processing method and type of personal information.

In addition, the Information Security Technology – Personal Information Security Specification (GB/T35273-2020) provides detailed guidance on data use scenarios, assumptions and scope under various circumstances.

4.5 What are the key contractual considerations?

Where a contract is signed directly between an information processor with an information provider, the terms of the contract

such as scope of data information processing, processing rules, exit restrictions, security measures, requirements for deletion, destruction or return of data and liability for breach of contract should be agreed on. The name and contact information of the personal information processor shall be informed in detail, and the purpose and method of processing the personal information, the type and retention period of the personal information processed, as well as other matters that are required to be informed according to laws and administrative regulations, shall be informed.

Where two or more personal information processors jointly process personal information, in addition to clearly specifying the above information, they shall also agree on their respective rights and obligations in the terms of the contracts.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The Civil Code clearly stipulates that a natural person's personal information shall be protected by law. For any unreasonable usage of personal information which infringes on the civil rights of individuals, the infringer shall bear civil liability according to law. For example, if a medical institution or its medical staff leak personal information, or disclose medical records without the consent of the patient, the medical institution shall bear tort liability.

The Criminal Law of the PRC stipulates corresponding criminal responsibility for infringement of citizens' personal information and violation of relevant laws.

In addition, those who violate relevant laws and regulations such as the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law or the Anti-Unfair Competition Law will also face corresponding civil, administrative and even criminal liabilities.

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

The Technical Guide for Clinical Trial Data Management regulates the management of clinical trial data and the prevention and treatment of data errors and deviations from the following aspects: the responsibilities, qualifications and training of data management-related personnel; the requirements of the management system; the standardisation of test data; the main contents of data management; the guarantee and evaluation of data quality; and safety data and severe adverse drug reaction cases.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

Generative AI companies shall comply with the provisions of the Interim Provisional Measures for the Administration of Generative Artificial Intelligence Services (effective from August 2023), which stipulates the development and governance of generative AI technology, service specifications, supervision and inspection, etc. Generative AI companies shall fulfil their obligations of network information security and personal information protection when providing services.

According to the requirements of the Measures, the relevant state authorities will subsequently improve the scientific supervision methods compatible with the development of innovations and formulate the corresponding categorised and graded supervisory rules or guidelines in light of the characteristics of generative AI technology and its service application in the relevant industries and fields.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The key issues to consider when sharing personal data include the following:

- whether the sharing of personal data complies with the principles of necessity and realisation of legitimate purposes;
- whether to inform and obtain personal consent;
- whether it meets the requirements of security measures necessary for data sharing;
- whether the contract signed by all parties to data sharing includes terms such as: the processing purpose; duration; processing method; type of personal information; protective measures; and rights and obligations of both parties;
- whether there is personal data that is prohibited from being shared; and
- whether a cross-border data transfer is involved.

5.2 How do such considerations change depending on the nature of the entities involved?

In addition to meeting the general data sharing requirements, entities of different natures should also comply with other relevant provisions, for example:

If the sharing party is the CIIO, it shall also abide by the Regulations on Security Protection of Critical Information Infrastructure.

However, if the receiving party is an overseas entity, specific conditions shall be met. For example, it must have passed the security assessment organised by the national network information department, passed the personal information protection certification conducted by professional institutions, or entered into a contract with the overseas recipient according to the standard contract formulated by the national network information department to stipulate the rights and obligations of both parties.

5.3 Which key regulatory requirements apply when it comes to sharing data?

First, the provider of the shared data shall: 1) conduct the impact assessment of personal information protection in advance; 2) inform the individual of the recipient's name, contact information, processing purpose, processing method and type of personal information, and obtain the individual's consent; 3) agree with the recipient on the purpose of entrusted processing, time limit, processing method, type and protection measures of personal information, as well as the rights and obligations of both parties; and 4) supervise the recipient's processing activities of personal information.

Secondly, the recipient of the shared data shall: 1) process personal information according to the agreement, and shall not process personal information beyond the agreed processing purpose and processing method; 2) if the relevant contract is not effective, invalid, revoked or terminated, the personal

information shall be returned or deleted and shall not be retained; 3) without the consent of the provider, the recipient shall not entrust others to process personal information; and 4) the recipient shall also take necessary measures to ensure the security of personal information and assist the provider in performing its personal information protection obligations.

In addition, attention should also be paid to the regulatory requirements involved in the cross-border transfer of personal information. For example, the CIIO or the personal information processor who processes personal information up to the amount specified by the national network information department shall store within China the personal information collected and generated in China. If it is necessary to provide it to an overseas recipient, the security assessment organised by the national network information department shall be passed. (If the laws, administrative regulations and national network information department stipulate that the security assessment may not be carried out, such stipulations shall prevail.)

In accordance with the Measures for Cybersecurity Review (issued on December 28, 2021, and effective on February 15, 2022), if network platform operators who hold personal information of more than 1 million users are to be listed abroad, they shall apply to the cybersecurity review office for cybersecurity review.

The Interim Measures for the Administration of Overseas Securities Offering and Listing by Domestic Enterprises issued by the China Securities Regulatory Commission (issued on February 17, 2023, and implemented on March 31, 2023) also clearly stipulate that domestic enterprises engaged in overseas issuance and listing activities shall strictly comply with national security laws and regulations such as network security and data security. For those involving security review, relevant security review procedures shall be carried out in accordance with the law before submitting an application for issuance and listing to overseas securities regulatory authorities, exchanges, etc.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

In March 2023, the General Office of the Central Committee of the Communist Party of China and the General Office of the State Council jointly issued the Opinions on Further Improving the Medical and Healthcare Service System, which stated, "[t]o build an industrial Internet platform for the medical field, accelerate the application of the Internet, blockchain, Internet of Things, artificial intelligence, cloud computing, big data, etc., in the field of healthcare, and strengthen health medical big data sharing and exchange and protection system construction". According to the Opinions, the standards for sharing medical data will be gradually improved in the future.

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

The federated models of healthcare data sharing are in the stage of exploration and gradual development in China, and there are no specialised laws and regulations to regulate this issue for the time being. Before the introduction of specialised laws and regulations, healthcare data sharing should follow the provisions of the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law and other relevant laws and regulations.

6 Intellectual Property

6.1 What is the scope of patent protection for digital health technologies?

Any technical solutions using natural laws can be the subject matter of invention patents or utility model patents. According to the International Patent Classification List published by the State Intellectual Property Office, technologies related to digital health can be patented. After a patent is granted, unless otherwise stipulated in the Patent Law of the PRC ("Patent Law"), no entity or individual may exploit the patent without the permission of the patentee.

6.2 What is the scope of copyright protection for digital health technologies?

The subject of copyright protection covers various works, which refers to intellectual achievements that are original and can be expressed in a certain form in the fields of literature, art and science. Software copyrights are available for software related to digital health. According to the Copyright Law of the PRC, copyright includes both property rights and personal rights, of which property rights mainly include: reproduction rights; distribution rights; and rental rights.

6.3 What is the scope of trade secret protection for digital health technologies?

In accordance with Chinese laws, a trade secret refers to commercial information such as technical information and business operation information not known to the public, which is of commercial value, and for which the rights holder has adopted corresponding confidentiality measures. In accordance with the Anti-Unfair Competition Law, obtaining trade secrets by improper means, disclosing and using trade secrets obtained by others by improper means, disclosing and using trade secrets in his possession but in violation of confidentiality obligations, or abetting, luring and helping others to commit such acts are all acts of infringing trade secrets and corresponding civil liabilities can be imposed. Serious trade secret infringements are defined as a criminal offence under the PRC Criminal Law and is punishable by up to 10 years' imprisonment. Trade secrets related to digital health are also protected by the above laws.

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

In China, the laws currently applicable to academic technology transfers include the Law on Scientific and Technological Progress of the PRC (revised in 2021), the Law on Promoting Transfer and Commercialisation of Scientific and Technological Achievements of the PRC (revised in 2015) and Several Provisions on the Implementation of the Law on Promoting Transfer and Commercialisation of Scientific and Technological Achievements of the PRC issued by the State Council of the PRC in 2016. Such laws and regulations have adjusted previous policies in this field and clarified that the project undertakers, on the premise of no conflict with national security or national/public interests, are legitimately authorised to own relevant intellectual property ("IP") rights arising from the government-funded projects. Furthermore, the project undertakers are

encouraged to legally transfer and commercialise these IP rights in various ways. However, any transfer or exclusive license to an overseas company shall be approved by the project administration organisation.

Public universities are conducting pilot programmes in guiding scientific researchers to transfer and commercialise IP rights in line with the laws. According to a document jointly issued by four national-level Ministries in 2020, Chinese universities will gradually establish disclosure systems for service inventions, establish and perfect technology transfer and IP management and operation departments, and explore the reforming of ownership of service inventions, such as division of ownership between universities and researchers, as well as permitting the scientific researchers to apply for patents in the form of non-service inventions in the event the university declines to apply for service patents.

6.5 What is the scope of intellectual property protection for software as a medical device?

SaMD enjoys two forms of protection in China. First, as it is regarded as a type of work protected under copyright, it does not require an application and examination process. Although the protection period is long, the disadvantage is, it is the form of expression that is eligible for copyright protection and not the technical idea. Secondly, SaMD can be protected as it is considered an invention patent. It should be noted that pure algorithms or calculation rules are unpatentable subject matter under the Patent Law: only when the technical features of the hardware are included in the claims can it be considered to be protected. Unlike copyright, what is protected by a patent is the technical solution itself and, therefore, this type of protection is thought to be more powerful.

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

In accordance with the current laws and regulations of the PRC, an inventor refers to a person who has made creative contributions to the substantive characteristics of an invention. It is generally understood that the inventor should be a natural person and, therefore, based on the current effective laws and regulations, AI devices are unlikely to be recognised as inventors in China.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

Please refer to question 6.4.

7 Commercial Agreements

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

In the case of collaborative improvements, a written contract is required to agree on the rights and obligations of each party; and it is necessary to take into account how to handle the failure of collaborative improvements, as well as the ownership and use of rights of patents and non-patented technologies generated in the collaboration. In the absence of such a written contract, according to the provisions of the Civil Code, the right to apply for a patent shall be jointly owned by the parties to the collaborative improvements. If one party transfers the patent application right jointly owned with other parties, the other parties shall have priority to such transfer under the same conditions. If there is no agreement or the agreement is not clear about the non-patented technological achievements, all parties have the right to use and transfer such achievements.

For Sino-foreign collaborative improvements, it is also necessary to consider the possible application of some mandatory laws and regulations. For example, if Chinese human-genetic resources are involved, especially in cases exporting Chinese human-genetic resource materials, according to the provisions of the Biosecurity Law of the PRC, an approval from the competent department must be obtained. Furthermore, as for the technological achievements produced by using Chinese human-genetic resources to carry out international cooperative research, the patent rights shall be jointly shared by the parties according to the Administrative Regulations on Human Genetic Resources of the PRC.

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

When signing agreements with non-healthcare companies, in addition to meeting the above requirements for data sharing, transmission and other processing, healthcare companies shall ensure that non-healthcare companies comply with the national and industrial regulations and requirements of the business they are engaged in, have the necessary business qualifications, have the abilities to implement relevant laws and regulations, implement relevant standards and guarantee data security, and have a comprehensive management system.

According to the Measures for Cybersecurity Review, if a healthcare company qualifies as a CIIO, when it purchases network products and services, it shall anticipate the potential national security risks after the products and services are put into use. Those products and services that affect or may affect national security shall be reported to the cybersecurity review office.

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

The agreements should clearly stipulate how the parties will divide the legal responsibility in the event of a data leakage incident causing damage to a third party.

In addition, if one of the subjects of the agreement is a non-healthcare company, please refer to question 7.2.

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

The parties using generative AI shall comply with the relevant provisions of the Interim Provisional Measures for the Administration of Generative Artificial Intelligence Services. The service providers are required to comply with service specifications and the using party shall, as far as possible, review whether the provider of the generative AI technology has assumed the responsibility of a network information content producer, fulfilled the obligations of network information security and personal information protection, in order to avoid penalties by the competent authorities as a result of the provider's failure to fulfil the above responsibilities or obligations, which could further affect the use of AI.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

As a common form of AI, ML is widely used in AI-aided diagnosis and treatment, medical imaging, wearable devices, genetic testing, pharmaceutical research, personal health management and hospital management, etc.

8.2 How is training data licensed?

Data licensing in AI involves the licensing of relevant IP rights, such as patents, software copyrights and trade secrets, and the licensed use shall apply to the Anti-Unfair Competition Law, the Patent Law, the Regulations on the Protection of Computer Software and relevant provisions.

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

According to the existing effective laws and regulations, AI can neither be an author in the context of the Copyright Law, nor an inventor or designer in the context of the Patent Law. As a result, the existing laws and regulations do not cover this area. However, with the rapid development of AI technology, the legislation of IP protection of AI-generated contents is an important issue that needs to be urgently addressed. Chinese academia has been holding discussions on this issue as well. However, to date there is no unified understanding or relevant legislative proposals.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Licensing data for use in ML in a business context mainly includes the applicable scope of licensing (duration, territory, sub-license or not), restrictions of data use, non-competition and confidentiality.

9 Liability

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

The Civil Code, the Product Quality Law, Administrative Regulations on Telemedicine Services and relevant provisions have specified the liabilities of adverse outcomes in digital health solutions.

Where defects in medical devices and other digital health products cause personal injury or damage to others, victims may claim compensation from the manufacturer of the products or the vendor of the products. After one party makes compensation, that party has the right to seek indemnification from other parties who may be held liable.

If any damage or harm to a patient is caused during the course of diagnosis and treatment by the defects of digital health products, such patient may request compensations from the manufacturer or the relevant medical institution. After making the compensation, the relevant medical institution has the right to recover the losses from the liable medical device manufacturer.

When a dispute occurs in the course of remote medical services, the inviter shall bear corresponding legal liabilities for remote consultation, and the inviter and the invitee shall jointly bear corresponding legal liabilities for remote diagnosis. In terms of remote consultation, where medical institutions conduct remote consultation, the invitee shall provide diagnosis and treatment opinions, and the inviter shall specify the diagnosis and treatment plan. In terms of remote diagnosis, where an inviter and invitee establish a counterpart support or form a medical consortia and other cooperative relationships, the inviter shall carry out auxiliary examinations such as medical imaging, pathology, electrocardiogram and ultrasound; the invited medical institution at a higher level shall conduct diagnosis, and the specific process shall be specified by the inviter and invitee through an agreement.

9.2 What cross-border considerations are there?

According to the relevant provisions of the Personal Information Protection Law, where a personal information processor needs to provide personal information to any party outside China, it should first obtain the individual's consent and conduct advanced assessment of the impact on personal information protection. If the data involves medical and health data, advanced security assessment and review shall also be carried out.

Pursuant to the Special Administrative Measures (Negative List) for Foreign Investment Access (2021 version), the provision of medical services by foreign medical service providers in China is limited to the form of Sino-foreign joint ventures, and foreign medical service providers shall not establish medical institutions in China in the form of sole proprietorship. In addition, foreign investment in the development and application of human stem cells, genetic diagnosis and treatment technologies is prohibited in China.

Where imported digital medical devices are involved, registration or filing of medical devices shall be completed according to the Medical Devices Regulations and relevant provisions, and overseas applicants shall submit the application materials to the medical products regulatory authority through a domestic enterprise, as well as the documents certifying the approval of the marketing of such medical devices by the competent department in the country/region where the applicants are located. (It is not required to submit such documents for innovative medical devices that have not been marketed abroad.) Furthermore, the instructions and labels of imported medical devices shall meet the relevant requirements.

The Interim Measures for the Administration of Overseas Securities Offering and Listing by Domestic Enterprises and relevant supporting regulatory guidelines clearly stipulate that domestic enterprises engaged in overseas issuance and listing activities shall strictly comply with foreign investment laws and regulations. Among them, Article 8 (1) stipulates that the situations where issuance and listing are not allowed include: 1) the "Negative Market Access List" issued by the National Development and Reform Commission and the Ministry of Commerce prohibits listing and financing; and 2) there are situations where laws, administrative regulations, and relevant national regulations restrict or prohibit listing and financing in areas such as industrial policy, safety production and industry supervision.

9.3 What are best practices to minimise liability risks posed by the use of generative AI in the provisioning of digital health solutions?

The users and providers of generative AI should reduce the risk of future liability by signing agreements. The agreements should include, but not be limited to, the following clauses: 1) the sharing of legal liability in the event that the AI causes infringement to a third party; 2) the sharing of liability between the parties in the event that such parties are penalised due to the AI's failure to comply with the Interim Provisional Measures for the Administration of Generative Artificial Intelligence Services and other laws; and 3) the sharing of legal liability in the event that the AI is used inappropriately or is technically defective.

10 General

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

Cloud-based services mainly involve issues such as cybersecurity and data protection. Users upload data to the cloud and cloud service providers will manage the data. This may cause issues such as cybersecurity and data breaches and information leakage.

In addition, medical and health data are required to be stored within the territory of China, and those that need to be provided overseas shall be subject to a safety assessment and review according to the relevant regulations. As for service providers who have established data centres in multiple jurisdictions, there may be a risk of illegal cross-border data transfer.

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

Non-healthcare companies that plan to independently and directly engage in the digital health industry should first obtain the qualification licence for the corresponding business according to law. For example, those intending to provide online consultation, paid medical information and other services and construct a medical big data cloud-based platform through medical websites and apps, shall obtain the approval of regulatory agencies and the relevant qualification licences.

If non-healthcare companies such as Internet companies intend to engage in the digital healthcare industry by cooperating with medical institutions, they shall agree with the cooperative medical institutions in a written agreement on the methods of cooperation, the responsibilities and rights of each party in medical services, information security, privacy protection and other aspects.

If non-healthcare companies choose to develop and produce AI medical software, wearable medical devices and other products, they shall also comply with relevant regulatory requirements on medical devices and AI-aided diagnosis technologies.

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

Apart from business models, business prospects and other commercial factors, VC and PE investors should also pay attention to key issues such as market-access requirements for the industry that the target company falls into, the business qualification and business licence, core technologies and key technicians, procedures for obtaining ownership of relevant IP rights, hardware facilities and cybersecurity protection, etc.

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

Pursuant to the Measures for the Administration of the Clinical Application of Medical Technologies and relevant provisions, medical technologies in China are subject to a "categorised" regulation system. AI-aided diagnosis and AI-aided treatment fall within the scope of "restricted technology", and a medical institution intending to carry out the clinical application of such restricted technology shall conduct self-assessment according to the standards for the administration of the clinical application of medical technologies. A qualified institution may carry out clinical application and shall report to the health administrative department for filing. New medical technologies which have not been verified in clinical practice are considered to fall within the scope of "prohibitive technology" and cannot be used in clinical diagnosis and treatment.

The clinical adoption of digital health products that fall into the scope of medical devices shall go through approval or filing procedures according to the Administrative Measures on the Registration and Recordation of Medical Devices, the Measures for the Administration of the Clinical Use of Medical Devices and relevant provisions, and shall comply with the requirements in the aspects of clinical trial institutions, systems, procurement, operation management and handling of safety involving the use of medical devices, failing which will result in administrative penalties from the competent authorities.

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 China, there are no physician certification bodies that influence the clinical adoption of digital health solutions. The qualification licence and relevant requirements for physicians engaged in clinical adoptions are mainly stipulated under the Physicians Law of the PRC, the Measures for the Administration of the Clinical Application of Medical Technologies, the Measures for the Administration of the Clinical Use of Medical Devices and relevant provisions.

The China Medical Practitioner Association mainly performs the following duties: to implement industry management, formulate self-discipline rules, provide support such as legal assistance for medical practitioners, provide continuous education for medical practitioners and organise academic meetings and seminars.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

In China, if patients have subscribed to or are covered by BIM, and the expenses of medical treatment items and medical service facilities are partially or completely covered by the BIM catalogue, the relevant expenses can be settled and reimbursed according to the medical service agreements signed between the government medical insurance agency and the designated

medical insurance institutions. In addition, patients can purchase private insurance and be reimbursed for relevant medical expenses from private insurance companies.

After the promulgation of the Guiding Opinions of "Internet Plus" Medical Services on October 24, 2020, "Internet Plus" Medical Services was formally permitted under the medical insurance payment. The expenses of examination and prescription incurred from return visits in "Internet Plus" Medical Services-designated medical insurance institutions by the insured in areas subject to overall planning can be reimbursed according to relevant regional medical insurance policies.

10.7 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.

With the advent of the digital era, digital health has undoubtedly become a key area in the construction of digital China. However, the current construction of digital health in China is still in its infancy.

We believe that in the future, China's digital health industry may have the following development trends:

First, "data" and "networks" are the core components of digital health. In the future, China may incorporate the informatics digital construction of medical institutions and medical service into new infrastructure.

In addition, as an emerging medical industry, digital health will profoundly change the medical organisational forms and medical behavioural patterns. The traditional Chinese legal governance framework, government management systems and multi-party relationship of rights, responsibilities and interests need to be readjusted or supplemented. In the future, China may: strengthen and improve the research work of digital medical legislation; improve relevant legislation in light of China's own industrial characteristics and international development trend; formulate and improve the healthcare data construction, opening, sharing and trading systems; clarify the rights and obligations of each participant in digital health; strengthen algorithm governance; and improve the risk-sharing mechanism of digital healthcare, to ensure the healthy and sustainable development of the digital health industry in China through legislation. In November 2022, the NHC and three other departments jointly released the "14th Five-Year Plan" for National Health Informatisation, which proposed the overall goal of "by 2025, we will initially build and form a unified, authoritative and interconnected national health information platform support and security system, and basically achieve the full coverage of public health institutions and the national health information platform".

Meanwhile, digital health, as a new medical model and business form, has also created new regulatory issues such as information leakage and privacy protection. In order to solve relevant problems, China will establish a governance mode compatible with the sustainable and healthy development of the digital health industry, innovate a coordinated governance model, and build a collaborative, efficient, inclusive and prudent digital medical supervision mechanism.

At last, the development of the digital health industry has accelerated the flat development of the medical service system structure. It is an inevitable trend to explore multiple co-governance in the new medical service system. In the future, industry self-regulation, platform governance, patient and medical staff rights protection may become increasingly important.

Cindy Hu focuses on the areas of corporate M&A, corporate finance and compliance. She is heavily involved in the pharmaceutical and healthcare industry, and leads the pharmaceutical and healthcare team of East & Concord.
Cindy has routinely advised well-known Chinese state-owned and private enterprises, publicly listed companies, and PE/VC funds in the area of pharmaceuticals and healthcare. She was recognised as one of the Top 15 M&A Lawyers by *ALB China*, as well as one of the Client Choice: Top 15 Compliance Versatile Practitioners by *LEGALBAND*. She was also endorsed as a Leading Lawyer in Corporate M&A by *Asialaw Profiles* and China's Top Lawyers (Corporate and M&A) by *LEGALBAND* multiple times. Cindy's team ranked on the list of Life Sciences and Healthcare in *The Legal 500* in 2022, and Pharmaceuticals and Life Sciences in *Asialaw Profiles* in both 2022 and 2023. Cindy is widely published both in China and internationally.

East & Concord Partners
22/F Landmark Building Tower 1, 8 Dongsanhuan Beilu
Chaoyang District, Beijing 100004
China

Tel: +86 10 6590 6639
Email: cindyhu@east-concord.com
URL: www.east-concord.com/tuandui/Article/201711/ArticleContent_550.html

Jason Gong is a partner in the Intellectual Property Department and a key member of the pharmaceutical and healthcare team of East & Concord. Jason's services cover various IP rights procurement and management, due diligence, enforcement and anti-counterfeiting, including both non-contentious, such as patent/trademark prosecution, advising on patent validity and freedom-to-operate, infringement analysis and consulting on patent portfolios, as well as contentious fields, such as patent validity proceedings, infringement litigation, customs protection and other administrative actions against infringers, and IP enforcement at fairs.
Jason has extensive experience in IP protection for the chemical industry, including pharmaceutical and life sciences. He represents foreign industry giants in pharmaceutical, agrochemical and refrigerant sections, and also local prestigious universities and academic centres. He frequently provides patent-focused advice for many bio-pharma companies and start-ups.

East & Concord Partners
22/F Landmark Building Tower 1, 8 Dongsanhuan Beilu
Chaoyang District, Beijing 100004
China

Tel: +86 10 6590 6639
Email: jianhua_gong@east-concord.com
LinkedIn: www.linkedin.com/in/jasongong86

Jiaxin Yang is the backbone member of the pharmaceutical and healthcare team of East & Concord, with extensive experience in M&A, compliance and risk control in the healthcare sector. She regularly provides support and advice for well-known Chinese state-owned and private enterprises, foreign-invested companies, as well as PE funds on projects concerning stem cell R&D, digital health, wearable medical devices, cybersecurity and data protection.

East & Concord Partners
22/F Landmark Building Tower 1, 8 Dongsanhuan Beilu
Chaoyang District, Beijing 100004
China

Tel: +86 10 6510 7422
Email: yangjiaxin@east-concord.com
URL: www.east-concord.com

East & Concord Partners ("East & Concord") has a well-earned reputation as one of the largest and most comprehensive law firms in China. With more than 600 legal professionals, the firm advises multinational companies, publicly listed companies, privately owned companies, state-owned enterprises, foreign invested companies, government offices and public institutions on a wide range of areas. Headquartered in Beijing, the firm has eight offices strategically located throughout China. The firm has also established extensive cooperation with many well-known international law firms so as to satisfy the development need for economic globalisation.
With more than 20 years of experience, the firm has gained a leading position and earned clients' trust and recognition in areas including: banking and finance; M&A; anti-dumping and anti-subsidy; pharmaceutical and healthcare; infrastructure and project financing; intellectual property; government legal affairs; cybersecurity and data protection; and dispute resolution.

www.east-concord.com

天達共和律師事務所
East & Concord Partners

Denmark

Kennedys Copenhagen


Heidi Bloch


Julia Tomaszewska


Janus Krarup

1 Digital Health

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

Although Denmark is one of the most digitalised economies and societies in the EU with a healthcare system characterised by extensive digitisation, electronic communication between healthcare providers and systematic use of data and digitised working procedures, there is no formal definition of "digital health" under Danish law.

The term "digital health" is used as a broad umbrella term referring to a wide range of hardware and software technologies used within the healthcare sector, including electronic medical records, telemedicine, robotic surgery, mobile apps, medical devices and much more.

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

In Denmark, healthcare services are among the most digitised in the world due to a long tradition of focusing on implementing and integrating digital solutions. The fundamentals for the advanced digital infrastructure in the healthcare sector in Denmark were created in the 1960s with the implementation of the Danish Civil Registration System (the CPR-register). The Danish CPR-register allows for a unique digital identification of all citizens with a unique person ID issued at birth to all Danes. The CPR-register allowed records of treatment, medicine, diagnosis and social care efforts to be traced across the entire Danish population forming the basis for digital health in Denmark.

A prime example of digital health in Denmark is sundhed.dk ("health".dk), which is the official Danish eHealth Portal providing both access to and information about all the Danish Healthcare Services. The platform facilitates communication and information exchange between citizens and healthcare professionals and enables all Danish citizens to access updated healthcare information from national health registers, medical records, laboratory tests, medications, and more.

Another example of digital health in Denmark is the Shared Medication Record ("*Fælles Medicinkort*"), which is an electronic register that provides citizens and healthcare professionals a digital overview of a patient's current medication. Citizens are able to look up information about their current and previous prescriptions as well as order renewals of their prescriptions. Patients are also able to access the shared medication record through sundhed.dk.

The e-record ("e-Journal") system is also an example of a system that gives both patients and healthcare professionals digital access to information from all public hospitals, including information on treatment, diagnoses, etc.

Some of the next key emerging digital health technologies in Denmark are in the areas of AI, telehealth and robot technology. Several platforms have already been launched in Denmark in order to develop and implement new solutions within these areas. One such platform consists of three centres: the Centre for Clinical Robotics (CCR); the Centre for Clinical Artificial Intelligence (CAI-X); and the Centre for Innovative Medical Technology (CIMT):

- CCR aims to improve hospital treatment and workflows by bridging robot technology and clinician needs.
- CAI-X focuses on bringing engineers, doctors and companies together to create AI solutions that address clinical workflows.
- CIMT focuses on apps, telemedicine, home monitoring, video consultations, VR and wearables.

With regard to telehealth, telemedicine, including tele-psychiatry solutions, is becoming more widespread in the Danish regions and municipalities and is currently one of the main focus areas within digital health in Denmark. Telemedicine enables patients to receive their treatment or part of their treatment in their home.

1.3 What are the core legal issues in digital health for your jurisdiction?

Given the nature of digital health solutions, which involve the processing of significant quantities of health information, including sensitive personal data, data privacy and cybersecurity emerge as paramount concerns. Safeguarding the integrity and confidentiality of this data is of the utmost importance in the realm of digital health. Processing of personal data, including health data, is regulated by national and EU regulations, including the EU Regulation 2016/679 (General Data Protection

Regulation – "GDPR"). Digital health solutions must adhere to strict privacy and data security standards, obtain informed consent, and handle data lawfully and transparently.

Another key issue in digital health is medical device regulation. Digital health solutions that qualify as medical devices must meet regulatory requirements. This includes obtaining necessary certifications, demonstrating safety and efficiency, and complying with quality standards.

In addition, liability and responsibility is also a core issue. Determining liability in digital health incidents is vital.

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

In recent years, Denmark has been at the forefront of digital health adoption and has invested significantly in digital healthcare infrastructure and initiatives.

However, there is no publicly available information.

More generally, it has been estimated that the revenue in the Danish digital health market will reach US$ 499.10m in 2024.

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

No public data is available.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

There is no comprehensive regulatory scheme related specifically to digital health under Danish law and Danish legislation regarding healthcare is generally characterised by a healthcare system that is government-funded with universal access.

Generally, Danish healthcare legislation is relatively broad and able to apply to digital health. The Danish Health Act ("*Sundhedsloven*") encompasses all legislation on benefits pertaining to public healthcare, including mental healthcare and patient's rights. However, in order to future-proof the Danish healthcare legislation, numerous acts, including the Danish Health Act, have been generally and continuously adapted to the ongoing digitalisation.

As an EU member, Denmark has an obligation to follow the EU rules. Therefore, Danish healthcare legislation changes on an ongoing basis and regulatory agencies also play an important role in administering healthcare-specific legislation in Denmark. As an example, the Danish Medicines Agency ("*Lægemiddelstyrelsen*") administers the medical devices legislation in Denmark, the Danish Act on Medical Devices ("*Lov om medicinsk udstyr*") and the related executive order on medical devices and *in vitro* diagnostic medical devices. The act is a framework act empowering the Danish Minister for Health to lay down the rules necessary for the implementation and application of the medical device legislation of the EU. Likewise, the Danish Medicines Agency has prepared a number of guidance documents in the area of medical devices for users, healthcare professionals and medical device companies to assist them with the interpretation of the requirements of the legislation.

The relevant EU regulation 2017/745 on medical devices (MDR) and the EU regulation 2017/746 on *in vitro* diagnostic medical devices (amended by regulation (EU) 2023/607 as regards the transitional provisions) are also directly applicable in the EU countries, including Denmark, supplemented by national executive orders.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

- The GDPR.
- Directive (EU) 2016/1148/EU of 6 July 2016 on Network and Information Security systems implemented into Danish law via sector-specific regulation.
- Act no. 3 of 3 January 2019, The Danish Product Safety Act.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

There is no regulatory scheme that applies to consumer healthcare devices or software in particular under Danish law. With regard to software in particular, please see question 2.6.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The Ministry of Health is responsible for the financing of medical devices and establishes the framework for the provision of health services. The Minister of Health also has the right to formulate specific requirements about the use of information and communication technology in the Danish healthcare system, including requirements concerning standardisation, use of common infrastructure, etc. The Ministry of Health is responsible for effectuating the intentions of the law. This implies ensuring enhanced overall national coordination of the development of digital health throughout the Danish healthcare sector.

The Danish Medicines Agency ("*Lægemiddelstyrelsen*") monitors the Danish market and ensures that incidents and accidents with medical devices are followed up so that causes are investigated and measures can be taken. Moreover, the agency interacts with the European Commission and other authorities and exchanges information on medical devices and safety matters.

The Safety Technology Authority ("*Sikkerhedsstyrelsen*") administers the Danish Products Safety Act. The authority supervises, monitors and issues orders and imposes fines for violations of the Danish Product Safety Act. The Safety Technology Authority may act both following a notification or on the basis of its own investigation, and its decision may be appealed to the Danish courts.

2.5 What are the key areas of enforcement when it comes to digital health?

The primary areas that regulatory authorities are targeting in relation to digital health are confidentiality, data security, data protection obligations, legal qualification as a medical device, medical secrecy regime, liability in case of damage and safety.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

In Denmark, the regulations for software as a medical device and its approval for clinical use are primarily governed by the Danish Medicines Agency ("*Lægemiddelstyrelsen*") and the Danish Health Authority ("*Sundhedsstyrelsen*"). These regulatory bodies have specific guidelines in place to ensure the safety, efficacy and quality of medical devices, including software used in a healthcare context.

The key regulations that apply to software as a medical device in Denmark and its approval for clinical use include:

- The MDR, which provides a comprehensive framework for the regulation of medical devices across the EU.
- The Danish Act on Medical Devices ("*Lov om medicinsk udstyr*"), which aligns with the MDR and specifies additional requirements for medical devices, including software marketed in Denmark.

According to Danish legislation, medical devices are not defined by the media or material that makes up the device, but by the intended purpose. Hence, while the software itself could be a medical device, it could also be a component of a medical device.

The full medical device definition is found in art. 2(1) of the MDR. Since the medical device definition is very broad, the European Commission has issued guidance for classifying software as medical devices.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

Please see the response to question 2.6. Like other software, AI-based software is classified as a medical device if it provides an effect in connection with, for example, diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of diseases for an individual.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Telemedicine involves the collection and processing of sensitive patient information and depends on reliable and secure telecommunications infrastructure. Health data protection, data privacy, network security, confidentiality, etc. are all core issues. Additionally, liability and professional standards and making sure that telemedicine services comply with Danish regulations are also key.
- **Robotics**
  Manufacturers and distributors of robotic technologies used within the healthcare system must conform to the Danish Product Liability Act, making product safety a core issue. Also, robotic systems used within the healthcare sector interact with health data, making data protection and privacy key.
  Ethical considerations including AI biases and safety standards are also worth mentioning.
- **Wearables**
  As mentioned under question 2.6, whether a device or software falls under the regulatory framework of medical devices depends on the intended purpose. Hence, depending on the wearable's features, strict compliance requirements for medical devices may apply.
  Additionally, as with telemedicine and robotics, data privacy and the protection of sensitive health data collected by the wearable are core issues. Depending on the wearable, product safety regulations might also apply.
  Legal issues might also arise with regards to advertising and marketing of wearables in Denmark, as this would be subject to the rules of the Marketing Practices Act and Good Marketing Practices.
- **Virtual Assistants (e.g. Alexa)**
  Depending on the purpose of the specific technology, a virtual assistant may be classified as a medical device and consequently greater compliance requirements will apply – for example, if the virtual assistant begins providing medical/diagnostic/therapeutic advice. Requirements regarding data privacy and health data protection will also apply.
  AI biases should also be considered.
- **Mobile Apps**
  As with wearables, virtual assistants, software, etc., the main legal and regulatory issues regarding mobile apps within healthcare concerns the legal classification of the app and whether the app falls within the definition of a medical device. In addition, requirements regarding data privacy and health data protection are key.
- **Software as a Medical Device**
  The use of software as a medical device gives rise to several legal issues in Denmark. Firstly, software used as a medical device is subject to Danish and EU medical device regulations including the MDR, as mentioned under question 2.1. As the use of software as a medical device often involves the processing of personal health data, compliance with requirements regarding data privacy and health data protection will also apply.
  Questions of product liability and medical malpractice may also arise in the event where the use of medical devices causes harm or errors. This might lead to issues regarding allocation of liability, insurance coverage and recourse, etc.
- **Clinical Decision Support Software**
  Based on the intended use and functionality of clinical decision support software, Danish and EU medical device regulations would most likely apply (see questions 2.6). The question of regulatory compliance is therefore key. Clinical decision support software stores and processes health data, which is why issues of data privacy and security arise. In addition, the question of liability is also introduced when it comes to the accuracy and reliability of the software's recommendations.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  Digital health solutions powered by AI/ML require processing large amounts of personal data and health data, making data privacy and security key. As with the above solutions, software that is powered by AI/ML may fall under the legal framework of Danish and EU medical device regulations, making regulatory compliance key.
  Using software based on AI/ML requires training of the AI models in order to learn patterns, etc. This might lead to bias in data training and lack of diversity, which might influence diagnostics, treatment recommendation, etc.
  In addition, the use of AI/ML-based software also raises liability questions and ethical considerations.
- **IoT (Internet of Things) and Connected Devices**
  The use of IoT and connected devices within the Danish healthcare sector has grown rapidly and is, for example, used for tracking patients with dementia. However, the use of IoT and connected devices requires reliable and secure telecommunications infrastructure, making health data protection, data privacy, network security, confidentiality, etc. all core issues.
- **3D Printing/Bioprinting**
  As with robotics, the use of 3D printing/bioprinting requires compliance with not only Danish and EU medical device regulations but also the Danish Product Liability

Act, making product safety a core issue. This also raises issued with regard to liability and compensation.
In addition, legal issues with regard to licences and intellectual property might also arise.

- **Digital Therapeutics**
  Digital therapeutics such as smart inhalers, cognitive behavioural apps, etc. may be subject to Danish and EU medical device regulations and the Danish Product Liability Act. Compliance with applicable law and regulations is key. The use of digital therapeutics may also give rise to questions about the qualifications, licensing and liability of healthcare professionals responsible for the recommended treatments, etc.
  As with the above solutions, data privacy and security are also key.
- **Digital Diagnostics**
  See above under Digital Therapeutics.
- **Electronic Medical Record Management Solutions**
  Electronic medical record management solutions involve the collection and processing of sensitive patient information and are dependable on reliable and secure telecommunications infrastructure. Health data protection, data privacy, network security, confidentiality, etc. are all core issues.
- **Big Data Analytics**
  A key component of big data analytics includes the collection, storage, management and processing of large volumes of diverse data from multiple sources. Ensuring compliance with data protection regulations is key.
- **Blockchain-based Healthcare Data Sharing Solutions**
  As with most data sharing solutions, blockchain-based healthcare data sharing solutions present challenges in terms of data privacy. Achieving compliance while maintaining the decentralised and transparent nature of blockchain technology can be complex.
- **Natural Language Processing**
  Natural language processing (NLP) is utilised in various sectors in Denmark and can be used to extract clinical information from Danish electronic health records. However, since only approximately six million people speak Danish, NLP solutions entirely based on the Danish language do not work optimally.
  As with digital health solutions powered by AI/ML, NLP requires processing large amounts of personal data and health data, making data privacy and security key. Additionally, dataset curation and training of NLP-models play an important role, making mitigation of biases key.

3.2 What are the key issues for digital platform providers?

Digital platform providers may be subject to the Digital Services Act (EU Regulation 2022/2065, "DSA"), which is an EU regulation that came into force in EU law on 16 November 2022 and will be directly applicable across the EU from 17 February 2024. The DSA applies to a wide range of online intermediaries, which include services such as internet service providers, cloud services, messaging, marketplaces or social networks and regulates the obligations of digital services that act as intermediaries in their role of connecting consumers with goods, services and content.

The scope of the DSA overlaps with the Platform to Business Regulation (EU Regulation 2019/1150, "P2B") already in force. The P2B regulates the commercial relationship between online intermediaries and the business users that offer goods and services via the intermediary platforms.

In addition to the above, digital platform providers are also subject to the requirements of the GDPR when handling health data.

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

The use of personal data is a fundamental part of the digitised Danish healthcare sector. The rise of digital health technologies has increased the need for collecting, processing and sharing personal data across the Danish healthcare sector.

Personal data is subject to the GDPR and the Danish Data Protection Act ("*Databeskyttelsesloven*"). The GDPR requires for personal data to be processed lawfully, fairly and in a transparent manner. Other principles such as: purpose limitation; data minimisation; accuracy; storage limitation; integrity; and confidentiality are also key.

According to the GDPR art. 9, health data is considered a special category of personal data and its collection and further processing is generally prohibited. However, art. 9(2)(h) of the GDPR allows health data to be processed where it is required for the purposes of preventative medicine, medical diagnosis, the provision of care or treatment, or the management of healthcare services. Art. 9(2)(i) of the GDPR further considers the necessity of processing health data for reasons of public interest in the area of public health. Hence, the use of personal data requires thorough investigation into the legal frame of data privacy and security and depending on the category of personal information used, comprehensive regulatory requirements may apply.

In addition to the requirements of the GDPR and the Danish Data Protection Act, the processing of health information is also regulated by the Danish Health Act ("*Sundhedsloven*"), which – under specific circumstances – allows healthcare professionals to collect and share relevant health information regarding patients currently undergoing treatment, without explicit consent.

4.2 How do such considerations change depending on the nature of the entities involved?

The GDPR applies both to European organisations that process the personal data of individuals in the EU, and to organisations outside the EU that target individuals living in the EU. Additionally, the GDPR applies regardless of the nature of the entities, whether public or private.

In order to lawfully process special category data, including health data, both a lawful basis and a separate condition for processing must be identified under GDPR art. 9 – e.g. explicit consent. However, according to art. 9 (2) (h) of the GDPR, processing health data is also permitted if processing is "necessary for the purposes of preventive or occupational medicine, […] medical diagnosis, [or] treatment". This exemption is typically relevant for the public healthcare sector and licensed healthcare professionals. However, this exemption does not necessarily apply to other authorities, e.g. private healthcare providers that would have to identify another legal basis to process health data.

4.3 Which key regulatory requirements apply?

The GDPR includes a comprehensive set of key regulatory requirements for processing personal data. Some of the key requirements are:

1. Full basis for processing: Personal data must be processed based on a valid lawful basis, such as consent, contract

performance, legal obligation, protection of vital interests, a public task or legitimate interests.

2. Data subject rights: Individuals have various rights, including the right to access their data, rectify inaccuracies, erase data, restrict processing, data portability, object to processing and not be subject to automated decision-making.
3. Data protection by design and default: Data controllers are required to implement data privacy features and data privacy enhancing technologies directly into the design of projects from the outset.
4. Data breach notification: In the event of a personal data breach, data controllers must notify the relevant supervisory authority within 72 hours, unless the breach is unlikely to result in a risk to individual's rights and freedoms. In certain cases, individuals must also be informed.
5. International data transfers: Transferring personal data outside the European Economic Area (EEA) is allowed only if the transfer is in compliance with the conditions laid down in Chapter V of the GDPR. Transfers may take place on the basis of an adequacy decision, or, if the controller or processor has provided "adequate safeguards". The European Commission publishes the list of its adequacy decisions on its website. In the absence of an adequacy decision, personal data may also be transferred when "adequate safeguards" are in place. A list of tools containing "adequate safeguards" can be found under art. 46 in the GDPR.

Other relevant regulatory requirements under the GDPR include:

- Keep a record: Entities must keep a register of the personal data that is processed by the entity and the purpose of the processing.
- Document compliance with the principles of good data processing: Entities must document that the entity adheres to the fundamental principles of data protection as outlined in the GDPR.
- Document implementation of appropriate technical and organisational measures: Entities must document that suitable technical and organisational measures in order to protect personal data have been implemented.
- Inform customers and employees about data processing: Entities are required to inform customers and employees about how their data is processed, including the purpose of the processing, rights, etc.
- Provide evidence of compliance with the regulations: The entity must be able to demonstrate that it complies with the GDPR.

4.4 Do the regulations define the scope of data use?

The strict requirements for processing data under the GDPR define the scope of data use. Hence, processing data is permitted under the GDPR when there is a legal basis for processing, such as the necessity for fulfilling a contract, compliance with a legal obligation, protection of vital interests, consent from the data subject, performance of a task carried out in the public interest or official authority, or legitimate interests pursued by the data controller or a third party. These legal bases provide the framework within which data processing activities can lawfully occur under the GDPR and automatically define the scope of data use.

4.5 What are the key contractual considerations?

GDPR regulations might require that an entity (controller) may only use data processors (processor) who can assure that they process personal data securely. This means that the processor must implement technical and organisational measures that are appropriate to the level of risk in the risk assessment of the processing. Under art. 28 of the GDPR, a written agreement (data processing agreement) is required. If two entities are jointly responsible for the processing of personal data, a joint controller agreement is required under art. 26 of the GDPR.

On 4 June 2021, the European Commission issued modernised standard contractual clauses under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR).

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

It is not possible under Danish law to secure comprehensive rights to personal or sensitive data that is used or collected. The GDPR's aim is to protect individuals' privacy and rights regarding their personal data, enhance individuals' control over their data, harmonise data protection laws in the EU, hold businesses accountable, etc.

Provided that an entity complies with the comprehensive regulatory requirements under the GDPR, processing of personal data is allowed. Please see questions 4.1 and 4.3 for more regarding the requirements. However, under the GDPR, individuals have certain rights regarding their personal data: the right to be informed; the right of access; the right to rectification; the right to erasure; the right to restriction of processing; the right to data portability; the right to object; etc.

Regardless of compliance with the GDPR requirements, the "ownership" or more accurately, the right to process personal data, is overshadowed by the data subject's rights under the GDPR.

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

As mentioned above, under the GDPR individuals have certain rights regarding their personal data, including the right to rectification and the right to erasure. There are currently no specific initiatives taken by the Danish regulatory authorities regarding data inaccuracy, bias and/or discrimination. However, the Danish Data Protection Agency ("*Datatilsynet*"), which is an independent supervisory authority, is responsible for ensuring compliance with data protection rules, including the GDPR. In addition, the Danish Data Protection Agency provides advice and guidance, processes complaints from individuals in relation to breaches of data protection rules and conducts inspections of authorities and companies related to breaches of data protection rules to ensure compliance with the rules.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

The use of generative AI is evolving rapidly and there are currently no concrete measures being taken under Danish law specifically with regard to generative AI companies and their use of data. However, as part of its digital strategy, the EU aims to establish regulations for AI in order to enhance the

development and utilisation of AI technology. In April 2021, the European Commission took a significant step by proposing the initial regulatory framework for AI within the EU. This framework involves the analysis and classification of AI systems used across various applications based on the level of risk they pose to users. Once these regulations are approved, generative AI would have to comply with transparency requirements.

However, the legal issues that the use of generative AI brings with it are highly debated and include:

- Data privacy and security: How are uploaded information being stored and used? What are the risks of data breaches or sharing confidential information?
- Copyright infringements or violations: Content created by generative AI is not copyrighted and most AI platforms do not take into account copyrighted inputs.
- Responsible and ethical use of AI: The use of AI might violate company policies.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Data protection regulations are becoming increasingly relevant as society becomes more digitalised. The scale of personal data collection and sharing has increased significantly.

As health data is sensitive personal data, the collection and processing of health data is regulated under national GDPR legislation and EU law. This means that public authorities are subject to certain rules that limit their right of disposal over the sensitive health data they collect from citizens. This is to protect citizens against misuse of the data, for example, when sharing it with third parties.

If the data is to be shared with third parties, e.g. in connection with a study, certain legal requirements under national and EU law apply. For example, there are certain requirements that the sensitive personal data must be anonymised, etc.

Please also see questions 4.1 and 4.3.

5.2 How do such considerations change depending on the nature of the entities involved?

All entities are subject to regulation under data protection laws, regardless of whether they are private parties or public authorities; however, the data protection regulation varies according to the specific circumstances, e.g. depending on the purpose of the sharing, who the recipient is, etc.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The sharing of personal health data is regulated under EU and national GDPR law. See the answers under questions 4.1 and 4.3.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

Denmark has various national health registries. What they have in common is that they all collect health information about citizens. The health registries collect information on, for example, surgeries, medical records, prescriptions, birth information, etc.

Health authorities have the ability to obtain and forward the health information in the registry to each other. However, this must be for a legitimate purpose and in accordance with the law. Citizens also have the ability to access their health information through the registries' websites or apps.

In addition, it must be stated that Denmark supports the European Health Data Space (EHDS), which the European Commission presented a draft regulation in 2022. At present, the EHDS is still under discussion, so the final design is still unknown.

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

The same issues apply as stated under question 5.1.

6 Intellectual Property

6.1 What is the scope of patent protection for digital health technologies?

Digital healthcare technologies enjoy the same level of patent protection as other industrial products. Patent protection in Denmark generally covers novel and non-obvious inventions related to hardware, software or a combination. This may include innovations in medical devices, data processing algorithms or communication protocols. The scope of the patent protection depends on the specific claims made in the patent application and how the innovation fulfils the fundamental criteria of novelty, inventive steps and industrial applicability.

6.2 What is the scope of copyright protection for digital health technologies?

Like in many other jurisdictions, copyright protection in Denmark primarily covers expression of a creative idea rather than the idea itself. In the context of health technologies this may include protection of the source code of software, graphic user interfaces and, for example, design elements. However, copyright does not typically protect ideas, algorithms or functional aspects. Copyright protection applies automatically upon creation; however, registration of the work can provide additional benefits.

6.3 What is the scope of trade secret protection for digital health technologies?

In Denmark, trade secrets are primarily protected under the Danish Marketing Practices Act, which implements the EU Trade Secrets Directive. The directive aims to harmonise the legal framework for trade secret protection across EU Member States, including Denmark.

Key aspects of the legal framework for trade secret protection in Denmark include:

1. Definition of Trade Secrets: The law provides a definition of trade secrets, emphasising information that is secret, has commercial value because it is secret, and has been subject to reasonable steps to keep it confidential.
2. Unlawful Acquisition, Use and Disclosure: The legal framework prohibits the unauthorised acquisition, use or disclosure of trade secrets. This includes actions such as industrial espionage, unauthorised access or breach of confidentiality agreements.

3. Remedies and Enforcement: The law provides for civil remedies, such as injunctions and damages, for the unlawful use or disclosure of trade secrets. Enforcement typically involves legal proceedings where the trade secret holder seeks protection and compensation.

For digital health technologies, trade secrets may include proprietary algorithms, manufacturing processes or confidential data analytics methods.

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

In 2000, the Danish Parliament adopted a piece of regulation making technology transfers a part of the assignment of Danish Universities. This regulation, called the Research Patent Act, defines technology transfer as the identification, assessment, protection and marketing of intellectual property with the purpose of commercial utilisation. The law applies to universities, as well as Danish hospitals. The fundamental elements of the law are:

- Employees at institutions are as an outset owners of innovations invented by themselves. For innovations invented as part of the employment, however, the institution can take over ownership rights in order to commercialise the innovation.
- The institution can make agreements with private undertakings about commercial exploitation of the innovations.
- A legal basis for the institutions to incur costs of taking out patents and create technology transfer units.
- How income from the innovations is split between the institutions and the employees.

With regard to software, this is regulated in the Danish copyright regulation. As a general rule, the employer automatically receives ownership to the rights.

Apart from the Research Patent Act, knowledge institutions engaging in public–private innovation partnerships must comply with a number of other regulations including the University Act, which stipulates freedom of research for researchers at Danish universities. On this basis, a private partner cannot require a researcher to perform specific research. Universities and other public knowledge institutions are also required to comply with the general rules of open government, access to information, etc. Such rules could potentially limit a private partner's desire to keep information confidential.

Universities and other public research institutions have a legal basis in the Danish Technology Transfer Act to establish limited liability companies under certain conditions and to obtain shares in limited liability companies established by other research institutions.

6.5 What is the scope of intellectual property protection for software as a medical device?

In Denmark, software is protected under copyright law. Copyright provides automatic protection as soon as the software is created, without the need for registration. Additionally, Denmark is a member of the EU, and software can also be protected through the EU Software Directive. Patents may apply to software in certain cases, but the criteria are strict.

Copyright law in Denmark, as in many other countries, provides protection to the creators of original works. For software, copyright protection relates to, for example, the source code, object code, and the overall structure and expression of the program. This means that the specific way in which the code is written and arranged is protected against unauthorised copying.

Copyright protection grants the software creator exclusive rights to reproduce, distribute, display and modify their work.

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

There is no specific case law in Denmark dealing with the question. However, a legal or a natural person is required in order to execute any rights under a patent. Under section 8 (4) of the Danish Patent Act, a patent application must include the name of the inventor. If a patent is applied for by someone other than the inventor, the application must include that the applicant has the rights to the invention. This wording ensures that the applicant has sufficient legal authority to claim rights to the invention. As an AI has no legal authority, it is unlikely that such an entity can be named as inventor.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

The core regulations of publicly funded innovations are laid down in the Danish Research Patent Act, which is described under question 6.4, which sets out the basis for how publicly funded research institutions can operate with regard to ownership to and income generation from innovations. Apart from the law, publicly funded innovations must consider how they comply with EU state aid rules and the principles of equal treatment. This applies to knowledge institutions as well as Danish government-funded innovation funds.

7 Commercial Agreements

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

Under section 22 of the Danish Procurement Act, Danish public institutions can enter into development collaboration contracts with private companies without a prior tender. This is solely designed to allow for collaborative research and development projects. The public institution can only buy the product after a public procurement process.

Sections 73–79 of the Procurement Act outline the requirements that apply to innovation partnerships. Such partnerships consist of three phases: 1) procurement; 2) innovation; and 3) purchase. Before the three phases can be initiated, the institution must conduct a market analysis in order to examine if applicable solutions already exist in the market place.

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

Apart from the regulatory elements described above, the parties should pay special attention to:

- The character and the extent of the collaboration.
- Changes in the collaboration.
- New contracting parties.
- Confidentiality.
- Termination.

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

In federated learning data sharing agreements, the parties should pay particular attention to the protection of sensitive client data and privacy issues. In healthcare, data used for federated learning will, with great certainty, be regarded as sensitive personal data under the GDPR. On this basis, the parties must consider how data can be protected. Such protection could consist of requirements for participating companies to anonymise data. Parties should calculate the sensitivity of the function that is used in the machine learning model in advance of entering into an agreement. The parties can further consider introducing a differential privacy mechanism, such as randomised response, or introducing noise in the system.

The agreeing parties should further consider how the ownership to the machine learning models developed through federated learning is shared among the participating companies and the rights and obligations of each participant, including each party's access to the use of developed models.

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

When dealing with generative AI in digital healthcare solutions, it is important to consider:

- Governability: It is important to ensure that while the AI system fulfils its intended purpose, humans must retain the ability to identify and prevent unintended consequences.
- Reliability: The generative AI models should have explicit and well-defined clinical use cases. A generative AI model designed for disease prediction must have a clear definition of the use situation and patient criteria. In addition, such generative AI models should be safe, secure and effective throughout their life cycles.
- Equality: The generative AI models, that potentially could have elevated data bias risks due to their pre-training on massive datasets, should not exacerbate this for certain marginalised, under-represented or low-education groups.
- Privacy: Privacy is necessary in most medical applications due to the confidential and sensitive nature of personal data. Generative AI systems in healthcare must be secure to prevent breaches and unauthorised use.
- Lawfulness: Developers must ensure AI software applications in healthcare respect various legal requirements, including health regulation, intellectual property rights, data privacy (GDPR) and cybersecurity.
- Liability: In case of non-compliance or wrongful diagnostics/medication, issues regarding potential liability can arise.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

AI and ML can be used to help doctors diagnose various diseases, such as different types of cancer, etc.

AI and ML need a lot of data to learn. It is difficult to collect all this data while complying with national legislation and EU GDPR law. Therefore, politicians must decide on strategies for developing and implementing AI solutions in healthcare while complying with current legislation.

8.2 How is training data licensed?

In connection with the revision of the guidelines for patenting, the European Patent Office might have opened up the possibility of obtaining a patent for ways to train an AI and ways to generate training datasets. However, this requires that the training method and the way of generating the datasets can be shown to provide a reliable and repeatable technical effect.

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

Under Danish law, it is only possible for individuals to obtain patent rights on their own inventions. This means that it is not possible for AI and ML algorithms to obtain patent rights. Presumably, it is possible for the creator of the AI or ML algorithm to obtain patent rights for the inventions of the AI or ML algorithm.

8.4 What commercial considerations apply to licensing data for use in machine learning?

As the data used in the training of ML often includes sensitive health information, the use of the data must be in accordance with national and EU GDPR law. This can limit the use of ML and AI, and the possibilities to get the outcome of the ML and AI licensed.

9 Liability

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

Civil liability:

- Product liability: With the rising popularity of digital health solutions in Denmark, product liability laws play a crucial role in safeguarding individuals from potential harm or damages caused by defective digital health products. Manufacturers, importers and distributors of digital health technologies are responsible for ensuring that these products are safe, reliable and meet applicable regulatory standards. In case of harm or damage caused by the use of a product, a consumer has the right to seek compensation under the Danish product liability regulations. However, digital heath solutions pose unique challenges in terms of liability due to related issues with regard to data privacy, cybersecurity and the accuracy of health information, etc.
- Contractual liability: Contractual liability becomes increasingly important between the various parties involved in the development, deployment and use of digital health solutions. Contractual relationships typically exist between technology vendors, software developers, data processors and healthcare providers. The contracts typically establish the terms and conditions between the parties and outline rights, obligations, potential liabilities, etc. Contractual liability becomes key in the event of harm or damage caused by a product arising from a breach of contract.

Criminal liability:

- Digital health solutions must comply with relevant EU and Danish regulations and laws. Breaches of regulations relating to medical devices, data privacy, cybersecurity, the Danish Health Act, etc. may result in administrative sanctions or prosecution.

9.2 What cross-border considerations are there?

Cross-border considerations regarding liability in the context of digital health solutions involve the legal implications and challenges that arise when digital health technologies and services are deployed or used across different jurisdictions. The key factors to consider are jurisdictional variations; different countries have different legal frameworks and regulations concerning: liability and digital health solutions; data protection and privacy; healthcare regulations and licensing; and dispute resolution mechanisms.

9.3 What are best practices to minimise liability risks posed by the use of generative AI in the provisioning of digital health solutions?

In Denmark, it is common for commercial contracts to include provisions regarding liability limitations. These provisions primarily aim to limit the risk of the contractual parties being held liable, including for damages. The principle of freedom of contract in Denmark allows parties extensive powers to shape liability limitations according to their preferences. This means that it is possible to include provisions that absolve the seller of a digital health technology from responsibility for the products or services provided. Parties can also agree that the seller is only liable for certain types of damages or that liability is limited to a maximum amount. However, please note that under Danish law, it is not possible to agree to limitations on liability for personal injury.

10 General

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

Cloud services offer several benefits, including accelerated IT development, enhanced scalability and a robust framework. The essence of cloud computing lies in the flexible sharing of resources, enabling users to pay only for the specific resources they utilise. Moreover, cloud services are typically operated at large scale, allowing for the implementation of comprehensive security solutions within the provider's data centres.

The key issues in cloud-based services for digital health are data security and compliance with the GDPR. The Danish Data Protection Agency ("*Datatilsynet*") has published a guide on cloud service usage and launched a working group to explore data protection best practices for cloud environments. The guidelines encompass suggestions for evaluations and prerequisites concerning data processors, alongside sections addressing the transfer of data to third countries via cloud services.

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

Before non-healthcare companies venture into the digital healthcare market, it is crucial for them to carefully consider a range of key issues. These include ensuring compliance with comprehensive relevant healthcare regulations and standards, establishing robust security measures and privacy protocols, addressing health data interoperability challenges and validating the efficiency and safety of their solutions through rigorous testing. By thoughtfully addressing these factors, non-healthcare companies can navigate the complexities of the digital healthcare market.

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

Some of the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures include: market size and potential; competitive landscape; regulatory compliance; scalability and sustainability; technology and infrastructure; and clinical validity and evidence.

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

Although Denmark's healthcare sector is recognised as one of the most digitised in the world, an even more widespread clinical adoption of digital health solutions is hindered due to challenges in digital infrastructure across sectors. These challenges include interoperability between different systems, lack of protocol standardisation, technical infrastructure, etc. Addressing these challenges requires ongoing investments and focus to improve the exchange of health data across sectors and deliver more coordinated care.

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 Danish clinician certification bodies that influence the clinical adoption of digital health solutions. The Danish Medicines Agency ("*Lægemiddelstyrelsen*") contributes to developing policies and regulations in the pharmaceutical area, both in Denmark and in dialogue with the EU's other regulatory authorities, including assisting the department of the Ministry of Health in pre-legislative work and ministerial services. However, the Danish Medicines Agency does not issue certifications.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

The general costs (reimbursement) of medical devices are provided by the Danish local municipalities. However, there is no specific reimbursement process for digital health solutions. If specific requirements are met, patients that are in need of medical devices, e.g. walking aids, special beds, wheelchairs, protheses, hearing aids, etc. can apply to local authorities for reimbursement.

10.7 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 digitalised healthcare services comprise a solid digital foundation on which to build, and although many digital solutions have been developed and implemented both nationally and locally in Danish regions and municipalities, ambitious digitalisation strategies have been set out in order to help address the health system's challenges in the years ahead. The ambition in the coming years is to integrate and streamline the way patient data are accessed and shared across the healthcare system, in order to make all relevant data accessible when needed and to accelerate the implementation of thoroughly tested solutions across the entire health service.

The focus is on expanding our digital healthcare system, so that citizens have better self-service tools available in order to provide a general picture of home-monitoring data, etc.

Heidi Bloch is partner in Kennedys' Copenhagen office and has worked in litigation since qualifying in 2004. Before joining Kennedys in 2019, Heidi spent three and a half years working in the Danish labour organisation FOA with its members' work-related injury cases in general and establishing an in-house legal office in that field. During her time at FOA, Heidi also participated widely in the law-making processes.
Heidi manages complex financial lines, cyber and transportation claims, as well as all manner of personal injury claims, including class actions.
Heidi is an exclusive contributor to *The Legal 500* Country Comparative Guides 2023 on Insurance & Reinsurance, International Arbitration, Class Actions and Product Liability and also contributed to *Chambers* Collective Redress Class Actions 2023 and Claims inflation and personal injury claims: a global review report, published in June 2023.
Further to this, Heidi contributed to the fourth edition of Kennedys' *Global Legal Handbook*, one of our most popular guides, which outlines the main legal and procedural issues that case handlers may encounter when dealing with claims across 53 jurisdictions globally.

Kennedys Copenhagen
Regnbuepladsen 5
4th Floor
Copenhagen V 1550
Denmark

Tel: +45 2331 8155
Email: heidi.bloch@kennedyslaw.com
LinkedIn: www.linkedin.com/in/heidi-bloch-4a78b544

Julia Tomaszewska is a senior associate in Kennedys' Copenhagen office. She qualified in Denmark in 2016.
Julia has represented insurers and local authorities in relation to professional indemnity claims, directors and officers claims, initial public offering claims, and all risk property claims including recourse claims. Julia has handled coverage issues for large international insurers and excess insurers in some of the most high-profile cases in Denmark.
Julia is also experienced within personal injury claims, life and health insurance, employers' liability, motor liability and product liability.
Julia is a member of the International Insurance Law Association and the Association for Compensation and Insurance.

Kennedys Copenhagen
Regnbuepladsen 5
4th Floor
Copenhagen V 1550
Denmark

Tel: +45 3373 7000
Email: julia.tomaszewska@kennedyslaw.com
LinkedIn: www.linkedin.com/in/julia-tomaszewska-05b4a53a

Janus Krarup is an associate at Kennedys' Copenhagen office. He graduated from the University of Copenhagen in 1993.
Since graduation, Janus has had an extensive career in the Danish public sector, including as Director in the Danish Business Authority and Director for Business Affairs in the Municipality of Copenhagen Agency. Janus has, in that background, achieved extensive knowledge into the Danish Public Sector.
Janus has been involved in a large range of legal issues including financial lines, cyber, consumer protection, coorporate law, employment law and data protection.

Kennedys Copenhagen
Regnbuepladsen 5
4th Floor
Copenhagen V 1550
Denmark

Tel: +45 3148 7017
Email: janus.krarup@kennedyslaw.com
LinkedIn: www.linkedin.com/in/janus-k-2763526

Kennedys in Copenhagen is a team of 11 legal professionals who provide specialist insurance law services to Danish, Scandinavian and international insurers.
The team's expert advice is based on a deep understanding of the Danish, Scandinavian and global insurance markets. Its primary focus is the insurance and reinsurance sector, including collective redress class actions within banking and finance, construction and engineering, directors' and officers' liability, employers' liability, cyber incidents and more, working closely with the Kennedys offices in EMEA, APAC, LATAM, the US and the UK.
The Kennedys Copenhagen office has represented insurers in several cases of material importance for the insurance sector in arbitration, the high courts and the Supreme Court. The Kennedys team in Copenhagen has panel lawyer appointments and co-operation agreements with several leading insurers in the Danish, Scandinavian and global markets, supporting its status as the go-to law firm within insurance.

www.kennedyslaw.com

Kennedys

France

Catherine Mateu

Pierre Camadini

Armengaud Guerlain

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 technologies 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 are the core legal issues in digital health for your jurisdiction?

Compliance with the General Data Protection Regulation (GDPR) and French Data Protection Act (DPA) standards, with intellectual property laws and with ethics (i.e. physicians and pharmacists) are key regulatory considerations. Health insurance reimbursement is also a key issue in France. Teleconsultations are reimbursed by the French health insurance system, provided they meet a number of conditions. In particular, teleconsultation must be part of the coordinated care pathway, with prior referral to the attending physician.

1.4 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. More 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.

1.5 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, Alan, Withings, Owkin and Qare.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

Whether in France or the European Union (EU), there is as yet no global regulatory framework for digital health. At present, the only transversal texts are non-binding texts that lay the foundations for future regulation. In 2022, France adopted a "doctrine for digital health", which explains the framework to be respected by all those who create, develop and maintain digital health products or services, in terms of basic rules (interoperability, ethics, security), basic identity services and basic exchange services.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

There are many different regulations that apply to digital health. To name only the most important, they include regulations on: data protection; medical devices (MDs); anti-kickback and transparency requirements; electronic medical records; and internet advertising. For example, any data that concerns health is considered sensitive data and the processing of such data is prohibited, unless it is necessary for reasons of public interest – developments in exactly what qualifies as a public interest reason is something all digital health organisations are obliged to follow very closely.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

French regulations are not yet clear on the distinction between consumer devices and MDs, which are subject to a specific

regime. At this stage, it should be assumed that consumer healthcare devices, insofar as they are not MDs or software, do not benefit from a special regime. Insofar as they are relevant, the above-mentioned regulations could be applied.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

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 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).

2.5 What are the key areas of enforcement when it comes to digital health?

One of the main areas of enforcement is the protection of health data: failure to comply with data protection standards (see question 2.2) can have serious consequences. For example, the CNIL has already fined companies several million euros for security breaches that led to the leakage of health data.

Another area of enforcement is related to liability for injuries that are suffered through the product-use that digital health services provide. This is done by the ANSM, whose power includes regulating the manufacturing of pharmaceuticals, and investigation or inspection. Setting up bodies to monitor life science products placed on the market ensures the safety and compensation of victims.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

If a software product falls within the European definition of a MD, it will be considered as such, and will have to comply with the applicable commercialisation and monitoring requirements. These requirements are laid down by: (i) the EU, Regulation (EU) 2017/745 on MDs (MDR) or Regulation (EU) 2017/746 on *in vitro* diagnostic MDs (directly enforceable in France and fully operative respectively since May 2021 and May 2022); and (ii) in France specifically, by the French Public Health Code. A particular feature of these European regulations is that their scope is extended to devices with no medical purpose (a list is drawn up). In addition, with regard to pre-market assessment, these regulations make cyber-security a new essential requirement.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

Neither France nor the EU has any legislation specifically governing AI and machine learning. Existing projects, notably the AI Act, specifically focus on the issue of data, which will be a central point for the regulation of AI in digital health. When applied to MDs, AI and software solutions will logically be subject to the texts applicable to MDs as described above.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  The notion of telemedicine includes a few things such as teleconsultation, tele-expertise and remote assistance. All these practices must be carried out with a minimum legal protection since patients provide their own information about themselves, via the platform, either their personal information, or their historical diseases and current health status. A doctor's practice should also be supervised by the law for the security of their practice. Platforms should ensure the protection of patients' information, and the ability of the doctors on the platform.
- **Robotics**
  Robotics call our attention to new technology products-related issues, such as product responsibility, in cases where misconduct of robots occurs, etc.
  From a practical point of view, the robots must be the object of legal regulation to ensure their ability, liability and practice ability.
  Managing robotics is a key subject. The question of financial compensation for a patient who is the victim of a wrong medical practice is a key issue that is not specifically addressed today.
- **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 individual's consent when the 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 which 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 (*Commission nationale de l'informatique et des libertés*) and ethical considerations are also mandatory.

3.2 What are the key issues for digital platform providers?

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 to consider for use of personal data?

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.

4.2 How do such considerations change depending on the nature of the entities involved?

The GDPR allows some derogations in certain situations. However, it applies regardless of the nature of the entities involved.

4.3 Which key regulatory requirements apply?

The GDPR applies. Apart from that, there are a few regulatory requirements such as the DPA (*Loi Informatique et Libertés*), other specific regulations or guidelines by the authority CNIL (*Commission Nationale de l'Informatique et des Libertés*) and the Telecoms and Electronic Communications Code.

4.4 Do the regulations define the scope of 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 What are the key contractual considerations?

The key considerations may regard: the consent of users for the ways to collect and use the personal data; to make sure that the use is strictly for the interest of users or the aim defined in the contract and no abusive of any data; the duration of use, its destruction after a certain period, and security measures to protect the data from leaking, and misuses of it; and the right for the individual to take legal action in case of breaching of contractual terms by the organism or platform.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Compliance with the applying regulatory requirements is essential.

Adequacy of contractual agreements is also very important as the negotiated contractual provisions must allow for an efficient use of data, a proper allocation of rights and liabilities and a prevention of sanctions.

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

Transparency requirements are used to address issues with data

inaccuracy, bias and/or discrimination. Indeed, according to the GDPR, data controllers must inform data subjects of the existence of automated decision-making. More precisely, they must communicate any meaningful information about the logic involved and its foreseeable consequences.

New prevented rules provided in the recently adopted AI Act also aim for the prevention of bias and discrimination in AI systems. These rules notably prohibit AI systems aiming to rank the trustworthiness of people based on their social behaviour or personal characteristics and may result in harmful treatment of people.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

Generative AI companies face unique data-usage legal and regulatory issues not only regarding data and intellectual property law, but also regarding civil and criminal law. As mentioned above, the recent AI Act directly addresses these issues. For example, the regulation provisions for a conformity assessment before the AI system is put into service or placed on the market.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Security is the main issue to consider when sharing personal data. It is indeed essential to ensure protection against unauthorised access, breaches, cyberattacks and cases of human negligence. More generally, compliance with data law is key, especially regarding the sharing of medical data. For instance, when dealing with information covered by medical secrecy, the respect of certain specific rules is crucial.

5.2 How do such considerations change depending on the nature of the entities 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

According to the GDPR, sharing personal data must always be subject to entering into an agreement and to adequate security measures during transmission. Regarding the sharing of data covered by medical secrecy, a specific regime requires patient consent to share its medical data with any party outside his healthcare team.

Additional requirements apply to personal data transfers to recipients located in non-EU countries, which do not ensure a sufficient level of protection: such transfers must be covered by appropriate safeguards. For this reason, they must conduct a risk assessment, use standard contractual clauses in data transfer agreements and guarantee the protection of personal data from access by foreign authorities.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

At the European level, the European Health Data Space (EHDS) was created in 2022. This health-specific ecosystem is composed of rules, common standards and practices, infrastructures and a governance framework. It provides a trustworthy and efficient set-up for using and sharing health data.

At the French level, the Health Data Hub was created in 2019 to facilitate the sharing of healthcare data. One of the main goals of this new platform is to promote standard norms for the use and exchange of health data.

5.5 What are the key issues 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 What is 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). For example, a cardiac monitor controlled by a neural network specially adapted to limit cases of false alarms has been considered patentable.

6.2 What is 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 multi-media 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 What is 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 What is 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 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 which does not have legal capacity. It can only be a human being with legal capacity, as a machine cannot defend and/or transfer any rights.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

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.

7 Commercial Agreements

7.1 What 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 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 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 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 is the role of machine learning in digital health?

Machine learning is key to advancing care for patients. Healthcare Providers (HCPs) can collect and manage patient data, identify statistics and trends and recommend treatments thanks to machine learning. Machine learning can also help medical practitioners improve decision-making and reduce risk.

8.2 How is training data licensed?

Intellectual property rights protect training data as an entire database if it is an original production. If it is not, it can still be protected if the owner demonstrates personal investment in obtaining and managing the data. Therefore, training data can be licensed as long as it meets certain normative requirements. Open databases can, however, be used without the need for a licence.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning 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 considerations apply to licensing data for use in machine learning?

Because of the growing importance of data governance, data integrity and transparency are key commercial considerations. Addressing these issues will allow companies to use recent reliable data in connection with their commercial objectives. It will also enable them to protect their clients' data and gain trust. A good use of data governance is therefore important for optimisation and improvement of business results.

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 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.

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 todays' 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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

These patients can be reimbursed by the government or private insurers under certain conditions. A recent law even provides for an early reimbursement for some therapeutic and telemonitoring digital MDs. Generally, MDs must be CE-marked, approved by the HAS and registered on a governmental list and prescribed by an HCP to be reimbursed.

10.7 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


Dr. Deniz Tschammler


Dr. Claus Färber


Steffen Woitz

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 technologies in your jurisdiction?

Prescription and reimbursement of medical apps: A new system for the reimbursement of medical smartphone apps (*Digitale Gesundheitsanwendungen* – "DiGA") has been introduced under the statutory health insurance ("SHI") regime in 2021. The DiGA concept applies to apps that are CE-certified medical devices under the Regulation (EU) 2017/745 on medical devices ("MDR") risk class I or IIa. 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. These positive effects in patient care have to be established with a comparative study which demonstrates the advantages of using the app, as opposed to not using it. Such study must generally be retrospective. It does not have to be a genuine clinical trial. Valid concepts are epidemiological studies, or studies using methods from other scientific fields such as healthcare research.

At present, BfArM has approved 55 medical apps. Twenty-two of these medical apps have obtained temporary approval subject to further proof of positive healthcare effects. Over the past years, the number of reimbursed medical apps has not increased as quickly as the industry had hoped.

At the current stage, the German Federal Government (*Bundesregierung*) has passed the Digital Act, which aims to amend pricing and regulatory requirements for DiGA. The law is expected to come into force at the beginning of 2024.

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. The practical implementation of these laws has been accelerated significantly due to the pandemic and related restrictions on public life. The number of video consultations, online prescriptions and other types of remote patient treatment have meanwhile reached an all-time high. Physicians are now also permitted to issue a certificate for sick leave in a video consultation. Simultaneously, restrictions on the advertisement of telemedicine have, to some extent, been lifted.

Regardless of the above, 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 implementation shall be completed in 2025. The ePA is a central element of digital and networked healthcare. Since 2021, patients insured with SHI are entitled to be provided with the benefits of ePA upon request, and all physicians and psychotherapists must have the necessary equipment to transfer data to the ePA. The aim of the ePA is to centrally store patient data in one virtual place if the patient consents and to the extent

covered by the patient's consent. Patient data include, *inter alia,* treatment data and vaccination records. Since 2023, the ePA also includes medication records and data collected through DiGA. Based on the digitisation strategy of the German Federal Government, an ePA shall be set up for every insured person in Germany who does not actively refuse their consent (opt-out principle). Furthermore, patient data stored in the ePA shall be made available for research and development purposes in certain circumstances.

1.3 What are the core legal issues in digital health for your jurisdiction?

Digital health trends are a major challenge for the German health sector, which is still characterised by many traditional rules and practices. The objective of the German Federal Government is to provide a functioning and secure healthcare telematics infrastructure that sets a digital framework and facilitates cooperation between various players in the domestic health markets. The telematics infrastructure seeks to achieve a balance between protecting the patients' fundamental rights of autonomy and confidentiality of their health data on the one hand, and creating digital health services and a high level of work efficiency across the health sector on the other hand. One of the key issues of digital health is the handling of sensitive patient data, the extensive use of which has considerable value for research and development, but is at the same time limited by a number of local, national and EU regulations, including Regulation (EU) 2016/679 (General Data Protection Regulation – "GDPR").

1.4 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.

1.5 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.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

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* – "MPDG").

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").

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

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 products 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.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

While there is no specific national scheme for "consumer healthcare devices", such products are subject to the laws and regulations described above. Under EU law, consumer products are generally subject to the General Product Safety Directive (EC) 2001/95 ("GPSD"). The GPSD will be replaced by the General Product Safety Regulation (EU) 2023/988 ("GPSR") from 13 December 2024. In the digital health sector, however, the GPSD and GPSR are of minor relevance because the more specific medical device regulations, including the MDR, would typically apply instead.

With the implementation of the Directive (EU) 2019/770 on digital content in the German Civil Code (*Bürgerliches Gesetzbuch* – "BGB"), the German legislator has reinforced consumer protection in this area. Where digital apps are marketed to consumers, manufacturer obligations under these provisions may even go beyond the general regulatory obligations under the MDR.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

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.

2.5 What are the key areas of enforcement when it comes to digital health?

Compliance of medical device software ("MDSW") with the sector-specific laws and regulations is mainly supervised by regional market surveillance authorities and notified bodies. This includes regular and *ad hoc* audits. Legal violations by the manufacturer of MDSW may lead to reputational damage and qualify as an administrative or criminal offence. Depending on the circumstances of the individual case, they may result in fines, orders of corrective and preventive measures, or a market ban.

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.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

Software with a medical purpose is often regulated as a medical device 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 ("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 ("MDCG") of the European Commission issued several guidelines on qualification and classification of MDSW.

2.7 What regulations apply to Artificial Intelligence/ Machine Learning powered digital health devices or software solutions and their approval for clinical use?

Germany has not enacted a specific law on AI so far. Products that include AI 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 software must comply with the requirements of the MDR or IVDR.

The EU Commission published a draft regulation on AI on 21 April 2021. The regulation is expected to come into force no earlier than 2024. As things currently stand, the draft regulation shall not supersede to the EU medical devices regime but apply in parallel. AI systems shall be subject to regulatory requirements that increase with the level of risk associated with them. High-risk AI, including certain AI systems for medical technology, shall be subject to comprehensive legal obligations imposed on the respective operator.

3 Digital Health Technologies

3.1 What are the core legal or 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 machine learning can be a powerful tool for medical diagnostics and monitoring.
  The training of neural networks and similar AI/machine learning 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 issues for digital platform providers?

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 to consider for use of personal data?

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* – "StGB").

For connected medical devices and other equipment, the Telecommunication-Telemedia Data Protection Act (*Telekommunikation-Telemedien-Datenschutzgesetz* – "TTDSG"), which transposes certain parts of Directive (EC) 2002/58, imposes additional restrictions on remote access to data, even if it is not personal data.

The upcoming EU Data Act (Proposal for a Regulation on harmonised rules on fair access to and use of data, procedure file 2022/0047(COD)) would also cover digital health products and services, and require the vendors to make available both personal data and non-personal data to the user and third parties requested by the user.

4.2 How do such considerations change depending on the nature of the entities 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.

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.

4.3 Which key regulatory requirements apply?

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 which 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 health providers 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.

4.4 Do the regulations define the scope of 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 the Regulation (EU) 2022/2065 (Digital Services Act), from 17 February 2024, digital platforms – whether health-related or not – will no longer be permitted to target advertisements based on profiling of health data or other special categories of data (Article 26(3)).

4.5 What are the key contractual considerations?

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 proposed EU Data Act, providers would also be required to inform the users about the non-personal data generated by a product or service before entering into a contract.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

German law does not generally provide for ownership in data as intellectual property or otherwise. Data can only be protected as part of a database under the *sui generis* database protection rights set out in Sections 87a *et seq.* of the German Copyright Act (*Urheberrechtsgesetz* – "UrhG"), which transposes Directive (EC) 96/9. This protection, however, only comes into play if there was a substantial investment specifically in the acquisition, verification or presentation of the contents of such database. Efforts undertaken to collect data for other commercial purposes, such as providing healthcare services or developing medical software, are not specific to the creation of the database and will thus not be considered. In addition, the proposed EU Data Act would clarify that databases containing data obtained from or generated by the users would not be eligible for protection. Such measures could also apply when data is shared in accordance with the proposed EU Data Act.

Failing a protection as a database, data can only be partially protected as a trade secret under the German Trade Secret Act (*Geschäftsgeheimnisgesetz* – "GeschGehG"), which transposes Directive (EU) 2016/943. For this protection to apply, adequate measures against unauthorised access must be taken.

Often, the ownership of the data is overshadowed by the rights of the patient or other data subjects under the GDPR. If the collection or processing of personal data is based on consent (as opposed to, e.g., the research exemption), this consent can be revoked at any time, and the data subsequently needs to be deleted. This usually means that data ownership is not the primary concern, provided that data is not aggregated or otherwise anonymised.

4.7 How are issues with 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.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

Generative AI is usually discussed in connection with copyright issues. Section 44b of the UrhG explicitly allows the use of digital or digitised work for data mining purposes. The copyright holder may, however, reserve these rights – for works that are online, this must be in a machine-readable format. "Works" created by generative AI are generally not eligible for copyright because they have no human author.

Generative AI also raises data protection issues, in particular regarding the use of personal data for training purposes. There are no special provisions for AI training in the GDPR or the BDSG. In many cases, the use of personal data for AI training may be permitted under the "legitimate interest" basis (Article 6(1)(f) GDPR). However, this will exclude the use of special categories of personal data, including health data.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

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 allows the transfer or 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 do such considerations change depending on the nature of the entities 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.

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) may be subject to additional restrictions from state data protection laws and governmental policies when sharing health data.

5.3 Which key regulatory requirements apply when it comes to sharing data?

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.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

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 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 What is 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 increased substantially to over 130,000 per year; the health sector is contributing significantly to this development.

6.2 What is 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 What is 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 GeschGehG – implement a confidentiality program 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 What is 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 seen as an intellectual achievement of a human and product of their personality, which an AI is not capable of.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

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 98"), e.g., require that the results be made available to research and teaching in Germany 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.

7 Commercial Agreements

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

Collaborations in the digital health sector are mostly subject to extensive contractual agreements that aim at a fair balance of IP rights allocation and commercialisation rights on the one hand, and regulatory responsibilities and product liability on the other hand.

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

When cooperating with healthcare companies or HCPs, non-healthcare companies should avoid granting any benefits, both unilaterally (e.g., gifts) and as part of (bilateral or multilateral) cooperation agreements. In such agreements, therefore, services and consideration must be equivalent, i.e. any remuneration must be at arm's length (principle of equivalence).

When granting benefits, companies should avoid the impression that there are any commercial expectations associated with such benefits. In particular, benefits must not create an incentive for the healthcare company or HCP to make a certain procurement or therapy decision. In other words, if companies grant any benefits, this should be for legitimate objective reasons and kept separate from other businesses or commercial interests (principle of separation).

In the event of a cooperation with healthcare companies or HCPs, any details of such cooperation should be agreed upon in written form and as transparently as possible. In particular,

companies should avoid any (additional) verbal agreements or other non-transparent arrangements as these give the impression of secrecy (principles of transparency and documentation).

7.3 What 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 consider data protection requirements, as feeding an algorithm with personal data is a process that requires a legal basis under the GDPR. In the case of healthcare or patient data, parties typically must obtain explicit consent for data processing activities. They must also determine if the results of the training of the algorithm still include personal data to some extent or whether they can be treated as anonymised and thus be shared freely.

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

Dealing with the use of generative AI will soon be governed by an EU regulation (the AI Act), which is not yet in force (see above question 2.7). According to the proposed AI Act, the rules will also apply to providers and users of AI systems established in a third country outside the EU, to the extent the output produced by those AI systems is used in the EU. Against this background, the proposed AI Act will also have an impact on contractual relationships of European operators with AI operators in third countries.

However, the AI Act is not yet in force, nor has Germany enacted a specific law or regulation on AI so far. Nevertheless, parties must consider general civil law in commercial agreements. In any case, it should be important to name the characteristics of the AI services provided and describe how the AI should work. In case of the provision of AI software, an agreement is likely to qualify as a software transfer/licence agreement.

In addition, due to the lack of clear case law on the ownership of AI-generated results, the parties should spell out in their contract who the owner will be.

Finally, parties should thoroughly examine data protection aspects when using generative AI in the provision of digital health solutions.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning usually refers to the use of an algorithm ("neural network") that is trained with representative input data (e.g., images or sensor information) and the desired output. The algorithm is thus trained to recognise patterns in input data and to produce a certain output.

Machine learning can be a powerful tool for diagnostic purposes to assist HCPs and to monitor the success of patient treatment. It can also be used for the early detection of potential health issues, even in consumer devices such as smartwatches or smartphones.

8.2 How is training data licensed?

Training data is often protected under the *sui generis* database protection rights set out in Sections 87a *et seq.* of the UrhG, which transposes Directive (EC) 96/9 on the legal protection of databases. In this case, it can be licensed in the same manner as other intellectual property.

Licensing training data will often be challenging, as it includes personal health data, which is under strict protection under the GDPR regime. Consequently, training data can often be licensed in anonymised form only. One of the main considerations is how to ensure that it will not be possible to re-identify individuals.

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

As a general rule, intellectual property can only be produced and owned by human beings, not by machines. For this reason, improvements made without active human involvement do not fall under the protection of most intellectual property rights.

In some cases, the results may be protected by *sui generis* database protection rights (see question 8.2 above). Unlike other types of intellectual property, this protection only requires a substantial investment, but not necessarily an intellectual achievement.

Furthermore, the improvements might be protected as trade secrets of the entity that made them.

8.4 What commercial considerations apply to licensing data for use in machine learning?

The main consideration is the ownership and/or access to the results of the training, i.e. the trained algorithm. As the algorithm may often not be protected by intellectual property rights (see question 8.3), it is crucial to clearly define the rights and obligations of each party with respect to its further use in the commercial agreement.

As training data will often include personal health information, it is also important to agree on liability and indemnification provisions in case the use of the licensed data turns out to be a violation of the GDPR. This could, e.g., be the case if the consent given by the patients is invalid or if the data has not been properly anonymised.

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 (not in force yet), the EU Directive on AI liability (not in force yet), the new GPSR (applying from 13 December 2024) and the new EU Directive on liability for defective products (not in force yet) will become relevant soon, 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 predominantly subject to Member State law. With regard to cross-border matters, the Regulation (EU) 593/2008 ("Rome I Regulation") and the Regulation (EU) 864/2007 ("Rome II Regulation") regulate the applicable national legislation. Under Article 4 of the Rome II Regulation, applicable law is determined on the basis of where the damage has occurred, irrespective of the country in which the act that has caused the damage took place. There are two general exemptions from this rule: (i) if the parties reside in the same country, the law of that country shall apply; or (ii) if a tort is apparently more closely connected to a country other than where the damage occurred or where both parties live – in that case, the law of that other country is applicable. Furthermore, exemptions apply with regard to certain types of liability. For product liability, specific rules apply according to Article 5 of the Rome II Regulation. Here, the place where the product was acquired can become decisive. Under the Rome I Regulation, parties are, under certain conditions, allowed to determine the applicable law by contract. In the absence of a contractual choice of law, with regard to services, the law of the service provider's residence is applicable. However, there are exemptions to this rule with regard to consumer contracts, where generally the law of the consumer's country of residence is applicable.

Given that cross-border liability cases can result in severe legal consequences and significant loss of reputation in all countries concerned, cross-border digital health companies should adopt a global compliance regime and establish an organisation that takes into account the specific legal requirements and pitfalls of each national legal system concerned.

9.3 What are best practices to minimise liability risks posed by the use of 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 IP; 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.

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 high-market entry, reimbursement and compliance requirements. The market entry of MDSW is largely restricted by certification procedures under the new MDR and IVDR regimes that often require the involvement of notified bodies. However, as the new regulations maintain the general certification system and do not introduce a genuine approval requirement for MDSW (unlike for drugs), they are still regarded as an efficient market-clearance system. 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?

The German Physicians' Chamber (*Bundesärztekammer*) supervises all physicians practising in Germany. 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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with 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 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 use of electronic prescription shall become mandatory for physicians and patients as of January 2024, and the ePA shall be made available to all patients by 2025. Both acts are expected to come into force in the beginning of 2024.

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 recently established in mid-2023, in order to facilitate availability of social insurance data and electronic prescriptions to physicians in other EU countries.

Acknowledgment

The authors would like to thank Dr. Katharina Hoffmeister for her contribution to the preparation of this chapter. Katharina focuses her practice on healthcare and life sciences with a focus on the pharmaceutical industry and industry-specific data protection and compliance issues in the healthcare market.

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

Dr. Deniz Tschammler, Partner, based in Frankfurt, counsels pharmaceutical companies, manufacturers of medical devices and *in vitro* diagnostics, providers of healthcare platforms as well as their investors in complex sector-specific projects. He advises his clients on the various regulatory challenges of the German and European health market, transactions and strategic collaborations, disputes in competition and with authorities, market entry and reimbursement pathways, data protection and the establishment of compliance organisations.

McDermott Will & Emery Rechtsanwälte
Steuerberater LLP
Oberlindau 54-56
60323 Frankfurt/Main
Germany

Tel: +49 69 951145 029
Email: dtschammler@mwe.com
LinkedIn: www.linkedin.com/in/dr-deniz-tschammler-4b02605a

Dr. Claus Färber, Counsel, based in Munich, represents clients on 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
LinkedIn: www.linkedin.com/in/cfaerber

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

McDermott Will & Emery is an international full-service law firm with a particular focus on Health and Life Sciences. We advise our clients on legal and regulatory challenges in an increasingly growing digital health market and provide tailor-made solutions for the successful market entry of new digital health products and services. With 23 locations on three continents, our team works seamlessly across practices, industries and geographies to deliver highly effective and extraordinary legal and strategic advice. More than 1,200 lawyers strong, we bring our personal passion and legal prowess to bear in every matter for our clients and the people they serve. Looking to the future, we will continue to expand geographically and enhance our existing practices and industry-focused strengths. We are committed to building from these strengths in order to best serve our clients and our communities.

www.mwe.com

Greece


Nefelie Charalabopoulou


Natalia Kapsi


Yolanda Antoniou-Rapti


Celia Karvouni

Zepos & Yannopoulos

1 Digital Health

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

Greek Law does not define "digital health" (nor "e-Health", which is also commonly used), yet the term is understood to encompass: (i) digital healthcare services, including telemedicine; (ii) software used as a medical device; (iii) medical devices used as diagnostic and/or monitoring tools; and (iv) other medical products that involve digital features. While digital health is not a defined legislative term, there is a single legislative reference to telemedicine to be found in Article 66 par. 16 of Law 3984/2011. Also, the Greek Ministry of Health (MoH) website refers to the definitions used by the World Health Organization: "[...] the efficient and safe use of information and communication technologies (ICTs) in support of health and health-related fields, including healthcare, monitoring and treatment, research and knowledge" and the European Commission "[...] tools and services that use ICTs to improve prevention, diagnosis, treatment, monitoring and management of health-related issues and to monitor and manage lifestyle-habits that impact health".

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

Key emerging technologies in digital health in Greece include various tools and platforms used by stakeholders that enable the monitoring, recording and health management, as well as digital tools for the remote provision of healthcare services, decision making, storing and sharing of data, managing clinical workflows, diagnostics and patient management and support. Examples include:

- Telemedicine.
- Wearable devices and biosensors.
- Mobile apps.
- Software as a medical device.
- AI digital health tools.
- Digital diagnostics.
- Health information exchange.
- e-Health records.
- Real-World Data and Real-World Evidence analytics.

1.3 What are the core legal issues in digital health for your jurisdiction?

The core legal issues in digital health in Greece are the applicability of and compliance with the regulatory framework, the categorisation of a digital tool or software as a medical device, liability issues regarding the interpretation of the data generated through the digital tools, and issues regarding data privacy and security and liability in general.

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

According to the Statista Market Forecast, Greece's revenue in the digital health market is projected to reach US$318.80 million in 2023. Revenue is expected to show an annual growth rate (CAGR 2023–2027) of 9.28%, resulting in a projected market volume of US$454.70 million by 2027.

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

Although no such data could be ascertained for Greece, there is an active innovation ecosystem in the field of digital health tools in Greece, with significant growth in recent years. Today, in "Elevate Greece" (which is the official platform and leading resource for in-depth information on the Greek Startup Ecosystem), there are 113 registered startups active in the field of life sciences (healthtech, medtech, biotech), constituting the most numerous category with 14.7%. More than half of them develop digital health applications and tools, mainly for disease management, telemedicine and wellness.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

Some healthcare regulatory schemes related to digital health are the following:

1. Greek Law 4931/2022 "Doctor for All, Equal and Quality Access to the Services of the National Services Health Organization (EOPYY) and Primary Health Care and other emergency provisions"; in particular Article 28.
2. Greek Law 4961/2022 on emerging information and communication technologies, which has introduced rules and obligations about digital governance.
3. Greek Law 4715/2020 "Arrangements to ensure access to quality health services establishment and statute of the Organization for Quality Assurance in Health S.A. (ODIPY S.A.), other urgent provisions under the competence of the Ministry of Health and other provisions", namely Article 23.

4. Greek Law 4633/2019; in particular Article 33.
5. Greek Law 4213/2013 transposing Directive 2011/24/EU on the application of patients' rights in cross-border healthcare and other provisions, specifically Article 6.
6. Greek Law 3984/2011; in particular Article 66 par. 16 on Telemedicine.
7. As EU regulations, the MDR (Regulation 2017/745 on medical devices) and IVDR (Regulation 2017/746 on *in vitro* diagnostics) are directly applicable in Greece and do not have to be transposed into national law.
8. A number of legislative initiatives concerning the EU's digital strategy, such as the Digital Services Act (EU Regulation 2022/2065) and the EU proposal for an AI Act.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

1. Law 4624/2019 "Protection of Personal Data and Measures for the Implementation of the GDPR", which enacts supplemental measures for the application of EU Regulation no. 2016/679 (GDPR).
2. Law 3471/2006 "Protection of Personal Data and Privacy in the Field of Electronic Communications".
3. Greek Law 1733/1987 on "Technology transfer, inventions and technological innovation" (Greek Patent Law).
4. Greek Law 1607/1986 on the "Ratification of the European Patent Convention".

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

As regards the consumer's protection, Law 2251/1994, which transposed into Greek law the Product Liability Directive 85/374/EC and Law 4933/2022, which transposed into Greek law Directive 2019/2161/EU (the omnibus directive of the "New Deal for Consumers" package) apply. On top of that, general provisions of the Greek Civil Code (Article 914 *et seq.* establishing tortious liability) are applicable in case they afford consumers more effective protection.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

According to Article 23 of Greek Law 4715/2020, as amended, the MoH is designated as the National Authority responsible for electronic health issues and in cooperation with the other involved agencies has the overall responsibility of coordinating the actions for the implementation of the national strategy for digital health. An important specialised agency is the MoH's National Council for eHealth Governance. Moreover, the Hellenic Data Protection Authority is concerned with ensuring the application of the GDPR regarding personal data protection. Last but not least, the Ministry of Digital Governance and its General Secretariat of Cybersecurity provide regulatory services for the security of informatic systems.

2.5 What are the key areas of enforcement when it comes to digital health?

Privacy, data security and product liability of medical devices (including software) are important key areas of enforcement when it comes to digital health.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

The MDR and the IVDR apply to Greece. As EU regulations, they apply automatically to Greece as soon as they entered into force, without needing to be transposed into national law.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

Greek Law 4961/2022 on emerging information and communication technologies contains provisions about AI, Internet of Things, etc. It is worth noting that the European Commission tabled a proposal for an EU regulatory framework on AI in April 2021.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care:** Health data protection, liability and security issues are emerging.
- **Robotics:** Liability allocation and regime of product responsibility are key.
- **Wearables:** The collection of daily precise health data raises the issue of data protection.
- **Virtual Assistants (e.g. Alexa):** Their training and their function relates with AI issues and data protection compliance.
- **Mobile Apps:** Security and data protection in particular in the use of apps that collect health data are really important.
- **Software as a Medical Device:** Medical Device regulations (MDR/IVDR), data protection and security are key.
- **Clinical Decision Support Software:** Liability allocation, Medical Device regulation (MDR/IVDR) and data protection are key.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions:** Where the technology is provided to a public institution, providers have the obligation to disclose details that allow the public institution to study how the system works and the parameters which, in view of the intended purpose, are taken into account for taking or supporting decisions or adopting acts, to improve the system and to publish or make available in any way such improvements. Also, any public body using an AI system is required to carry out an algorithmic impact assessment before the system becomes operational.
- **IoT (Internet of Things) and Connected Devices:** Manufacturers, importers and distributors of such devices will have particular obligations, including from a data protection standpoint, once the relevant provisions of Greek Law 4961/2022 come into force, which is expected to happen in March 2024. Medical Device regulations may also apply depending on the features.
- **3D Printing/Bioprinting:** The use of the technology of 3D printing raises intellectual property and consumer protection issues and the Intellectual Property Law 2121/1193 and Law 2251/1994 on Consumer Protection shall apply. There is no specific regulatory framework on bioprinting; nevertheless, data protection and security regulations are likely to apply as well as the MDR/IVDR depending on the purpose of use.

- **Digital Therapeutics:** Liability allocation and data protection are emerging issues.
- **Digital Diagnostics:** The development and use of digital diagnostics technology may raise industrial property and data protection issues.
- **Electronic Medical Record Management Solutions:** The use of electronic management solutions for medical record keeping may raise data protection issues.
- **Big Data Analytics:** Big data analytics raise data protection issues.
- **Blockchain-based Healthcare Data Sharing Solutions:** The use of blockchain technology in the context of healthcare data solutions may raise issues concerning data protection and data security.
- **Natural Language Processing:** Proper and secure use of AI and data protection are important issues.

3.2 What are the key issues for digital platform providers?

Digital platform markets are rapidly maturing, raising issues about regulatory constraints, compliance with security standards, effective supervision and consumer protection.

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

The use of personal data constitutes processing of personal data and therefore, compliance with the provisions of the GDPR and Law 4624/2019 should be complied with. The key issues to consider are ensuring compliance with the processing principles of the GDPR, processing personal data under an appropriate legal basis, ensuring that the data subjects are being informed about the processing of their personal data, implementing appropriate technical and organisational measures for the protection of personal data, maintaining records of processing activities and, if applicable, appoint a data protection officer (DPO). Also, health data are considered special categories of personal data as defined under Article 9 of the GDPR.

4.2 How do such considerations change depending on the nature of the entities involved?

The data protection legislation applies regardless of the nature of the entities involved. Law 4624/2019 includes different provisions for controllers who are public and controllers who are private entities, for instance, when it comes to processing personal data for reasons different that the ones they were collected for, and in relation to processing activities on special categories of personal data.

4.3 Which key regulatory requirements apply?

1. As follows:
   a. Entities processing personal data shall be able to demonstrate compliance with the following processing principles: lawfulness; fairness; and transparency. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
   b. Purpose limitation principle: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
   c. Data minimisation principle: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
   d. Accuracy principle: Personal data shall be accurate and, where necessary, kept up to date. Reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without undue delay.
   e. Storage limitation principle: Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
   f. Principle of integrity and confidentiality: Personal data shall be processed in a manner that ensures the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisation measures.
2. The processing of personal data must be based on an appropriate legal basis. Different legal bases are provided for special categories of personal data, who are afforded greater protection, as opposed to non-special categories of personal data.
3. Data subjects must be informed about the processing of their personal data, including details about the controller's identity and contact details, the purposes of the processing and the legal basis, the recipients of their personal data, whether their personal data are being transferred outside the EU/EEA and under which safeguards, the retention period and their data protection rights. Where the personal data are not being collected directly from the data subject, the information provided should also include the source they originate from and the categories of personal data.
4. Controllers should respond to, and without prejudice to limitations provided by applicable legislation satisfy requests made by data subjects exercising their rights of access, rectification, restriction of processing, data portability, objection and the right not to be subject to automated decision making.
5. The roles of the parties involved in the personal data processing activities must be determined, i.e., controllers, processors and joint controllers. In a controller-to-processor relationship, an appropriate agreement in writing must be put in place in accordance with Article 28 of the GDPR. In case where two or more parties jointly determine the means and purposes of the processing activity, an agreement must be put in place pursuant to Article 26 of the GDPR.
6. The core processing activities must be evaluated in relation to determining whether there is an obligation to appoint a DPO. In case a DPO is appointed, either because it is required or as a best practice, said appointment must be announced to the data protection authority. The Hellenic Data Protection Authority expects that the DPO should be able to communicate using the Greek language; therefore, in case a DPO is appointed at Group level and does not speak Greek, a Greek-speaking local contact point should be also appointed and announced to the authority.
7. Processing activities, in particular those that involve the use of new technologies, that are likely to result in a high risk to the rights and freedoms of natural persons, require the carrying out of a Data Protection Impact Assessment (DPIA). Large-scale processing activities

on health data is an example that requires a DPIA and is specifically mentioned by the GDPR. The Hellenic Data Protection Authority has also issued a decision setting out an indicative list of processing activities that are subject to the requirement for a DPIA.

8. Appropriate technical and organisational measures should be put in place to ensure a level of security to the personal data that is appropriate to the relevant risk.
9. Controllers should ensure that appropriate arrangements are in place in order to be able to identify and assess personal data breach incidents and, where required, notify the Hellenic Data Protection Authority and communicate the breach to the affected data subjects.
10. In case personal data are transferred outside the EU/EEA, compliance with Chapter V of the GDPR should be ensured (e.g. standard contractual clauses).

4.4 Do the regulations define the scope of data use?

The scope of data use is defined, in the sense that data processing must comply with the above-mentioned principles (see question 4.3). The meaning of "processing" is the same as defined under the GDPR.

4.5 What are the key contractual considerations?

Where the controller engages a processor, their contractual relationship must determine the subject-matter, duration, nature and purpose of the processing, and the type of personal data and categories of data subjects, as well as the parties' rights and obligations. In particular, the contract should stipulate the obligations set out under Article 28 of the GDPR. The same contractual considerations apply when the processor engages a subprocessor, in the sense that the subprocessor should undertake the same obligations that the processor has undertaken against the controller. In case two or more controllers jointly determine the purposes and means of a processing activity, they should determine in a transparent manner their respective responsibilities for compliance with their data protection obligations, and in particular in relation to their obligation to inform the data subject about the processing of their personal data and their obligation to respond to requests by data subjects exercising their data protection rights.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

As analysed under question 4.3 above, the data protection notice provided by controllers to the data subjects should include information about their rights and contact details of the controller and, where applicable, the DPO, where the data subjects can exercise their rights. Where the request is made by electronic means, the controller should respond by electronic means as well, unless the data subject requests otherwise. In other respects, as provided by the GDPR, the right to withdraw consent should be as easy as it was to give consent, and controllers have the obligation to respond to data subjects' requests within one month. That period may be extended by two more months if it is necessary considering the complexity and number of requests received. In any case, the data subject should be informed of any such extension and the reasons for the delay.

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

Data inaccuracy, bias and discrimination issues are addressed by the Hellenic Data Protection Authority under the power conferred to it to monitor compliance with Greek Law 4624/2019 and the GDPR, which amongst others as set out under question 4.3 above, establishes the principle of lawfulness, fairness and transparency, and the principle of accuracy. In general, violations of the data protection regulatory framework may lead to the imposition of administrative sanctions, as provided by the GDPR. Moreover, data subjects may also raise civil claims of the Greek Civil Code. Lastly, certain violations of the data protection regulatory framework may entail criminal sanctions.

Providers of AI systems to public bodies have the obligation to implement by design appropriate measures to safeguard the prohibition of any discrimination, the protection of equality between women and men, freedom of expression, access for individuals with disabilities and the rights of employees. Also, companies who use AI tools in the context of evaluating employees or candidates should ensure compliance with the principle of equal treatment and non-discrimination.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

There is no specific legislative framework for Generative AI companies. Compliance with all data protection requirements should be ensured. Also, Greek Law 4961/2022 includes specific provisions that impose obligations to entities who provide AI systems to public bodies.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The same issues as set out under question 4.1 above should be considered in the context of sharing data as well. Sharing personal data across borders of the EU/EEA gives rise to the compliance obligations of Chapter V of the GDPR, in the sense that in principle they are prohibited unless there is an adequacy decision issued by the European Commission or other appropriate safeguards in place (e.g. standard contractual clauses).

5.2 How do such considerations change depending on the nature of the entities involved?

Law 4624/2019 includes different provisions for controllers who are public and controllers who are private entities, for instance, when it comes to processing personal data for reasons different from the ones they were collected for, and in relation to processing activities on special categories of personal data.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The key regulatory requirements mentioned under question 4.3 are applicable in the context of sharing data.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

As mentioned in question 2.1 above, many governmental initiatives have taken place in Greece in order to establish a legal framework regarding those issues.

5.5 What are the key issues 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. The key issues to consider that apply are the issues mentioned under section 4.

6 Intellectual Property

6.1 What is the scope of patent protection for digital health technologies?

According to the Greek Patent Law, as well as Greek Law 1607/1986 on the "Ratification of the European Patent Convention", inventions are patentable provided that they are new, they involve an inventive step and are susceptible of industrial application. According to par. 2I of Article 5 of the Greek Patent Law, computer programs are not patentable; however, the foregoing exclusion from patent protection applies to the extent that the patent application relates to a computer program as such. Inventions involving software are not excluded from patentability as long as they have a technical character. Additionally, the patentability of AI technology is also debatable. According to the European Patent Office's Guidelines for Examination, even though AI technology is based on computational models and algorithms and the latter as such are excluded from patentability, nevertheless, inventions using AI technologies can be patentable when they solve a technical problem in a field of technology. In terms of inventorship, it should be noted that under the European Patent Convention (EPC), the legal concept of inventorship requires a human being to be the inventor.

6.2 What is the scope of copyright protection for digital health technologies?

Greek Law 2121/1993 on Copyright (Greek Copyright Law) protects both literary and artistic works in a broad sense. The foregoing law confers protection to computer software as well. It should be mentioned, however, that copyright is an unregistered right and thus, protection achieved under the provisions of the Greek Copyright Law might be less efficient than the protection conferred under patents.

6.3 What is the scope of trade secret protection for digital health technologies?

Greek Law 4605/2019 on the harmonisation of Greek legislation to Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure may be invoked for the protection of AI systems from illegal possession or usage from third parties.

A trade secret means information that fulfils all of the following conditions: (a) it is secret; (b) has commercial value resulting from its secret nature; and (c) the person lawfully in control of that information has made reasonable efforts, taking into account the circumstances, to protect its confidentiality.

Trade secrets are unregistered rights and thus, provided that the foregoing conditions are met, wrongful acquisition or disclosure of such information is prohibited.

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

Under the technology transfer contract, the technology donor is obliged to provide the receiver with the technology and the receiver is obliged to pay the agreed price. The contract shall be registered in the Technology Transfer Register. Academic technology transfer in Greece is regulated under the provisions of Articles 21 and 22 of the Greek Patent Law, Article 23 of the Greek Law 2741/1999 and Law 4310/2014. The aforementioned laws apply, *inter alia*, to technology transfer contracts, filing of technology transfer contracts with the National Industrial Property Organization, licensing and institutional matters.

6.5 What is the scope of intellectual property protection for software as a medical device?

Under the provisions of the MDR, software may be considered as a medical device under certain conditions defined in Annex VIII to the MDR and can be classified in all four risk classes, according to their intended purpose and their inherent risks. As to the protection of software *per se* either under the patent or the copyright legislative framework, the analysis under questions 6.1 and 6.2 applies *mutatis mutandis*.

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

Whether an AI device can be recognised as inventor of a patent is a much-discussed issue. In the context of the Greek Copyright Law and Greek Patent Law, which follow an anthropocentric approach, the creator/inventor of a work always corresponds to natural persons. Therefore, for the time being, as analysed hereinabove, in compliance with the EPC, only humans can be considered inventors and thus, can be granted patents in Greece.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

The provisions on service or dependent inventions, as per Article 6 of the Greek Patent Law, apply *mutatis mutandis* to the IP rights on government-funded inventions.

7 Commercial Agreements

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

Collaborating parties shall clarify the applicable legal and regulatory framework. In their contract they shall agree on the results of their partnership, the allocation of IP rights, liability-related matters, including, *inter alia*, product liability issues.

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

Agreements between healthcare and non-healthcare companies shall ensure that the non-healthcare companies comply with the specific rules and regulations applicable to healthcare companies, in particular on a regulatory level, including, indicative compliance with the provisions of the overseeing authorities' circulars, announcements, guidelines and the applicable code(s) of ethics.

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

Federated learning allows multiple healthcare institutions to collaborate and train machine learning models based on decentralised data without the need for sharing sensitive patient information. Parties shall consider the importance of patients' security and data protection.

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

Parties should take into consideration the strict regulatory and legal requirements that apply and guarantee the protection of patients' personal data and rights through their transparent activity.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning has an assistive role in digital health. It provides physicians with accurate information, helping them in their research, their practice and their decision making. It also contributes, among others, to automating hospital processes and even diagnosing diseases.

8.2 How is training data licensed?

Currently, in Greek Law there are no provisions specifically regulating the licensing of training data; said are subject to the general provisions on licensing.

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

Currently, in the context of the Greek Copyright Law, which follows an anthropocentric approach, IP rights are owned only by natural persons who were involved in the development of the algorithms.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Security, data protection and transparency are key.

9 Liability

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

1. Civil Liability: Healthcare service providers may bear contractual and non-contractual liability towards patients if they act illegally and cause damage to patients by fault or negligence. Provisions of Greek Civil Code, in particular Articles 914 and 330, and provisions of Greek Law 2251/1994 on Consumer Protection, namely Article 8, are applicable.
2. Criminal Liability: Healthcare service providers may bear criminal liability in accordance with the provisions of the Greek Criminal Code.
3. Regulatory liability: Competent authorities may impose administrative functions in case of non-compliance with the regulatory framework.

9.2 What cross-border considerations are there?

From a data protection standpoint, see the answer to question 5.1.

9.3 What are best practices to minimise liability risks posed by the use of generative AI in the provisioning of digital health solutions?

Compliance with the protection legislation and the AI-related provisions under Law 4961/2022 are key to minimise risks posed by the use of generative AI in the provisioning of digital health solutions.

10 General

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

From a data protection legislation standpoint, compliance with applicable legislation is a key issue and in particular the personal data transfer provisions where Cloud-based services are not hosted within the EEA.

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

Companies that wish to engage in the digital healthcare market must be particularly mindful of the deficient regulatory framework and institutional gaps which create considerable market ambiguities.

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 healthcare ventures in Greece presupposes a thorough understanding of the regulatory landscape and the local market. Venture capital and private equity firms should consider, *inter alia*, the following key issues before making an investment in digital healthcare in Greece:

1. Regulatory environment: Understand the regulatory framework (or lack thereof) and institutional gaps.

2. Market landscape: Assess the level of adoption of digital health technologies locally. Identify key players, competitors and potential areas for disruption.
3. Healthcare infrastructure: Evaluate the existing infrastructure and assess how well digital solutions can integrate within the current healthcare system.
4. Patient data privacy and security: Assess how patient data shall be handled in compliance with data privacy and date security rules.
5. Reimbursement policies: Understand the potential for reimbursement and assess whether the existing landscape supports or hinders a particular digital health solution.

By thoroughly examining these factors, venture capital and private equity firms can make more informed decisions when investing in digital healthcare ventures in Greece.

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

Lack of existing legislative and regulatory provisions, as well as reimbursement-related matters, could be considered as some of the key barriers for adopting digital health solutions in Greece, on a wide scale.

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 MoH is primarily the competent body for any health-related decisions, policies and solutions; depending on the matter at hand, the Ministry of Digital Governance may also be competent.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Digital health tools are not, in general, reimbursed in Greece and no operational framework exists for digital health providers in particular.

10.7 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 the context of its strategic planning for its digital transition, Greece has prioritised the digital transformation of the healthcare sector, through the Digital Bible of Transformation, and the Recovery and Resilience Plan Greece 2.0. The Bible includes 22 digitisation projects, 10 of which are ongoing. These include the completion of the electronic patient file, the upgrade of digital infrastructures in the public sector hospitals (with an emphasis on the development of clinical information systems and the input of data available in the electronic health record), the expansion of telemedicine solutions and the digitisation of cancer management. So far, they have been included in two pillars, with a total budget of over €780 million and should be completed by the end of 2025. Indicatively, the most important are:

- The projects for the digitisation of the Public archives, the provision of Cloud infrastructure and the national payer's (EOPYY) digital transformation.
- The digitisation project of the NHS archives (€235.6 million), which concerns the digitisation of approximately 200 million pages and imaging examinations that shall be available through the electronic health record.
- The extension of the National Telemedicine Network.
- The projects of improving the digital readiness of hospitals (€173.1 million) and the National Electronic Health File (€55.9 million).
- The project of installing RIS PACS systems in public hospitals (€36.3 million).

Bearing the above in mind, it can be said that so far, emphasis has been given by the State to the digitisation of systems and processes, as well as promoting interoperability. Next steps should also include the establishment and/or updating of the corresponding regulatory frameworks and providing strategic incentives to investors to invest in digital health solutions.

Nefelie Charalabopoulou is head of the Zepos & Yannopoulos healthcare, pharma & life sciences practice. Nefelie practises corporate, commercial and healthcare law. She focuses on advising clients in highly-regulated industries on all inherent legal and compliance issues, with an emphasis on pharmaceuticals, medtech products, biotech and cosmetics. She also advises them on their corporate law matters. Her extensive experience in the life sciences sector is particularly valuable; it allows her to thoroughly understand and analyse the complex environment in which her clients operate and helps them to achieve breakthrough results. She supports domestic and multinational stakeholders on a wide range of regulatory and compliance issues, such as marketing authorisations and registrations, pricing and reimbursement, licensing and distribution, interactions with HCPs/HCOs, clinical trials, promotional activities, etc.

Zepos & Yannopoulos
280 Kifissias Avenue
152 32 Halandri, Athens
Greece

Tel: +30 210 6967 000
Email: n.charalabopoulou@zeya.com
LinkedIn: www.linkedin.com/in/nefelie-charalabopoulou

Natalia Kapsi is a member of the Zepos & Yannopoulos healthcare, pharma & life sciences practice. She focuses on corporate, commercial, pharmaceutical and IP law. She has experience in advising multinational healthcare companies on regulatory, commercial and compliance issues, with an emphasis on regulations, standards and codes of practice related to the marketing and promotion of pharmaceutical products, medical devices and cosmetics. Natalia also provides advice to multinational tobacco companies on a wide variety of regulatory and commercial matters, particularly the marketing, promotion and advertising of Next Generation Products. In addition, she focuses on all areas of IP – such as trademarks, copyrights and patents – advising clients on both contentious and non-contentious IP issues and representing them before the Administrative Committees, as well as Civil and Administrative Courts.

Zepos & Yannopoulos
280 Kifissias Avenue
152 32 Halandri, Athens
Greece

Tel: +30 210 6967 000
Email: n.kapsi@zeya.com
LinkedIn: www.linkedin.com/in/natalia-kapsi

Yolanda Antoniou-Rapti focuses on Greek and EU data protection, privacy, cybersecurity, competition & antitrust, corporate and commercial law. She advises on all aspects of EU and Greek data protection compliance issues, including assisting clients in identifying compliance gaps, both in the context of GDPR compliance audits and M&A due diligence reviews, assessing and managing relevant risks, and in taking steps to ensure overall compliance, including conducting trainings and workshops. Yolanda's practice also covers data protection litigation, as well as advisory and assistance tasks on day-to-day matters, including drafting and negotiating privacy terms in contracts, drafting privacy policies and notices, data processing agreements, consent forms, the use of new technologies, ePrivacy issues, data breach management and notification, international data transfers and carrying out data protection impact assessments.

Zepos & Yannopoulos
280 Kifissias Avenue
152 32 Halandri, Athens
Greece

Tel: +30 210 6967 000
Email: y.antoniou@zeya.com
LinkedIn: www.linkedin.com/in/yolanda-antoniou-rapti

Celia Karvouni is a member of the Zepos & Yannopoulos M&A and project development practice, as well as the healthcare, pharma & life sciences practice. She joined our team as a trainee lawyer with great interest in corporate, pharmaceutical and civil law. Celia regularly focuses on corporate and commercial matters on the day-to-day operations of international and domestic clients, including the drafting and review of commercial contracts and corporate resolutions. She joined the firm in September 2023.

Zepos & Yannopoulos
280 Kifissias Avenue
152 32 Halandri, Athens
Greece

Tel: +30 210 6967 000
Email: c.karvouni@zeya.com
LinkedIn: www.linkedin.com/in/vasiliki-celia-karvouni-629a18208

Zepos & Yannopoulos is a leading Greek law firm known for its long heritage, legal acumen and integrity. As a full-service business law firm, we take pride in our distinctive mindset and offering. This shows not only in responsiveness, but also our ability to field versatile, approachable, easy-to-work with teams of practitioners who truly understand our clients' interests. Our strong international orientation is echoed in our structure, standards and approach, and ultimately attested in the profile of our client base, our rankings and the network of our affiliations and best-friend law firms around the world. Established in 1893, we know that change, whether in the legal or economic environment, is inherent to our jurisdiction; we are accustomed to implementing untested legislation, structuring innovative solutions and putting our bold legal argumentation to the service of our clients. For more details on our firm and practice please visit our website.

www.zeya.com

ZEPOS & YANNOPOULOS

India

LexOrbis


Manisha Singh


Pankaj Musyuni

1 Digital Health

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

The term "digital health" signifies a broad idea that entails establishing an alliance among digital technologies and the healthcare business in order to improve healthcare efficiency and provide patients with more personalised care. Although the phrases "digital health", "digital medicine" and "digital therapeutics" are not specifically defined in India, the Digital Information Security in Healthcare Act of 2018 (DISHA) defines "digital health data" as providing an electronic record of an individual's health-related information. The relevant information on a person's physical and mental health, the treatments they have gotten from health providers, any body parts or biological material they have donated, and test and examination results are often included in the term "said data". The integration of genetics and digital technologies for early disease detection and treatment best exemplifies the concept of digital health.

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

Many businesses have embraced digital transformation as a fact of the information age. After all, it is important to provide value to customers. M-Health, digital pathology, telemedicine, health wearables, digital and social connectivity, big data analytics, virtual reality, ambupods, blockchain and electronic medical records are some of the key emerging digital health technologies.

1.3 What are the core legal issues in digital health for your jurisdiction?

Data security is necessary for ensuring the privacy of health-related information shared between patients and medical practitioners, including recommendations and outcomes. The Information Technology Act of 2000 (IT Act), the Intermediaries Guidelines of 2011 and the Data Protection Rules of 2011 are meant to address this need and should be consulted in every circumstance; however, no standards have been developed to mandate the implementation of data security and protection due to their stringent compliance requirements. Concerns around patient privacy and data security are also increasing in tandem with the proliferation of digital and other advanced healthcare technologies. The key concerns with transmitting personal data include confidentiality, data exchange control, security and privacy, as well as awareness, trust, accountability and responsibility.

The Ministry of Health and Family Welfare (MoHFW) has suggested establishing the National Digital Health Authority (NeHA), which will be responsible for developing India's Integrated Health Information System (IHIS). It is proposed that it serve as an agency that supports, monitors and establishes policies to lead India's transition to digital health and the benefits gained in the health sector. On August 11, 2023, India passed the Digital Personal Data Protection Act, 2023 (DPDP Act). This new law governs how personal data is handled in India. It aims to protect people's privacy while also establishing a framework for data accountability and governance. The DPDP Act will have a significant impact on the Indian healthcare sector, which is still in the early stages of digital transformation. The DPDP Act, which is focused on digital personal data, does not cover non-personal data. When the DPDP Act's provisions take effect, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data of Information) Rules, 2011 (SPDI Rules) and Section 43A of the IT Act will be superseded. These pieces of legislation address the legal and ethical challenges in digital health.

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

In light of the growing prominence of digital healthcare business and favourable government policies, India's digital adoption has increased significantly. The digital health industry in India is expected to increase from $3.83 billion in 2022 to $18.34 billion by 2030, at a CAGR of 21.6% between 2022 and 2030. According to Insights10, a healthcare-focused market research agency, a combination of a vast potential market and supporting government regulations is projected to generate robust growth in the Indian digital health market in the coming years.

1.5 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. More promising digital health start-ups in India include Netmeds, HealthifyMe, cult.fit, PharmEasy and Innovaccer.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The IT Act, the SPDI Rules and the Intermediary Guidelines comprise India's general framework for data protection. The IT Act's enhanced security safeguards make online transactions and electronic data transfers safe. The IT Act governs various internet activities, including the legal status of electronic records and the authentication of digital signatures. The IT Act covers a wide range of cybercrimes, including hacking and denial-of-service attacks. Furthermore, India enacted the DPDP Act. The DPDP Act's key purpose is to increase accountability and responsibility for enterprises that operate in India, such as mobile app developers, internet service providers and companies that collect, store and handle personal data on Indian citizens. This Act, with a particular emphasis on the "Right to Privacy", strives to ensure that these companies function clearly and are accountable when it comes to handling personal data, therefore prioritising Indian individuals' privacy and data protection rights.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The IT Act and the SPDI Rules control India's present legislative framework for e-health protection, which give some protection for the collecting, disclosure and transfer of sensitive personal data such as medical records and histories. The government and the MoHFW announced the National Digital Health Mission (NDHM) and published a blueprint recommending the establishment of a National Digital Health Ecosystem to enable interoperability between digital health systems at the patient, hospital and ancillary healthcare-provider levels. The Health Data Management Policy for the ecosystem was issued by the MoHFW. Furthermore, India established the DPDP Act, the primary goal of which is to promote accountability and responsibility for enterprises working in India.

Among the significant ongoing digital health initiatives being carried out by the MoHFW are 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. Since health is a state duty, the National Health Mission funds states for related services such as hospital information systems, telemedicine, teleradiology, tele-oncology and tele-ophthalmology.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The Designs Act of 2000 safeguards healthcare devices. Only qualities of shapes, configurations, patterns, decorations, or line or colour compositions given to an "article" are called "designs". The two key areas of digital health that require design protection are the graphic user interface (GUI) of programs and the design of devices. The Designs Act, specifically Article 14-04 of the Design Rules, 2001, which covers "Screen Displays and Icons", may safeguard a GUI. Furthermore, the Central Drugs Standard Control Organization (CDSCO) has produced a draft list of risk classifications for medical devices into 24 major groups, with independent software classified separately.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The CDSCO is the primary regulatory body responsible for enforcing the Drugs and Cosmetics Act, 1940 and "rules made thereunder" (DCA). Additionally, the Medical Council of India regulates medical practice. Moreover, the Office of the Controller General of Patents, Designs and Trademarks is in charge of intellectual property protection, while the Copyright Office is in charge of copyright. Both are divisions of the Department for Promotion of Industry and Internal Trade. The Indian Council of Medical Research has also done a lot to promote research in support of the National Digital Health Blueprint from the MoHFW.

Typically, the following significant acts govern the legal and regulatory framework:

- The IT Act, composed of the SPDI Rules and the Information Technology Rules of 2011.
- The New Telecom Policy of 1999 Requirements for Other Service Providers.
- The DCA.
- The Indian Medical Council Act of 1956 and the Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations of 2002.
- The Drugs and Magic Remedies Act of 1954 and the Drugs and Magic Remedies Rules of 1955, which regulate the use of drugs and magic remedies.
- The Commercial Communication Customer Preference Regulations of 2010 and the Unsolicited Commercial Communications Regulations of 2007.
- The Clinical Establishments Act of 2010.
- The DPDP Act.

2.5 What are the key areas of enforcement when it comes to digital health?

It is essential to enforce rules that ensure the security, confidentiality and privacy of patients' health and medical records. Considering private health information and records are kept under confidentiality agreements and are only used for data interpretation for market analysis, marketing and regulatory sharing, keeping track of data protection and violations is necessary.

2.6 What regulations 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 CDSCO is led by the Drug Controller General of India (DCGI). Certain medications (vaccines, large-volume parenterals, blood products and r-DNA-derived products), medical devices and novel drugs are approved by the DCGI. The DCA govern the manufacture, importation, sale and distribution of medical equipment in India. Only the notified medical devices listed below are currently controlled as "drugs" in India under the DCA:

(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, tubal rings).

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

There are currently no official rules.

3 Digital Health Technologies

3.1 What are the core legal or 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 Internet of Things (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 issues for digital platform providers?

Digital platform providers are typically preoccupied with assessing and overseeing the transitional stage of delivering new technologies to market, as well as mitigating risk. Consequently, some of the most important things for digital platform providers to focus on include personnel training, understanding the importance of market demand and in-line supply, upgrading and improving IT systems, and practising sound leadership.

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

When it comes to the use and implementation of personal data, data privacy is extremely important. In 2013, the first Electronic Health Record (EHR) standards in India were proposed. They were chosen from among the finest available and have already implemented international EHR standards due to their relevance in India. As a result, the 2016 EHR Standards document was alerted to and made available for implementation in national IT systems by healthcare institutions and providers. The MoHFW is promoting its adoption by making standards such as the Systematized Nomenclature of Medicine–Clinical Terminology free to use in India and establishing an interim National Release Centre to manage the clinical terminology standard, which is gaining global acceptance among healthcare IT stakeholder communities. The MoHFW plans to promote and adopt e-health standards, enforce privacy and security measures for electronic health data, and regulate the storage and exchange of EHRs.

4.2 How do such considerations change depending on the nature of the entities involved?

Among the entities involved in collecting data, record-keeping and information exchange are hospitals, research organisations and technology service providers. Furthermore, these procedures can be adjusted in response to continuing experiences and problems observed during the consumer-service provider transition, lag period and linkage.

4.3 Which key regulatory requirements apply?

The MoHFW intends to create a statutory national digital health authority to promote and implement e-health standards, enforce privacy and security safeguards for electronic health data, and govern the storage and sharing of EHRs. The planned Authority (NeHA) will also be in charge of developing India's IHIS. It is suggested that it will act as a promotional, regulatory and standard-setting agency, guiding and supporting India's digital health. It also defines the NeHA's proposed functions and governing structure. The DISHA intends to legally establish the NeHA and promote online patient data exchange in order to avoid duplication of efforts and resources.

4.4 Do the regulations define the scope of data use?

Yes, the regulations establish the scope of information use with beneficiary and service provider consent, as well as the requirements for "sensitive health-related information" and "sensitive personal information".

4.5 What are the key contractual considerations?

Contracts are the most effective approach to ensure that all aspects of the investigation, from data gathering to data use, remain secret and discreet. Employees and other influencers who participate in the research, for example, should sign non-disclosure and personal privacy agreements, and more choices should be available if pre-defined contractual criteria are violated.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Data confidentiality and sampling with intent are key concerns, and the lack of clearly defined legal remedies causes challenges. There is an imperative necessity to defend and preserve full rights so that individuals can receive better care and a more evidence-based healthcare system.

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

It is important to address issues about data inaccuracy, bias and/or discrimination through a comprehensive legislative framework governing the acquisition and dissemination of personal data. The DPDP Act is now in effect, and it governs the processing of digital personal data in India, regardless of whether the data was obtained in digital or non-digital format and then digitised.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

Inadvertently, generative AI models can learn and repeat sensitive information from training data. As a result, outputs containing secret information may be generated, which, if shared or made public, may jeopardise confidentiality. There are numerous legal and ethical concerns with generative AI. Biased and incorrect information, copyright and intellectual property difficulties, and data privacy violations are the three most serious risks. The Consumer Protection Act (CPA) sets a structure for resolving consumer disputes and safeguards consumer interests. The CPA was developed to provide clients with a mechanism to settle grievances without having to go through the time-consuming and expensive process of filing a civil lawsuit.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Some of the most significant considerations when exchanging personal data include flexibility and data collection and transfer, security and privacy during the transformation process, and information sharing, trust, responsibility and accountability.

5.2 How do such considerations change depending on the nature of the entities involved?

Such variables are critical and highly influenced by the overall number of participants and scientific entities. Furthermore, the goal of leveraging data protection and privacy to acquire answers quickly may have an impact on data sharing, which is a crucial consideration that all parties involved should consider at each stage of the process.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The DISHA concept was developed by the MoHFW with the goal of preserving healthcare data in India and allowing customers ultimate ownership over their health data. For example, if a patient goes in for a check-up and the doctor looks up the patient's previous medical history and inputs the current diagnostic results into an EHR, the DISHA ensures that the information is secure as it moves around the healthcare system. The DISHA identifies three key data protection objectives: establishing a national and state digital health authority; implementing privacy and security measures for electronic health data; and regulating electronic health information storage and exchange.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

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 to consider with respect to federated models of healthcare data sharing?

Meeting regulatory standards, enhancing trustworthiness and ensuring data sovereignty are critical issues for data healthcare sharing.

6 Intellectual Property

6.1 What is the scope of patent protection for digital health technologies?

The Patents Act of 1970, which provides patent protection and

is consistent with the Agreement on Trade-Related Aspects of Intellectual Property Rights, has been adopted and implemented by India. In addition to meeting the patentability requirements of novelty, inventive step and industrial applicability, to obtain patent protection in India, the invention must fall outside the scope of Sections 3 and 4 of the Act. Section 3(k) of the Patents Act, which prohibits the patentability of a computer program by itself, is applicable because digital health applications rely on software and a computer program. In addition, the Delhi High Court clarified that not all computer programs are exempt from Section 3(k) and that the invention is patentable if the computer program demonstrates a "technical effect" or "technical contribution".

According to Section 3(i) of the Patents Act, a patent cannot be granted if the program or method relates to "a process for the 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". In contrast, the apparatus and method for using an *in vitro* mechanism are patentable.

6.2 What is the scope of copyright protection for digital health technologies?

In India, intellectual property is protected by the Copyright Act of 1957. Original literary, dramatic, musical or aesthetic works, cinematograph films and sound recordings can all be protected by copyright. Although copyright registration is not required, it serves as *prima facie* evidence in establishing a legal claim. Because digital health applications are fundamentally software, they fall under the definition of "computer program" and are thus protected by copyright laws.

6.3 What is the scope of trade secret protection for digital health technologies?

In India, there is no explicit law governing the handling of sensitive information and trade secrets for digital health technologies. Non-disclosure and confidentiality agreements are commonly employed in the new digital health industry to secure this type of sensitive information.

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

In India, the concept of academic technology transfer is still in its infancy. Although colleges and some organisations have adopted this approach and set standards for strategically deploying breakthroughs and rewarding inventors, the vast majority of organisations have not. Furthermore, intellectual property protection in the digital health industry is still in its infancy; yet, it is growing at an exponential rate, and academic and research institutions are becoming increasingly conscious of its significance. This pattern appears to be gaining traction and yielding better results. Academic technology transfer activities include: evaluating and assessing the proposed invention in terms of patentability and commercialisation; protecting intellectual property; and searching for and finding the best partner for licensing and monetising the proposed technology and how it works.

6.5 What is the scope of intellectual property protection for software as a medical device?

Section 3(k) of the Patents Act prohibits the patentability of computer programs in general. The Delhi High Court has clarified that Section 3(k) does not apply to all computer programs and that such programs can be patented if they demonstrate a "technical effect" or "technical contribution". A patent cannot be granted under Section 3(i) of the Patents Act if the program or process relates to "a process for the 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.

As digital health applications are fundamentally software, they should be classified as "computer programs" and granted copyright protection under Indian law. A trademark can also be registered in class 9, which includes computer software and computer programs.

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 identified as the inventor of a patent in India. Various provisions of the Indian Patents Act and related patent forms specifically provide for humans as inventors, and thus cannot be extended to AI applications or devices unless clearly mentioned.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

There are currently no specific regulations for government-funded inventions.

7 Commercial Agreements

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

A number of factors can be considered to ensure collaborative improvements work, including the collaboration's main goals, information about all eligible members and parties involved, governance and contract management, confidentiality, and evaluation of current intellectual property and technology transfer procedures, together with data on existing intelligence.

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

The working principles and work-flow methods of healthcare and non-healthcare organisations are radically different in terms of internal communications and offering services externally; nonetheless, client satisfaction is the top goal for both sectors. In addition to the confidentiality protocol for data exchange, data protection, security and privacy, approaches to information sharing must be reviewed while reviewing agreements.

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

It is significant to monitor and study design, consistent protocols for data gathering, structured reporting and advanced

methodologies for finding bias and concealed stratification, as well as sign a non-disclosure agreement.

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

Companies should not put sensitive information or personal data into generative AI tools. Entering such data into a generative AI tool may be prohibited by data protection regulations, or it may violate a confidentiality agreement given to a third party. Maintaining data privacy and interpretation is also significant.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning's key roles in digital health include: facilitating the use of numerous methods and processes to reduce cost, time and effort; assisting with drug development and production; examining machine learning-based behaviour modifications; keeping and securing medical records; outbreak prediction; and clinical experimentation, data collection and data mining.

8.2 How is training data licensed?

In the absence of particular AI, Cloud computing and machine learning rules in India, operations involving these technologies must abide by ordinary IT laws and regulations. A confidentiality agreement between the licensee and the data owner, as well as a strategy for how the data will be utilised, would be beneficial.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning 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 considerations apply to licensing data for use in machine learning?

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, term and termination are all important factors to consider.

9 Liability

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

Liabilities for negative consequences may be civil or criminal, and they differ between service practitioners and service providers such as institutes and internet service providers. In addition to filing a legal complaint, the CPA's remedies may be used in civil proceedings. A consumer may also file a complaint with the Medical Council of India's ethics committee in the event of a doctor's carelessness. Criminal responsibility is further addressed in the Indian Penal Code, which is vital for digital health solutions as well.

9.2 What cross-border considerations are there?

It is critical to use data programs and to customise data.

9.3 What are best practices to minimise liability risks posed by the use of generative AI in the provisioning of digital health solutions?

Maintaining confidentiality and privacy, establishing work groups to oversee the process, educating and training leaders, defining AI policy, updating privacy policy and conducting security assessments are all part of the process.

10 General

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

The costly expense of developing and maintaining health information technology, as well as storing data while maintaining confidentiality and privacy, is a persistent worry in digital health. Another consideration is the security and privacy of data management at various phases of transformation.

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

Non-healthcare businesses must understand that the healthcare industry maintains secure manufacturing and marketing standards, as well as excellent financial planning and data protection and security measures. Furthermore, consumer protection laws apply to the healthcare industry.

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

Before investing in digital healthcare startups, venture capital and private equity firms should consider a number of crucial aspects. These include a sound business plan, market opportunities, strategic relationships, an understanding of the company's financial and key metrics, potential risk, estimated valuation, regulatory compliances and intellectual property protection.

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

Data interoperability, particularly for health records, data security and privacy are the key impediments to widespread implementation of digital health technology in clinical settings.

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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with 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 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 expected to flourish in a variety of sectors, including telemedicine, personalised medicine, genomics and wearables. To develop and deliver breakthrough treatments and services, organisers and healthcare providers are embracing sophisticated technologies such as AI, Cloud computing, extended reality and IoT. These technologies offer better healthcare delivery, better patient experiences, and the creation of personalised and data-driven medical treatments. The government is working to create an integrated digital health ecosystem.

Paperless and hassle-free access to digital health records is required. Government initiatives in India, such as the NDHM and Make in India, are hastening the pace of healthcare digitisation. As the government focuses on digital innovation, opportunities for healthcare companies and manufacturers will multiply, and patient outcomes will improve even more. The NDHM is focused on establishing the necessary infrastructure to establish the country's integrated digital health ecosystem. These patterns illustrate the ongoing digital revolution in the Indian healthcare industry. They have the potential to improve care access, patient outcomes and healthcare delivery. It is essential to address issues such as legislative frameworks, data protection, infrastructure shortages 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, FICPI, and is actively involved in their committee work. She is an active writer and regularly authors articles and commentaries for some of the 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

Pankaj Musyuni is an advocate registered with the Bar Council of India, as well as a patent agent. He has a Master's degree in pharmaceutical science and management. He regularly advises clients on IP strategy and portfolio management. Pankaj has in-depth knowledge of patent law and the healthcare regulatory framework in India, as well as extensive experience in patent filing, drafting, prosecution and advisory matters, especially in the chemical, pharmaceutical and start-up fields. He has written several articles and delivered talks at various forums on patent law practice, the regulatory landscape and clinical research.

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

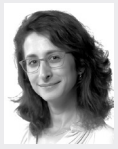
LexOrbis is a premier law firm, and one of the fastest growing IP firms in India, with offices in three strategic locations: Delhi; Mumbai; and Bengaluru. With a team of over 90 highly reputed lawyers, engineers and scientists, we act as a one-stop shop and provide practical solutions and services on all IP and legal issues faced by technology companies, research institutions, universities, broadcasters, content developers and brand owners. Our services include Indian and global IP (patents/designs/trademark/copyright/geographical indication/plant varieties) portfolio development and management, advisory and documentation services on IP transactions/technology-content transfers and IP enforcement and dispute resolutions at all forums across India. We have a global reach with trusted partners and associate firms.

www.lexorbis.com

LexOrbis Intellectual Property Attorneys & Advocates

Israel

Eran Bareket



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.*"

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 technologies 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 are the core legal issues in digital health for your jurisdiction?

The core legal issues in digital health in Israel are:

- How conventional healthcare regulation is to be applied to digital health services.
- Secondary use of health data and how it is de-identified (determining standards of de-identification/hiding identity) – currently regulated in part by the Director-General circular on secondary uses of health data.
- Ownership of health data and rights of use.
- Ownership of products developed based on health data.
- Rights of state hospitals and healthcare organisations to hold equity in start-ups.
- Privacy protection of holders of health data – regulated by the Protection of Privacy Law, 5741-1981 and the Protection of Privacy Regulations (Data Security), 5777-2017.
- Creating a uniform platform for collaborations based on databases of different entities (competition law, standardisation of information, etc.).

The Israeli MOH published in April 2017 "a Digital Health Strategy" document, which sets forth the key enactments for creating a digital health support policy:

- Regulation for the use of health data (goals, manner of use, users, transparency).
- Regulation for the use of remote medical care (the manner in which the service is provided and service provider obligations).
- Regulation for the access of personal electronic health record files by patients.
- Regulation for determining the minimum content of the electronic health records.
- Regulation applying on outcome measures of health data, which collect and monitor health data.
- Regulation for the development and maintenance processes of clinical information systems.
- Regulation for aspects of cyber protection of data.

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

According to Israel's 2022 Annual HealthTech Ecosystem Report published by aMoon-IVC Report, one out of five high-tech companies are healthtech companies. Healthteach companies raised about $2.8 billion in 2022.

According to the website of "The Times of Israel", in the first half of year 2023, Israeli life sciences firms (consisted of digital health, medical devices, biotechnology and pharmaceutical therapeutics) raised $1.4 billion. There is no publicly available data regarding market size in terms of revenues.

1.5 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, according to Israel's 2022 Annual HealthTech Ecosystem Report published by aMoon-IVC Report, the top 10 healthtech financing rounds in 2022 include the following companies: aidoc, a developer of AI algorithms to assist radiologists in the analysis of medical images, such as CT scans, MRIs and X-rays; Viz.ai, a healthcare technology company that focuses on AI applications for the analysis of medical images, particularly in the field of stroke care; Hello Heart, a developer of an application that allows users to manage and monitor their blood pressure; MDClone, a developer of a technology enabling any user or healthcare organisation to organise, access and protect the privacy of patient data; and Lumen, which developed a portable device to measure, track and analyse metabolism.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The General Director ("GD") of the MOH published a few circulars referring specifically to digital health, as listed below:

- GD Circular, dated 17 January 2018, regarding secondary uses of health data.
- GD Circular, dated 17 January 2018, regarding collaborations based on secondary uses of health data.
- GD Circular, dated 11 November 2019, regarding patient access to personal health data: "*Healthcare under your Control.*"

The health data circulars currently prescribe the extent of protection over health data. In general, unless otherwise specified by law or approved by an explicit opt-in, any data under secondary use will be de-identified. Furthermore, any secondary use of health data for research purposes must be pre-approved by the Helsinki Committee.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The following general regulations apply as well to digital health:

- National Health Insurance Law, 5754-1994.
- Public Health Ordinance, 1940.
- Public Health Regulations (Clinical Trials in Human Subjects), 5741-1980.
- Patient's Rights Law, 5756-1996.
- Public Health Ordinance (Food) (New Version), 5743-1983.
- Protection of Privacy Law, 5741-1981 and Protection of Privacy Regulations (Data Security), 5777-2017.
- Class Actions Law, 5766-2006.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The relevant laws applying to consumer healthcare devices or software are:

- The Medical Equipment Act, 5772-2012.
  The MOH nonetheless operates a MAD division (medical accessories and devices), which registers and grants marketing authorisations for medical devices. On a formal level, such registration and approval is voluntary. In practice, hospitals and health maintenance organisations ("HMOs") will not purchase non-approved devices. In addition, the MOH guidelines govern the process of obtaining MOH approval to import and sell medical equipment.
- The Liability for Defective Products Law, 57-401980 is a general law that imposes no fault liability for bodily injury resulting from faulty devices.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The MOH is responsible for registration and marketing approvals (see question 2.3 above), regulates the approval of clinical trials and regulates secondary use of health data.

The Privacy Protection Authority regulates maintenance of databases containing private data and privacy requirements applicable to uses of such data. The privacy protection commissioner has enforcement authority in cases of unauthorised use of data.

In general, the Authority for Law, Technology and Information (responsible for, among other things, the protection of privacy) is the entity responsible for regulating, monitoring and enforcing Israeli privacy laws, including personal data in digital databases. As mentioned above, uses of health data and collaborations involving health data are also regulated and monitored by the MOH.

The courts have jurisdiction over all issues.

2.5 What are the key areas of enforcement when it comes to digital health?

Further to what is stated in question 2.4 above, because 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.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

Software MADs are registered as medical accessories, e.g., CoroFlow Cardiovascular Measurement System & Accessories (software which 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.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

To date, no regulations applying specifically to AI have been enacted in Israel. Notwithstanding the above, digital health devices based on AI were registered in Israel by the MAD Department in accordance with customary guidelines applying to such devices abroad.

The national programme for AI was launched by the Ministry of Innovation, Science and Technology ("MIST") in July 2022. In October 2022, MIST published policy principles of regulatory and ethics for AI in Israel. These principles stated that regulation for the entire field of AI was not necessary at this stage. Instead,

they suggested that each regulator should examine the need for specific regulation in their own field. They also recommended maintaining a government policy based on risk management, dialogue and coordination among government agencies, and the use of soft and advanced regulatory measures (such as voluntary standardisation and self-regulation in appropriate cases).

3 Digital Health Technologies

3.1 What are the core legal or 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? (See question 2.3 in this regard.)
- **Clinical Decision Support Software**
  Clinical decision support systems are currently being developed by various start-ups in Israel. Today 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, simulate professionals' behaviour, by using machine learning. 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, 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 which 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**
  We are not aware of any digital therapeutics widely used in Israel.

- **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 ("NLP") may be used as part of machine learning 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 issues for digital platform providers?

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 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 to consider for use of personal data?

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 privacy protection of the data (including compliance with the Protection of Privacy Law, 5741-1981). See further below.

4.2 How do such considerations change depending on the nature of the entities 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 apply always, regardless of the nature of the entities.

4.3 Which key regulatory requirements apply?

In general, the manner in which health data is used is not statutorily regulated, except for regulation in connection with the protection of data privacy (Protection of Privacy Law, 5741-1981 and Protection of Privacy Regulations (Data Security), 5777-2017). The MOH has issued circulars aimed at regulating secondary use of health data (see question 2.1). Additional relevant law provisions and guidelines include the Patient's Rights Law, 5756-1996, the MOH's guidelines for maintaining the confidentiality and privacy of patients' personal data, and a document of ethics rules of the Israel Medical Association.

4.4 Do the regulations define the scope of 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 What are the key contractual considerations?

The main contractual issues that must be taken into account 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, 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 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Even though the traditional IP rights do not necessarily apply to

data, the key legal issues regarding the securing of comprehensive rights are ownership and exclusivity in the use and collection of the data. For example, exclusivity in the use of data may be beneficial, and the manner in which the data is used is crucial in order to ensure an appropriate use, in accordance with the applicable regulations.

4.7 How are issues with 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.

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.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

Generative AI encompasses legal and regulatory challenges that companies must address, including as explained below:

- Intellectual property – 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 Israel, a recent ruling by the Patents Registrar established 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.
- Data privacy – since generative AI models use large amounts of data (including personal and sensitive data) to train and generate content, generative AI companies must ensure compliance with all privacy protection laws and proper security measures in order to avoid any unauthorised access, misuse or theft.
- Content regulation – generative AI companies must ensure that the contents generated by AI models are not harmful, misleading, offensive or illegal. In addition, such companies should ensure that the content they generate or distribute is accurate, authentic and ethical.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The key area to be considered is the Protection of Privacy Law; for example, does such sharing require consent of the data subject? The general rule is that sharing/disclosure of identified data requires informed consent, while sharing/disclosure of properly de-identified data does not.

Since the use of personal health data (including de-identified data) for research is considered a "clinical trial", the necessary approvals must be obtained beforehand.

5.2 How do such considerations change depending on the nature of the entities involved?

According to the circulars of the GD of the MOH that apply to medical organisations, personal health data should also not be used for inappropriate social purposes, with an emphasis on discrimination in insurance or employment.

In addition, sharing medical data possessed by medical organisations is subject to regulation set by the MOH.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The Protection of Privacy Law, 5741-1981 prohibits the use of personal data or its delivery to another not for the purpose for which it was provided; this presumably does not apply to de-identified data.

In addition, the Protection of Privacy Regulations (Data Security), 5777-2017 states that, in the event of a contract of a database owner with an outside entity for the purpose of receiving a service, a number of provisions must be stipulated in the agreement, including: the data that the outside entity may process and the purposes of the use permitted in the contract; the manner of implementation of data security obligations the holder has; the contract term; and the return of the data to the owner at the end of the contract.

When it comes to medical data, there are specific conditions for data sharing. 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. Data sharing should also be done to advance the medical field. Moreover, this circular prohibits use for improper social purposes, with emphasis on discrimination in insurance or employment. Exclusive use of secondary health data is limited.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

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:

- Innovative Healthcare Data Sharing System – a pioneering system facilitating the exchange and transfer of healthcare data among HMOs and hospitals.
- The 'Tamna' system (Research Infrastructure for Big Data) 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) 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.

5.5 What are the key issues 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, its standardisation, 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 What is the scope of patent protection for digital health technologies?

Patent protection is governed by the Patents Law, 5727-1967. The law defines a patentable invention as one that is a product or process in any area of technology, which is novel, has inventive step and has utility and industrial application. However, the law excludes a certain type of invention: a process for human medical treatment. Diagnostic and veterinary methods are not excluded *per se*.

A discovery, scientific theory, mathematical formula, game rules and computer software *per se* are not patentable, due to case-law precedents. In general, if the invention involves a technological solution to a technological problem, it is patentable, whether the solution is in the software or not. There is no specific legislation applicable to digital health inventions or technologies, and every application is examined on its merits.

6.2 What is 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 ("GUIs") 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.

6.3 What is the scope of trade secret protection for digital health technologies?

Trade secret protection is governed by the Commercial Torts Law, 5759-1999. A trade secret is defined as "business information, of all kinds, which is not in the public domain and is not easily disclosed by others lawfully and the confidentiality of which affords its owners a business advantage over their competitors, provided that its owners take reasonable steps in protecting its confidentiality". The law prohibits misappropriation of a trade secret which is defined as: (1) taking a trade secret without the owner's consent by improper means, or the use of the secret by the acquirer; (2) use of a trade secret without the consent of its owner where the use is contrary to a contractual obligation or a duty of trust the user has to the trade secret owner; and (3) acquiring a trade secret or using it without the consent of its owners, where it is clear that the trade secret has been unlawfully obtained according to (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 but there is no specific legislation applicable to digital health technologies.

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 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 What is 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 (see above).

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 are the core rules or laws related to government-funded inventions in your jurisdiction?

The Law for the Encouragement of Industrial Research and Development, 5744-1984 sets forth the establishment of the Israel Innovation Authority ("IIA") (previously known as 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 State grants funding, generally 50 per cent of the capital required for the completion of the development plan including protection of IP. 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.

7 Commercial Agreements

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

In general, the following points should be addressed:

- the Research and Development ("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;
- Intellectual Property: ownership and licences to background and foreground IP; and responsibilities and duty to collaborate in the enforcement of foreground IP; and
- 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 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 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 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:

- Intellectual property – 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 is the role of machine learning in digital health?

Healthcare and academic entities, as well as companies, use machine learning in order to develop personalised, preventive, predictive and participatory medicine, including medical tools. For example, machine learning is used for drug repurposing or digital pathology (analysis of pathology slide images). In research performed in Israel, a deep learning algorithm trained on a linked data set of mammograms and electronic health records was found to be able to assess breast cancer at a level comparable to radiologists and to have the potential to substantially reduce missed diagnoses of breast cancer.

8.2 How is training data licensed?

There is neither specific legislation nor case law on the subject, but it seems that a licence must be obtained; as such, activity will more probably than not be considered fair use.

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

Ownership of an enhanced machine learning 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 intellectual property created by machine learning, 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 considerations apply to licensing data for use in machine learning?

Some of the main commercial considerations are:

- restrictions on the ability of the owner/possessor of the data to out-license the data (for example, due to privacy law restrictions);
- preventing misuse of licensed data (e.g. unlawful copying or unlawful disclosure to third parties); and
- remuneration to be received (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).

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 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.

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, 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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with 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 regulatory defined as MAD (medical accessories and devices), 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 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 Privacy Protection Authority 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.

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

Alexandra Cohen holds an LL.B. degree, 2016, from Tel Aviv University.
She handles various aspects of IP rights, including patents, trademarks, designs and copyrights, and represents clients in litigation proceedings before Israeli courts and the Registrar of Patents, Designs and Trademarks. She also provides services with respect to commercial law as well as privacy law and regulations.
In 2016, Alexandra started her internship at Gilat, Bareket & Co. and gained experience in patents, trademarks, copyrights and commercial wrongs litigation. As of 2018, Alexandra continues her practice as a lawyer at Gilat, Bareket & Co.

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 Intellectual Property 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.
Reinhold Cohn Group and its team of professionals are internationally renowned for excellence and continually ranked amongst the top tiers in leading international and local guides.

https://gilat-bareket.rcip.co.il/en

Gilat Bareket Attorneys at Law | Reinhold Cohn Group

Italy


Sonia Selletti


Giulia Gregori


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 (ICT) 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, WHO). 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 technologies in your jurisdiction?

Though technological advancement occurs at a fast pace, technology applications and their use do not take place at the same speed. The factors that slow down the use of technologies in healthcare in Italy mainly concern costs related to the initial economic investment, cultural resistance of a part of the population (not necessarily the elderly, which according to some studies have shown to be able to use digital technologies for healthcare purposes), and regulatory compliance.

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 (Ministerial Decree of 7th 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.

However, it should be considered that a recent survey conducted for FNOMCeO (the National Association of Surgeons and Dentists) highlighted that 92% of Italian people are in favour of AI, but only as an ally and to support physicians.

Furthermore, in November 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 more and more 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 are the core legal issues in digital health for your jurisdiction?

The main legal issues are: protection of privacy (see section 4); safety; and liability for damages to the subjects involved in their use. Informed consent is even more important: the user must be properly informed in accordance with current legislation. This includes the scope of the health act, the use of innovative (digital) means and the benefits/risks that may result. The use of new healthcare IT implies requirements and training for the various subjects involved (HCPs, healthcare organisations (HCOs), suppliers, producers, developers, patients, etc.), and wise liability management.

1.4 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 electronic health records or the first regulations governing telemedicine.

Given their potential as regards health safeguards and costs, it is reasonable to expect that digital solutions will become increasingly

widespread over the next few years. This is also the direction taken by Italy's National Recovery and Resilience Plan (PNRR) (a document drawn up by the Italian Government to illustrate how it intends to manage the funds of the Next Generation EU programme set up by the EU in response to the pandemic). The PNRR subdivides its interventions into six main missions, including digitalisation, health and ecological transition, which provides for a substantial fund to be set up, on the one hand to strengthen so-called proximity networks, intermediate structures and telemedicine for territorial healthcare, and, on the other hand, to enable the upgrade and development of the existing technological and digital structures in the health sector.

In this context, it is vital that the development of digital health be accompanied by specific, uniform legislation guaranteeing appropriate regulation and support, so that all the potential offered by digital technology can be exploited in full.

1.5 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 Dedalus Italia S.p.A., 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.

In strategic terms, it is important that companies active in digital health form relationships with the public sector in order to establish essential public/private collaboration, generating positive synergies. Public investment and private investment are a means to make the health service stronger.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

In Italy, the public system for protecting citizens' health is structured around the *Servizio Sanitario Nazionale* (National Health System – NHS), established with Law no. 833/1978 and inspired by the principles of universality, equality and equity in access to care, as per Art. 32 of the Italian Constitution, which protects health as a "fundamental right of the individual and an interest of the community", and entrusted to the State and public bodies of the NHS. In one word: the State identifies the fundamental principles and determines the essential assistance levels (LEA) guaranteed as a standard throughout the country; the Regions establish health policies for local organisations and access to care. Health services are provided by the public structures of the NHS (hospitals and local health facilities), as well as by private structures duly authorised and accredited to exploit health activities with charges borne by the NHS.

According to the Ministerial Decree of 23rd June 2023, in 2024, patients will have access to the new LEAs ensured by the NHS, which, for the first time, include different digital health technologies, such as IT and communication aids (including eye communicators and keyboards suitable for people with very serious disabilities), digital technology hearing aids, home automation equipment and control sensors, advanced technology artificial limbs and voice recognition systems.

Healthcare also includes the supply of medicinal products (mostly reimbursed by the NHS) through authorised public or private pharmacies which guarantee full coverage of the entire country, including areas at a geographical disadvantage.

This system of a public nature also leaves private operators with margins of entrepreneurial autonomy.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

To date, there are no specific regulatory schemes that apply to digital health solutions; general laws shall apply, such as those relating to product safety, medical liability, medical devices and intellectual property.

However, the Italian Parliament is working on a proposal of law on digital therapeutics (DTx) presented on 7th June 2023, which defines digital therapies and founds a Committee aimed at monitoring promptly scientific and technological developments of such therapies also for the inclusion in the LEAs.

In any case, the organisation of the Italian NHS (see question 2.1) has seen a new "model" emerging in recent years, which is destined to have a significant impact on the management of healthcare in Italy: the use of new technologies in the delivery methods of patient services.

Healthcare is one of the sectors of public administration that has seen the greatest growth in the use of new technologies, which serves to improve the quality of care and make it more economic, efficient and effective. While waiting for standardised regulations, the Health Authority (primarily the Ministry of Health) has issued specific guidelines, such as for telemedicine ("soft law" is efficient and flexible enough to "rule" fast-evolving sectors).

Furthermore, within the PNRR (see question 1.4), the Ministry of Health is working on specific decrees in order to implement the digital transformation of the NHS, through AI and digital health solutions. One of these decrees (Ministerial Decree dated 30th September 2023) is dedicated to telemedicine projects and rules the acquisition of telemedicine solutions in compliance to the guidelines (approved by the same decree) that identify the clinical areas in order to ensure homogeneity at a national level and efficiency of telemedicine services.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The wide expansion of mobile devices and apps with their software has rapidly turned to tools for medical purposes generating mHealth, which not only includes wellness and lifestyle apps, but also real medical-therapeutic apps.

The rapid development of technology does not go hand-in-hand with regulatory provisions, such that applicable regulatory schemes are derived from specific legislation existing at an EU and even US level in an interpretative manner.

Consumer protection legislation applies for apps in general, which provides for obligations and responsibilities of the various parties involved in the distribution chain (Legislative Decree no. 206/2005, the Consumer Code, recently amended by Legislative Decree no. 26/2023, which also introduced specific rules on online marketplaces), as well as e-commerce legislation, which requires general and pre-contractual disclosures (Legislative Decree no. 70/2003), and the legislation on privacy (EU Regulation no. 2016/679, "GDPR", and the Italian Privacy Code). Where an app falls within the definition of a medical

device, the legislation on medical devices also applies (EU Regulation no. 2017/745, "MDR", and the recent Legislative Decree no. 137/2022, which is an adaptation of the Italian legislation to MDR).

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

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 the 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.

2.5 What are the key 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 healthcare professionals – both the new generations and the already active health workers – an increasing number of universities offer courses on the subject and continuing medical education (CME) 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.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

Software as a medical device is governed by MDR on medical devices (including active implantable medical devices), applicable as of 26th May 2021, and by Regulation EU no. 746/2017 (IVDR, which governs *in vitro* diagnostic medical devices), applicable as of 26th May 2022. Local decrees have been issued to complete the framework: no. 137/2022 (adaptation to MDR); and no. 138/2022 (adaptation to IVDR). Such rules, *inter alia*, recognise the possibility to sell medical devices online (within certain limits).

That said, the first essential step is to ascertain if and when software falls within the definition of a medical device. The assistance of technical experts is advisable as well as careful evaluation of the legal profile: proper qualification will enable correct and effective market access.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

At the time of writing, there are no specific regulations regarding AI/machine learning powered digital health devices or software solutions and their approval for clinical use (a proposal of law on digital therapies is currently being discussed, see question 2.2). When such instruments qualify as medical devices, the relevant regulations apply (see question 2.6). Otherwise, the distinguishing characteristics of each solution will have to be identified in order to establish the relevant regulations.

3 Digital Health Technologies

3.1 What are the core legal or 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). This represented an important clarification for the development of new digital health initiatives. Furthermore, in the context of the remote provision of health services, the Regional Administrative Court considered that, in the absence of a data analysis and processing function for medical purposes (which cannot be found in the mere archiving and classification of the same), the software platform used cannot be qualified as a medical device (Regional Administrative Court of Milan, decision no. 452/2022). These indications are important for the many projects of public administrations aimed at implementing the infrastructures necessary for telemedicine and which also involve private operators.
- **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); 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 app (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 (see question 4.1).
- **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), 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 Machine Learning, 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 machine learning 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. In October 2023, for the first time in Italy, a simultaneous double implantation of prosthesis, aortic and mitral was carried out with a beating heart on a 66-year-old patient, after having first experimented with the operation on a 3D copy of the cardiac organ.
  3D printing can also be used to reproduce biological material for the replacement of human organs and tissues (bioprinting).
  The spread of 3D printing technologies in the healthcare sector certainly has an innovative scope that involves a multitude of corporate and professional entities. It faces many ethical and regulatory challenges, including the correct qualification of the systems in question (namely the applicability of legislation on medical devices), product safety, manufacturer and user responsibility, as well as the processing and protection of data collected by said systems and intellectual property. To date, the legal framework is still fragmented and the application of the rules remains uncertain.
- **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 7th June 2023, see question 2.2).

The working paper also identifies three conditions necessary for DTx to be used by patients:

- authorisation of the national health institution;
- medical prescription; and
- state funding, in order to ensure all patients have the same opportunities for accessibility.

- **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 healthcare professionals 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 are used in the healthcare sector to improve the patient experience of health services.

The main issue related to Big Data Analytics is connected to the criteria of collection, management and analysis of data and the adequacy of the systems of collection and management, that shall ensure the security of data and protect them from any unauthorised access.

Big Data connected to the state of health of patients are very "precious" and should be protected from any irregular access aimed at improper use of such data.

- **Blockchain-based Healthcare Data Sharing Solutions**

Blockchain in healthcare has the main benefit of ensuring data integrity; however, the process to affirm it in the NHS is slow because new technologies that can even overturn the current organisational patterns need time for their study and adaptation.

The main legal issue is to ensure that the systems are compatible with each other, safe and ensure the confidentiality of personal data shared.

- **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 issues for digital platform providers?

The main issue is the liability for illegal content uploaded to digital platforms.

As regards copyright, according to the Italian 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 to consider for use of personal data?

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.

Another critical issue is that of the identification of a legal basis suitable for legitimising the processing of health-related personal data as carried out through digital tools.

The main issues related to data processing carried out through digital technologies are highlighted in the order adopted in 2023 by the Italian Privacy Authority, which imposed a temporary limitation on the processing of Italian users' data by the company managing a chatbot based on AI and machine learning because no legal basis underpinned the massive processing of personal data collected to "train" the algorithms on which the platform relied, no information was provided to users and data subjects whose data were collected and the information made available by the chatbot did not always match factual circumstances, so that inaccurate personal data were processed. Furthermore, no easily accessible tool was implemented to allow data subjects to exercise their right to object to the processing of their personal data as relied upon for the operation of the algorithms used by the chatbot.

4.2 How do such considerations change depending on the nature of the entities involved?

According to the Privacy Code, as amended by Decree Law no. 139/2021, 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 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 7th 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 healthcare professionals, regardless of whether they operate as freelancers or within a public or private healthcare facility.

4.3 Which key regulatory requirements apply?

The main regulatory source is the GDPR, along with national provisions applicable to data processing activities carried out in the context of digital health. With provision no. 55/2019 (see question 4.2), the Italian Privacy Authority established that the relevant processing activities "only in a broad sense, for care, but not strictly necessary" require, "even if carried out by health professionals", a legal basis other than the need to pursue the purposes of care referred to in Art. 9(2)(h), of the GDPR, "to potentially consist of the consent of the data subject or another legal basis". These processing activities can include those connected to medical apps if data (including health data) are collected for purposes other than telemedicine, or if these data are accessed by subjects other than health professionals and not bound by professional secrecy. Data controllers operating in the health sector that perform various particularly complex operations (e.g. healthcare companies) shall submit the information required by the GDPR to the data subject in a progressive manner, providing:

- information to patients in general only as related to processing activities included in providing ordinary health services; and
- information to patients actually involved in additional processing as regards these specific activities (such as the delivery of online medical reports).

With regard to the storage period of personal data, the Italian Privacy Authority refers to sector provisions that provide for the specific retention times of health-related documentation, in addition to more general rules, including Art. 2946 of the Italian Civil Code, which establishes a 10-year term for rights such as those deriving from contractual liability, among others.

4.4 Do the regulations define the scope of 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 What are the key contractual considerations?

If a contract between the data controller and another party involves data processing on behalf of and according to the instructions of the data controller, this party must be considered a data processor. Processing activities carried out by a data processor are governed by a specific contract or other legal act in accordance with EU or Member State law, which contains the requirements provided for in Art. 28 of the GDPR. Given the special nature of tools used by digital health, the data controller must pay attention to the contractual rules carried out by the data processor, as well as the implementation by the latter of suitable technical and organisational measures provided for in Art. 32 *et seq.* of the GDPR, identifying the provider that offers suitable guarantees of compliance with privacy provisions, and in consideration that it could lose direct and effective control over its data by relying on a remote supplier. The data controller may acquire a prior declaration (supported by documents) from the supplier on the measures taken to comply with the GDPR and carry out periodic audits.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

In order to secure comprehensive rights to data, one should consider not so much the jurisdiction as the means used to process data and to provide the information as at Art. 13 and Art. 14 of the GDPR.

When personal data is processed through apps or other digital tools, the information required by the GDPR is not always supplied in an adequate and sufficiently clear manner, partly because of the difficulties involved in making this information available in full and as smart information on these digital tools.

Furthermore, exercise of the rights envisaged by the GDPR must be guaranteed by making it easy for the data subject to forward requests to the data controller.

The data controller must enable the data subject to submit a request without the requirement of any particular formalities (for example, by registered letter, fax, email, etc.) and to this request, the data controller must provide an appropriate response within one month from its receipt (this period can be extended by two months, if necessary).

If the response to an application is not received within the indicated time frame or is not satisfactory, the data subject may contact the judicial authority or the Italian Privacy Authority.

Violation by the data controller of the provisions on the rights of the data subject is subject to administrative pecuniary sanctions of up to 4% of the total annual worldwide turnover of the previous year.

4.7 How are issues with 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*. With particular reference to the issue of discrimination, the Italian Privacy Authority has recently issued a fine amounting to 2.6 million euros against an Italian food delivery company which implemented a treatment of personal data of its employees based on an algorithm, putting in place different violations of the GDPR, also generating discrimination among workers. With this provision, the Italian Authority ordered the company to lay down measures preventing inappropriate and/

or discriminatory applications of the reputational mechanisms based on the feedback from customers and business partners (decision no. 234 of 10th June 2021).

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

On 10th October 2023, the Italian Privacy Authority adopted a document that sets out 10 rules regarding the supply of national health services through AI systems.

These rules take into account the main issues connected to the processing of personal data put in place by AI generative companies:

1) the correct legal basis, which must be identified in legal or regulatory provisions that provide for adequate measures to protect the rights, interests and freedoms of the data subjects;
2) the principles of accountability, privacy by design and privacy by default, which require the data controller to demonstrate compliance with the obligations of the GDPR;
3) the roles of the various subjects involved in the processing of personal data put in place through AI techniques, which must be correctly identified, taking into account the activities actually carried out and in light of the tasks institutionally delegated to each;
4) the principles of knowability, non-exclusivity and algorithmic non-discrimination, which must govern the use of algorithms and AI tools in the execution of tasks of significant public interest;
5) the Data Protection Impact Assessment, which must always precede the processing of personal data carried out through a national centralised system using AI, since it leads to large-scale systematic processing of data of health workers and is therefore included among those at "high risk";
6) the quality of data, which must be ensured through specific measures aimed at concretely guaranteeing the accuracy and updating of the data;
7) the integrity and confidentiality of data, which must be protected by adequate measures to mitigate the risks deriving from the use of machine learning techniques;
8) transparency and correctness in decision-making processes based on automated processing, which constitute one of the fundamental pillars underlying the development and use of AI systems, in light of the risks, including discriminatory ones, that may derive from the use of such instruments;
9) human supervision (and, in particular, of healthcare professionals), which must remain central in the algorithm training phase, without entirely leaving the decision to the machines; and
10) dignity and personal identity, respect for which must always be guaranteed, excluding choices that, although apparently lawful and materially possible, may produce discriminatory effects, in particular, towards vulnerable subjects (e.g. minors, elderly and sick persons).

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

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.

5.2 How do such considerations change depending on the nature of the entities involved?

Data-sharing operations require more caution for health-related data processing as performed by healthcare professionals. 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

National provisions other than those contained in the GDPR do not exist, which, in this regard, constitutes the main regulatory reference. For the transfers of data outside the EU, in addition to the intention to carry out the transfer, the data controller must also indicate the condition of lawfulness of such transfer in the disclosure among those expressly provided for in Art. 44 *et seq.* of the GDPR. Such transfers are only allowed to countries that guarantee the same level of protection of personal data as provided for by legislation in Member States and, only residually, with the express consent of the data subject.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

An initiative recently adopted by the Ministry of Health concerns the "electronic health records 2.0" ruled by Ministerial Decree of 7th September 2023 (see question 1.2), 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.

5.5 What are the key issues 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.

6 Intellectual Property

6.1 What is the scope of patent protection for digital health technologies?

At the time of writing, there are no specific laws governing patent protection for digital technologies: therefore, the rules of

Legislative Decree no. 30/2015 (Industrial Property Code, IPC) governing patent protection shall apply.

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 What is the scope of copyright protection for digital health technologies?

At the time of writing, there are no specific laws governing copyright protection for digital technologies: therefore, we shall refer to the protection offered by copyright law, which in Italy is Law no. 633/1941, which gives the creator the exclusive right to use his/her work. This right 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 What is the scope of trade secret protection for digital health technologies?

Since in our jurisdiction there are currently no specific rules governing trade secret protection for digital health technologies, the laws on the protection of confidential know-how shall apply.

In Italy, the 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 What is 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 (SIAE) in order to obtain proof of authorship. Copyright must be governed in any software contract (development, licence, 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 Software as a Medical Device (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 are the core rules or laws related to government-funded inventions in your jurisdiction?

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.

7 Commercial Agreements

7.1 What 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 varying legal nature, depending on the scope and purpose pursued, such as: consortia; contractual joint ventures; 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 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 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 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 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 is the role of machine learning in digital health?

AI is a matter of great interest in Italy and also includes the Public Administration. On 24th November 2021, Italy adopted the Strategic Program for AI 2022–2024; the result of the joint work of the Ministry of University and Research, the Ministry of Economic Development and the Minister for Technological Innovation and Digital Transition. The Program outlines strategic policies to enhance the AI system in Italy, through the creation and enhancement of skills, research, development programs and AI applications, also in the healthcare sector.

This Program should soon be revised, as announced by the Government, in order to adequate it to emerging technological trends, such as generative AI (chatbots such as ChatGPT).

Digital healthcare is affected by the use of machine learning systems, which help physicians improve diagnoses, predict the spread of disease and customise treatments. AI allows the remote monitoring of patients' health conditions (telehealth), optimisation of the management of administrative issues and plays a fundamental role in "precision medicine", an emerging approach that takes individual variability into account in order to develop custom treatments. Through the use of smart machines that analyse a huge amount of data, it is not only possible to make early diagnoses and identify a life-saving therapy faster than traditional methods, but also allow reliable predictive medicine-based approaches. This will allow the research activity to be more effectively focused, such as the potential optimal identification of patients enrolled in clinical studies. Robotics is making a valuable contribution in operating rooms (such as tools that allow surgical intervention in a more

precise and less invasive manner through the supply of maps of the parts of the body, prepared on the basis of AI algorithms, thus allowing a shorter hospital stay for patients and economic savings for healthcare facilities).

8.2 How is training data licensed?

The stipulation of a specific contract is necessary in order to obtain the training data of third parties, in which the scope of the agreement must be outlined, specifying if the ownership of the data is transferred or exclusive or non-exclusive use is granted (i.e. licence), the duration of the agreement, any right of withdrawal, rights of termination, privacy profiles that may be relevant, as well as the liability of each party. The contents of the agreement varies according to the actual needs of contractors and is based on the principle of autonomy of the parties (Art. 1322 of the Italian Civil Code), without prejudice to the principle of compliance to the law and the limitation of acts contrary to it.

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

Italian legislation poses some obstacles to the recognition of intellectual property rights for that created by machine learning 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 considerations apply to licensing data for use in machine learning?

One of the main issues is the identification of the criteria for the adequate financial valorisation of intangible resources, such as machine learning 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.

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 (machine learning), 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 generative AI in the provisioning of digital health solutions?

Liability risks posed by the use of generative AI can be minimised by:

1) setting clear objectives;
2) ensuring data quality and integrity by establishing data governance practices and maintaining data privacy in compliance with relevant regulations;
3) encouraging continuous learning and upskilling within the organisation in order to effectively drive innovation;
4) considering ethical concerns associated with AI, such as bias and discrimination, by ensuring fairness, transparency and accountability;
5) implementing policies and guidelines in order to set out clear rules governing the initiative and the activities to be carried out; and

6) assessing the contents of the agreements between the parties involved and defining clearly the respective roles and responsibilities.

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 Electronic Health Record (see question 1.2), 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 healthcare professionals 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 healthcare professionals 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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Italian law includes provisions guaranteeing the free supply of aids, equipment and prostheses for disabled patients (for example, made-to-measure ocular prostheses, acoustic equipment, corsets, wheelchairs, walking frames, incontinence catheters, etc.).

A step forward has been made with the new LEAs, which provide for the reimbursement of different digital health solutions (see question 2.1).

The need is felt to identify which access and reimbursement models are usable and sustainable for the new digital tools, also because, besides the close attention paid to the creation of regulatory and clinical development procedures, consideration should be given to the fact that the generation of significant revenue flows is, and will be, one of the main challenges in this sector on all markets.

In this context, the orientation also among private insurers is to identify bespoke insurance packages that enable the user to choose personal prevention, diagnosis, treatment and convalescence services, which facilitate access to digital health solutions.

10.7 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 in1994. 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 gained 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. She is co-author of *e-patient e social media, Il Pensiero Scientifico Editore*, 2016.
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 2 885 561
Email: sonia.selletti@studiolegaleastolfi.it
LinkedIn: www.linkedin.com/in/sonia-selletti-b25953164

Giulia Gregori graduated in law from the University of Pavia in 2011. She has been a member of the Milan Bar Association since 2019.
Giulia has been working with Astolfi e Associati since 2013, where she mainly works in the field of pharmaceutical and healthcare law. She has also gained experience in data protection law.
She is an Editorial Assistant and 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 2 885 561
Email: giulia.gregori@studiolegaleastolfi.it
LinkedIn: www.linkedin.com/in/giulia-gregori-04174b58

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 2 885 561
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 advise 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 technologies 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 are the core legal issues in digital health for your jurisdiction?

The core legal issue for a digital health product is the applicability of the regulations under the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices ("PMD Act") to such product as a medical device, which may impose a greater burden on the provider. Medical devices authorised under the PMD Act are also usually subject to reimbursement under the National Health Insurance ("NHI") system, which makes it easier to disseminate the product in medical settings.

The core legal issue for a digital health service is whether such service constitutes a medical practice. In principle, medical services can only be provided by physicians or other qualified health care professionals ("HCPs"). In addition, there are certain restrictions on how and where HCPs may provide medical services.

The core legal issue common to both digital health products and services is the regulation of personal information and data. While medical and health-related information would be subject to stricter regulations as sensitive information, the utilisation of personal information and data is essential for the digital health field, and law amendments and special laws were enacted to promote such utilisation.

1.4 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.

1.5 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.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

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 Ministry of Health, Labour and Welfare ("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 2.6.

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 shall be met.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The application of the regulations under the Act on the Protection of Personal Information ("APPI") is a key issue. For the details of the regulations, please see the responses to questions 4.1 through 5.5.

In addition, 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 regulatory schemes apply to consumer healthcare devices or software in particular?

Consumer healthcare devices or software that fall under the category of medical devices are subject to the regulations under the PMD Act. Please see the responses to questions 2.1 and 2.6.

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 Act Against Unjustifiable Premiums and Misleading Representations ("AUPMR").

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The principal regulatory authorities for the PMD Act are the 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 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 AUPMR is the Consumer Affairs Agency.

2.5 What are the key 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.

2.6 What regulations 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 GCP must be observed. Recently, the MHLW published evaluation indices for the safety and efficacy of SaMD that induces behavioural changes for disease treatment.

2.7 What regulations apply to artificial intelligence/machine learning 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. In addition, an expert committee at the PMDA is currently discussing methods for the examination of adaptive AI devices that are intended to autonomously change their performance after being marketed.

3 Digital Health Technologies

3.1 What are the core legal or 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 response to question 2.6.
- **Clinical Decision Support Software**
  Please see the responses to questions 2.6 and 2.7.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  Please see the response to question 2.7.
- **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 response to question 2.6.
- **Digital Diagnostics**
  Please see the response to question 2.6.

- **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 issues for digital platform providers?

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 to consider for use of personal data?

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 do such considerations change depending on the nature of the entities 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).

4.3 Which key regulatory requirements apply?

Business operators that handle personal information (including medical institutions and academic research institutions) must take safety control measures, and they are required to supervise their employees and contractors.

Special obligations are imposed on business operators that handle Anonymously Processed Information or Pseudonymously Processed Information, such as the prohibition of acts that re-identify the principal.

4.4 Do the regulations define the scope of data use?

Apart from certain exceptions stipulated in the APPI, the use of personal information 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 What are the key contractual considerations?

It is advisable to confirm that (i) the provided personal data has been acquired appropriately, and (ii) the provision thereof has been authorised properly through the necessary procedures (e.g., consent of the principal) under the APPI and Ethical Guidelines, as applicable, and to request warranties from the counterparty, as necessary.

When outsourcing the handling of personal information, it is advisable to stipulate the security control measures to be taken by the contractor, as well as the reporting obligation and audit provisions to confirm the compliance status.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

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. 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.

4.7 How are issues with 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.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

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. In addition, the government is now preparing guidelines for businesses regarding the appropriate uses of generative AI.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

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. On the other hand, 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 do such considerations change depending on the nature of the entities 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Apart from certain exceptions stipulated in the APPI, the provision of personal data without the consent of the principal is not permitted. 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.

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.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

Under the APPI, the provision of medical information to a third party 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 provision 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 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 What is 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". 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 What is the scope of copyright protection for digital health technologies?

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 What is the scope of trade secret protection for digital health technologies?

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 What is 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.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

With respect to certain intellectual property rights that are associated with the results of government-contracted research and development ("R&D"), 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.

7 Commercial Agreements

7.1 What 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 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 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 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 is the role of machine learning in digital health?

Machine learning is playing a role in improving the accuracy of diagnosis using images such as CT and MRI. Machine learning is also expected to improve the accuracy of disease diagnosis by learning from past electric medical records, and to identify mental illness by performing natural language processing of patients' statements. In addition, machine learning is expected to play a role to efficiently perform a vast amount of analysis and work in pharmaceutical R&D and the genome analysis area.

8.2 How is training data licensed?

Training data may be protected under the Copyright Act of Japan. The Copyright Act provides that a database that involves creativity, by reason of the selection or systematic construction of information contained therein, is protected as a work. Training data may fall under a database and its selection of data or systematic organisation of data may involve creativity. In such situation, the training data can be treated and licensed as a copyrighted work. Even when training data is not treated as a copyrighted work, there is a possibility that training data is treated as "Shared Data with Limited Access" under the UCPA. Wrongful acquisition, use and disclosure of "Shared Data with Limited Access" can be treated as "Unfair Competition" under the UCPA, and the person who wrongfully acquired, used or disclosed the data may be enjoined to do so and/or be held liable for the damages under the UCPA. "Shared Data with Limited Access" is defined as "technical or business information that is accumulated to a significant extent and is managed by electronic or magnetic means as information to be provided to specific persons on a regular basis (excluding information that is kept secret)". In the case where the training data falls under this definition, the training data can be licensed as "Shared Data with Limited Access". Even when training data does not fall under a copyrighted work or "Shared Data with Limited Access", some businesses still enter into a "licence agreement" on training data. However, as use of such training data without authorisation does not cause any liability, such "licence agreement" is just a declaration that the "licensor" will not object to the use of the training data by the "licensee".

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

If there is no active human involvement in the software development at all, no intellectual property 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 considerations apply to licensing data for use in machine learning?

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.

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 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.

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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Digital health solutions may be reimbursed under the NHI. 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 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 order to accelerate the dissemination of medical device programs, a new regulatory approval framework is being introduced for certain types of medical device programs that are not high-risk. In such framework, (i) first-stage approval may be granted for medical device programs to the extent that evaluation data confirms the probability of a certain level of efficacy, (ii) further evaluation data on efficacy and safety will be collected from actual uses in clinical settings, and (iii) second-stage approval may be granted when the evaluation data collected in clinical settings demonstrates a clinically meaningful degree of efficacy.

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. The firm's 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. 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. In addition to our capabilities spanning key commercial areas, the firm is known for path-breaking domestic and cross-border risk management/corporate governance cases and large-scale corporate reorganisations. The over 500 lawyers of the firm work together in customised teams to provide clients with the expertise and experience specifically required for each client matter.
(*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 technologies 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 early 2000s. In recent years, software as a medical device (SaMD) products have become a key emerging part of the digital health industry, and the Ministry of Food and Drug Safety (MFDS) established a guideline for the regulatory approval of digital health products in August 2020.

1.3 What are the core legal issues in digital health for your jurisdiction?

First, under the Medical Service Act, which requires medical services to be provided by healthcare professionals at a medical institution, it can be difficult to adopt and implement new digital health technologies in a swift and broad manner (e.g., limited allowance of telemedicine).

Second, due to Korea's universal national health insurance system, any new digital health technology or product is required to be evaluated and included in the national health insurance system in order for it to be widely used in the healthcare service market.

Third, the Personal Information Protection Act of Korea imposes very strict restrictions on the collection and use of personal data, and these restrictions can present substantial challenges in developing and using new digital health technologies and products.

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

According to the data announced by the Ministry of Trade, Industry and Energy, the revenue of the digital health industry in Korea in 2020 was around KRW 1,354 billion (USD 1 ≒ KRW 1,200). It is understood that the Korean digital health industry has grown by at least 10% annually since then.

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

No public data is available.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

A bill to promote and provide a framework for digital health was submitted to the National Assembly in 2022, but has not yet been enacted. As such, currently, there is no general statutory regulation governing digital health in Korea.

The Medical Devices Act is the current statutory regulation that serves as the central regulatory scheme for digital health. If a digital health product falls within the scope of medical device, prior approval or certification by the MFDS is required for market entry. If a product is classified as a wellness product, no prior approval or certification is required. In this connection, the MFDS has established guidelines for digital health product approval, mobile medical app and wellness products, etc.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Certain new digital heath technologies are required to undergo the new health technology assessment (nHTA) pursuant to the Medical Service Act prior to use at a medical site. Further, telemedicine is restricted under the Medical Service Act.

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 heath product or service to be eligible for reimbursement under the National Health Insurance Act for commercial success in the market.

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.

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.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

As explained in question 2.1, the Medical Devices Act and the MFDS guidelines provide the basic regulatory scheme. Having said that, if a digital health product falls within the scope of medical device, prior approval or certification by the MFDS is required for market entry. However, if such product is classified as a wellness product, no prior approval or certification is required.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

Regarding medical device qualification or requirements, the MFDS is the principal regulatory authority under the Medical Devices Services Act. If a particular digital health service relates to telemedicine or another type of medical service, or if the eligibility for national health insurance reimbursement becomes an issue, the Ministry of Health and Welfare (MOHW) is the authority in charge. Further, the Personal Information Protection Commission will have the authority if personal data protection issues are concerned.

2.5 What are the key areas of enforcement when it comes to digital health?

Since it is more likely that digital health technologies or products may fall within the purview of medical device, the MFDS will be the primary law enforcement authority relevant for Korea. The MOHW will be involved if the digital heath technology is required to undergo the nHTA prior to be used by healthcare professionals or the eligibility of the national health insurance reimbursement is concerned.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

First, an SaMD should be approved or certified by the MFDS. Further, if an SaMD is classified as new medical technology under the Medical Service Act, such SaMD will be subject to the nHTA, as explained above. In addition, as Korea adopts a universal national health insurance system without allowing patients or medical service providers to opt-out, the SaMD may be required to be reviewed for eligibility for the national health insurance reimbursement.

2.7 What regulations apply to artificial intelligence/ machine learning powered digital health devices or software solutions and their approval for clinical use?

The Medical Devices Act and the MFDS's guidelines based thereon will apply.

3 Digital Health Technologies

3.1 What are the core legal or 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 Services 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 the 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**
  Notable SaMD products are introduced in Korea, and it is understood that significant investments continue to be made for SaMD development. According to the MFDS data, 49 SaMD products were newly approved in 2022 while only six products were approved in 2018. As SaMD products are rapidly introduced into the market, the Health Insurance Review Assessment & Assessment Service, a government agency which oversees the National Health Insurance eligibility of drugs and medical devices under the

National Health Insurance Act, established the Guideline on the National Health Insurance Enrollment of SaMD.

- **Clinical Decision Support Software**
  The majority of SaMD products approved by the MFDS may be classified as clinical decision support software. According to the MFDS data, 31 SaMD products were classified as clinical decision support software among 49 SaMD products that were approved in 2022.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  Artificial Intelligence (AI)/Machine Learning 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**
  Among the 49 SaMD products approved in Korea, 17 products are digital therapeutics. The diseases for which these digital therapeutics are intended to be used include ADHD, mild cognitive impairment, developmental disorder, alleviation of addiction, as well as insomnia.
- **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. However, due to the fact that the adoption of EMRs was based on the individual policies of medical institutions rather than a national project, there are issues with compatibility of EMRs among different medical institutions. To address this, the government has been making efforts to enhance the quality and inter-compatibility of EMRs by implementing an EMR certification system since 2020.
- **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 issues for digital platform providers?

Digital platform providers face many challenges under the current regulatory scheme:

(1) "Physician-to-patient" telemedicine and online dispensing of drugs are strictly restricted under the Medical Service Act and the Pharmaceutical Affairs Act.

(2) It is difficult for a digital platform provider to collect and manage patients' data from diverse medical institutions so as to provide tailored services to each patient under the data privacy laws.

(3) It is generally accepted that Korean medical institutions are highly digitalised; however, due to the lack of a standardised system, there are technical difficulties in achieving system connection among medical institutions.

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

The Personal Information Protection Act regulates the collection and processing of (i) "general" personal information, (ii) "sensitive information" which is deemed to present clear risks of invading the data subject's privacy – including information relating to health or sex life (this includes the subject's historic and current medical history, physical/mental disability and sexual orientation, but excludes information on blood type), genetic information, bio-identifying information (information relating to a person's physical, physiological or behavioural characteristics collected through certain technological methods for the purpose of identifying/certifying a particular individual), and (iii) personal identifying information such as resident registration number, passport number and foreigner registration number. "General" personal information can be processed in the following circumstances in principle: (i) upon the consent of the data subject; (ii) if particularly required by law or if necessary for the purposes of complying with the law; or (iii) if necessary for the purpose of executing and performing a contract with the data subject. In the case of "sensitive information", processing is allowed only if (i) consent for the use of "sensitive information" separate from consent for the use of "general" personal information is obtained from the data subject, or (ii) the processing of the information is specifically required or permitted by law. If the data subject is less than 14 years of age, consent by such data subject's legal representative is required. Finally, controllers may process pseudonymised information, including use, provision and combination, without the consent of the data subject for the purposes of statistical compilation, scientific research, public interest record preservation, etc.

4.2 How do such considerations change depending on the nature of the entities involved?

No change is recognised, in principle.

4.3 Which key regulatory requirements apply?

The following main duties apply with respect to the processing of personal data:

- Duty to implement safety measures for the protection of personal data: protection measures in accordance with

the "Personal Information Safety Measure Standards" must be implemented to prevent the loss, theft, leaking, forgery, modification or damage of personal information. Additionally, bio-identifying information (i.e., information relating to a person's physical, physiological or behavioural characteristics collected through certain technological methods for the purpose of identifying/certifying a particular individual) must be encrypted when transmitting or storing.

- Duty to prepare and disclose a privacy policy: a privacy policy including legally mandated matters must be disclosed through methods such as uploading on the processors homepage.
- Duty to designate a personal data protection officer: a personal information protection officer must be appointed to comprehensively take charge of personal information processing.
- Duty to notify and report personal data leakage.

4.4 Do the regulations define the scope of data use?

The Personal Information Protection Act stipulates as its basic principle that only minimal personal information necessary for the relevant purpose should be legally collected, and that the information should not be used for any purpose other than the purpose it was collected for.

When obtaining the data subject's consent, the "purpose of collection and use of the personal information" must be disclosed to the data subject, and the Personal Information Protection Act provides that the collected information cannot be used for any purpose other than the purpose disclosed to the data subject.

4.5 What are the key contractual considerations?

As explained in question 4.1 above, the Personal Information Protection Act requires a data subject's consent for the processing of personal information, unless such processing is specifically permitted or required by law. As far as health data or medical data is concerned, the data subject's informed consent is required.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

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.

4.7 How are issues with 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.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

As there are no specific laws or regulations uniquely applicable to data usage by generative AI companies, the current Personal Information Protection Act is applied uniformly. According to the Personal Information Protection Commission, for the collection and use of personal information for AI development, obtaining the consent of the data subject is generally required. However, if the AI development or service meets the criteria of being (i) reasonably related to the original collection purpose, (ii) predictable, (iii) does not unfairly infringe on the interests of the data subject, and (iv) includes necessary measures to ensure safety, then the use of previously collected personal information is possible without additional consent.

Additionally, in cases where publicly available information is collected or used, personal information can be collected and used without the data subject's consent (a) within the objectively inferred scope where the data subject's consent is deemed to exist, or (b) when the legitimate interests of a generative AI company clearly take precedence over the rights of the data subject.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

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 do such considerations change depending on the nature of the entities involved?

No change is recognised, in principle.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The same rules apply as explained in question 5.1 above.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

It is happening on two fronts. The first relates to Personal Health Records. Individually collected health information from various medical institutions and public agencies (e.g., Korea Disease Control and Prevention Agency, Health Insurance Review Assessment & Assessment Service, National Health Insurance Service) will be subject to active integration and management by individuals (i.e., data subjects), and furthermore, the data subjects will have the right to request the relevant institutions holding this information to provide it to third parties according to the individual's request. Based on the Medical Service Act, the MOHW has been implementing this project through its "My Healthway Platform Project" policy since 2021.

The other front involves the sharing of anonymised medical information held by medical institutions with third parties.

This became possible in 2020 following the amendment of the Personal Information Protection Act. However, unlimited data sharing is not permitted, and even when anonymised, sharing is only allowed for the purposes of statistical compilation, scientific research and record preservation for public interest purposes.

5.5 What are the key issues 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. In response to these societal changes, the government is formulating and implementing policies as explained in question 5.4 above.

6 Intellectual Property

6.1 What is 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 What is 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 What is 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 by the holder of said information, and trade secret was defined as being information "maintained in confidence through reasonable efforts" prior to the amendment on January 8, 2019 (effective July 9, 2019), but has since been amended by deleting the phrase "through reasonable efforts", and therefore, represents information "maintained 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 What is 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 is that AI cannot be recognised as the inventor for the purpose of obtaining

a patent. For reference, in 2022, the Korean Intellectual Property Office (KIPO) rendered a decision of invalidation for a patent application that listed AI as the inventor. Additionally, on June 30, 2023, the Seoul Administrative Court upheld the validity of the KIPO decision. The case is currently being reviewed by the Seoul High Court.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

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, 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.

7 Commercial Agreements

7.1 What 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 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 considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

As explained in question 5.4 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 considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Currently, there are no specific regulations in place. However, given the government's interest, there is the possibility of new regulations being developed in the near future.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Medical services by AI, especially machine learning, are rapidly moving away from post-treatment centred on analogue devices and towards preventive healthcare based on intelligent healthcare solutions by combining ICT. Preventive healthcare refers to analysing healthcare big data based on data science and intelligent solutions in order to take pre-emptive measures to prevent diseases from occurring.

Machine learning is simply a process to produce a model as a result of training using statistical techniques on a given data. Large-scale data preparation is important for constructing a more accurate prediction model, although it is necessary to prepare a complete, accurate and consistent dataset by properly processing raw data through pre-processing.

Such machine learning can be used for digital healthcare, real-time monitoring of patients, disease prediction and diagnosis, which tracks the causes of abnormal conditions for individuals in digital health and provides personalised health care guides.

8.2 How is training data licensed?

The right to use a training dataset is essentially regulated by contract between the parties giving and receiving the data.

Generally, data can be protected with intellectual property rights (e.g., copyright, trade secrets) if certain requirements are met. If a licence is granted for data protected with intellectual property rights (e.g., copyright, trade secrets), certain restrictions on its use may apply not only from the licence agreement, but also from the relevant intellectual property laws.

For training datasets, the dataset itself may be protected as a copyright if individual data is protected as copyright, or if the dataset meets the requirements of a database under the Korean Copyright Act (a compilation that systematically arranges or organises materials that individually allows access to or search of such materials).

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning 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.

Differing views exist regarding whether or not the creation of AI, such as machine learning, will be protected with intellectual property rights, with those in favour stating that it will promote the development of cultural industries, and those against it voicing concerns of monopoly.

There are conflicting views on how to attribute the creation of AI to individuals between those that view that it should be attributed to (i) the developer of the AI, (ii) the owner of the AI, or (iii) the AI itself. Among these, the view that intellectual property rights should be attributed to the AI itself can be understood to be in anticipation of the emergence of strong AI with self-awareness that can conduct work without direct orders from humans.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Various commercial considerations should be taken into account when licensing data for machine learning. In such cases, machine learning 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 machine learning using the data, and the right to sublicense should all be considered.

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 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.

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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with 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 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

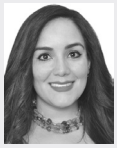
Sungil Bang is a partner in the IP Practice Group and the Healthcare/Life Sciences Team of Lee & Ko. His practice at Lee & Ko focuses on legal issues in the areas of healthcare and intellectual property, with a special emphasis on medical device, pharmaceuticals, food and cosmetics. In addition to his 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.bank@leeko.com
LinkedIn: www.linkedin.com/in/sungil-bang-973356240

Mexico


Christian López Silva


Carla Calderón


Marina Hurtado Cruz


Daniel Villanueva Plasencia

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 stand-alone "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, "*expands 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 technologies in your jurisdiction?

Telemedicine, electronic prescription, medical apps, online platforms for e-commerce, online communities of physicians or patients, different digital platforms for health services, electronic health records and online pharmacies.

1.3 What are the core legal issues in digital health for your jurisdiction?

As the existing legal framework was designed to address a physical world (including products, services and establishments) and not digital or virtual environments, the applicability of old rules to new situations is far from clear, generating great legal uncertainty, which turns into commercial uncertainty and risk.

Some adopt the position that existing regulation can be made applicable through standard legal interpretation. Others, however, argue that the new situations are in fact not regulated.

For us, the two core legal fields in relation to digital health are announced in the term itself and therefore are: (i) the regulation of information technologies, which encompasses privacy; and (ii) the regulation of health.

At the same time, considering that neither of those regulatory fields are harmonised internationally, but that the nature of the operations of the digital health industry are typically of a cross-boundary nature, this adds a further layer of legal complexity.

Now, digital health applications generate an important amount of health data, which then becomes a strong currency driving further innovation. Therefore, legal issues such as ownership, access, processing, use and commercialisation of data, in different contexts and multiple platforms, become crucial factors.

There are, of course, other legal implications that are also very important to consider, such as intellectual property, tax, product liability and contracts, which can also impact the development of a market of digital health, although the regulatory aspect is fundamental.

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

According to Statista, the revenue in the digital health market in Mexico is set to reach US$1.93 billion and is expected to show an annual growth rate in the next five years of 7.65%.

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

Yana, Previta, Eden, Vitau and Prixz.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

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 medical devices ("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.

More recently, a new sub-category of MD was added as a Technical Standard. On December 21, 2021, NOM-241-SSA1-2021 on Good Manufacturing Practices for Medical Devices ("NOM-241") was issued, which introduces the notion of Software as a Medical Device ("SaMD").

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.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

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 Mexican Data Protection Authority (the "INAI") 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. In addition, it should be considered that other laws such as the federal consumer protection law 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.

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 same 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 has publicly recommended their implementation. 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 regulatory schemes apply to consumer healthcare devices or software in particular?

Our local health regulatory framework does not contain a regulatory category for "consumer products" or "consumer devices". This is rather a commercial term that can refer to a variety of regulatory categories, including (i) medicines, particularly over-the-counter drugs, (ii) MDs, (iii) cosmetics, (iv) dietary supplements, and (v) food and beverages.

In the context of digital health, as mentioned before, 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.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The Federal Commission for the Protection against Sanitary Risks ("COFEPRIS") is the federal authority in charge of health regulation, which includes drugs, MDs and healthcare services.

The 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.

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 in the protection and enforcement of IP rights.

2.5 What are the key areas of enforcement when it comes to digital health?

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 practice 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 is still a highly active regulator as is shown in its latest report for 2022, with 119 recorded proceedings and having concluded 78 of them, which derived in total MX$60 million in fines (approx. US$1,226,333.31). The INAI also began 249 Right Requests to confirm compliance with the law, from which 144 relate to the access right, five to rectification, 102 to cancellation and 35 to opposition. In addition, the INAI has been encouraging companies with respect to the processing of biometric data and has 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.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

A technical standard for MDs entered into force, NOM-241 – Good Manufacturing Practices of Medical Devices. NOM-241 incorporated as a sub-category the notion of SaMD.

The second most-relevant regulatory instrument is the Supplement on Medical Devices of the Pharmacopeia, which was amended in 2023 to introduce a full Appendix X on SaMD.

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 of 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.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

In 2018, Mexico issued an Artificial Intelligence ("AI") Strategy to create a framework for the development of an AI, becoming the 10th country to formalise an approach to AI. However, the current Administration of President Andrés Manuel López Obrador decided not to carry on with this strategy. Therefore, it is unlikely we will see any policy development on AI soon. Nevertheless, the 2023 two draft bills to regulate AI are being discussed in the Chamber of Commons and the Chamber of Senators.

Since Mexico does not have a particular regulation addressing AI or machine learning, their healthcare applications are regulated only by the health regulatory framework. Depending on the application and business model of certain AI or machine learning, one or more regulatory schemes would be triggered, including the regulation for the processing of personal data through automated decision-making technologies.

The INAI has 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/machine learning 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/machine learning 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.

3 Digital Health Technologies

3.1 What are the core legal or 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 2.1 and 2.6. 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 issues for digital platform providers?

From a health regulatory perspective, we often see that digital platform providers see the model of marketplaces to avoid regulatory obligations, thinking that it would be the product or service provider who would bear alone the responsibility. We typically suggest for them instead to first understand what the regulatory implications of their business model are, and second, identify more clearly in the agreements that will need to be executed with relevant parties in the model, what the obligations are and how compliance will be audited.

Also, digital platform providers frequently need to understand that some digital versions of business models, even if they are not regulated specifically, are likely to be caught by the regulation that was built for a physical version of a similar business model. Thus, for example, the rules for brick-and-mortar pharmacies or medical consulting rooms typically apply to online pharmacies or telemedicine.

From an information technologies perspective, it is key for digital platform providers to comply with the requirements set forth by the corresponding data protection legal framework, depending on whether the data controller is a private or public entity, which include the delivery of a privacy notice and obtaining consent from the data subjects for the processing of their personal and particularly their sensitive personal data, as well as their consent for transferring the data to any third party that is not a data processor.

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

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) to deliver and comply 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.

4.2 How do such considerations change depending on the nature of the entities 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.

4.3 Which key regulatory requirements apply?

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.

4.4 Do the regulations define the scope of 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 What are the key contractual considerations?

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 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Under the Mexican Constitution and the Law, data subjects have the constitutional right to request access, rectification, cancellation, opposition and revocation of their personal data. After having received a request, the data controller has a particular period to analyse the request and provide confirmation; after having confirmed, there is another period for complying with the same. This must be detailed in the privacy notice that must be delivered to data subjects prior to the processing of their personal data.

It should be considered that in Mexico, data controllers may develop and implement self-regulation schemes to ensure compliance with privacy laws and to evidence proven accountability. Self-regulation schemes are a broad term which encompass Privacy Management Compliance Programs ("Privacy Programs"), Binding Corporate Rules ("BCRs") and compliance seals, among other self-regulation institutions. Data controllers who manage to have their privacy programs certified by the INAI are afforded regulatory benefits, such as lesser fines in case of infringements to the Law.

4.7 How are issues with 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.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

To recall, there is no dedicated regulation for digital health, much less for AI. Consequently, the general regulatory framework for medical products and services is largely applicable. Lacking a specific regulatory category for AI digital health applications, these would likely be captured by the concept of SaMD and face the same challenges regarding blurred frontiers between product categories. Nonetheless, companies must consider the regulation for the processing of personal data through automated decision-making technologies which may be applicable to some extent depending on the technology that is used.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Please see the answer to question 4.5.

5.2 How do such considerations change depending on the nature of the entities 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Please see the answer to question 4.5.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining, and 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 entered into force in 2012, we are still waiting to see implementation on a large scale.

5.5 What are the key issues 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 What is 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 What is 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 What is the scope of trade secret protection for digital health technologies?

The FLPIP defines trade secret as (Art. 163) 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 previous paragraphs, as well as a definition for misappropriation and misappropriation infringement and offenses. 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 What is 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 Copyrights. 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 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.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

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.

7 Commercial Agreements

7.1 What 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 intetllectual 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 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 considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

When collecting health data for machine learning 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 5.5.

7.4 What 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 is the role of machine learning in digital health?

Machine learning is at the heart of AI. However, its role in digital health, from a health regulatory perspective, represents important challenges. The problem is that, continuously using performance data generated by users to improve a product, quite closely resembles what constitutes "health-related research conducted in relation to a product", which is subject to both ethical and regulatory approval, in relation to a research protocol. However, having to obtain such approval would significantly inhibit the process. If the data were obtained indirectly from data repositories and not directly from the users, one may argue that a privacy consent would suffice. Fortunately, so far, the new regulation that was recently introduced (Appendix X on SaMD to the Supplement on Medical Devices of the Pharmacopeia), by replicating large portions of the IMDRF documents, introduced a positive stance regarding the continuous learning capabilities of AI. Appendix X now states, for example: "SaMD manufacturers are encouraged to leverage SaMD's technology capability to capture real world performance data to understand user interactions with the SaMD, and conduct ongoing monitoring of analytical and technical performance to support future intended uses." We will have to see how the local health regulator interprets and implements the now complete regulatory framework.

At the same time, attention must be paid to the fact that, from a health regulatory perspective, if the product improvement is such that (i) it creates a new functionality of the device, then it requires a new product approval, or (ii) it results in a significant software update, then a modification of the original product approval is required.

8.2 How is training data licensed?

It has not been discussed yet in Mexico whether health data should be licensed for AI training. At the same time, databases can be protected under copyright law, thus their licensing would have to abide to the copyright regime.

In addition, from a data protection perspective, one of the self-assessment questions to be asked, in connection with the Recommendations For The Processing Of Personal Data Arising From The Use Of Artificial Intelligence, is whether staff developing the AI product or service critically assess the quality, nature, source and quantity of personal data used, reducing unnecessary, redundant or marginal data during the development and training phases, and then monitor the accuracy of the model as it is fed with new data.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning 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 considerations apply to licensing data for use in machine learning?

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.

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 13 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? 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 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, as described in question 10.1.

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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with 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 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 that (i) contain a sensor or transductor to measure physiological parameters, and (ii) digital health apps installed in a smartwatch. This is consistent with the trend

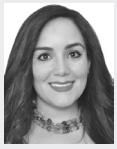
of regulation of digital health applications with a bottom-top approach which hastens the regulation process as it is done at an administrative, rather than at a parliamentary level.

There have been multiple draft law initiatives submitted in the Federal Congress in the last two 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 and AI. 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, 2024 is an election year for Mexico's new President, therefore any bills approved will be highly politicised and it is unlikely any key regulations regarding digital health will pass in 2024.

Christian López Silva has more than 20 years of experience in the regulation of life sciences, pharmaceutical law and biotechnology matters, having worked in the private and public sectors and at the national and international level. For several consecutive years, Christian has led the rankings for Life Sciences in Mexico (*Chambers Latin America*, *The Legal 500 Latin America*). He holds a law degree from ITAM in Mexico and both a Master's degree in Biotech Law and Ethics and a Ph.D. in International Regulation of Life Sciences from the University of Sheffield in the United Kingdom.

Baker McKenzie
Edificio Virreyes, Pedregal 24, 12th Floor
Lomas Virreyes/Col. Molino del Rey
Mexico City, 11040
Mexico

Tel: +52 55 5351 4141
Email: christian.lopez-silva@bakermckenzie.com
LinkedIn: www.linkedin.com/in/xtianlopezsilva



Carla Calderón is an experienced attorney in the regulation of life sciences, pharmaceutical law and biotechnology matters. She regularly advises on matters in the intersection of regulatory, data privacy and intellectual property for the manufacturing, import, distribution, advertising, labelling, commercialisation and post-market vigilance of medicines, medical devices, food and beverages, cosmetics, seeds, cannabis, veterinary products, chemicals, alcohol and tobacco. She has experience in consultancy, government relations, administrative proceedings, product registration and contractual work.

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-calder%C3%B3n-143a0321

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 Plasencia is a technology partner of the IP Practice Group at Baker McKenzie Guadalajara. He has extensive experience in: data privacy, information and cybersecurity matters; regulatory issues related to information technologies and consumer protection; and intellectual and industrial property, especially focused on digital environments, including the use and licensing of trademarks, patents and copyrights. Daniel is a Certified Information Privacy Administrator by the International Association of Privacy Professionals. Before joining the firm, he was a founding partner of a local firm in Guadalajara.

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

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. The Firm works with the leading companies in both the healthcare sector and the information technologies market.

www.bakermckenzie.com

Pakistan

Majeed & Partners, Advocates & Counsellors at Law

Saqib Majeed

1 Digital Health

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

The term 'digital health' is not formally defined under Pakistani law. However, the National Digital Health Framework 2022–2030 ("***NDH Framework***"), prepared by the Ministry of National Health Services, Regulations and Coordination of the Government of Pakistan ("***GOP***") in collaboration with provincial health departments, borrows the definition of this term from the Global Strategy on Digital Health 2020–2025 of the World Health Organization. Accordingly, the expression 'digital health' is defined in the NDH Framework as "the field of knowledge and practice associated with the development and use of digital technologies to improve health".

The NDH Framework further clarifies that digital health has a broad scope, encompassing wearable devices, mobile health, telehealth, health technologies, disease modelling, diagnostics, health services management, artificial intelligence ("***AI***"), big data analytics, the internet of things and telemedicine.

Some provincial legislations, particularly those in the Sindh Province, provide definitions for expressions that may generally fall under the category of digital health. For instance, the Sindh Telemedicine and Telehealth Act, 2021 ("***Sindh Telemedicine Act***"), defines the term 'telemedicine' as: "The delivery of healthcare services through secure two-way audio or video connections, including the application of secure video conferencing or store and forward technology, electronic media, or other telecommunications technology, or an automated computer program, encompassing AI. This includes, but is not limited to, online adaptive interviews, remote patient-monitoring devices used by all healthcare professionals, utilising information and communication technology for the exchange of information for the diagnosis, treatment, and prevention of diseases and injuries, as well as for research and evaluation."

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

Pakistan currently lacks an advanced digital healthcare system. Digital health technologies in the private sector mainly encompass telemedicine, telehealth, mobile health and e-pharmacies. In the public sector, there is a growing utilisation of digital health technologies, including electronic health records, health information systems, big data analytics, AI and Cloud computing. These advancements aim to enhance the governance of public-sector healthcare resources for better efficiency.

1.3 What are the core legal issues in digital health for your jurisdiction?

Digital health technologies inherently involve handling an individual's sensitive personal data. The Constitution of Islamic Republic of Pakistan, 1973 ("***Constitution***"), as interpreted by local court, recognises the right to privacy of personal information as a fundamental human right.

However, there is currently no legislation addressing the essential aspects of personal data management, including collection, use, storage, sharing, transfer and security. The absence of a comprehensive legal framework regulating the processing of personal data raises significant concerns for both digital health service providers and patients. This gap heightens the risks associated with compliance. Moreover, the lack of specific standards for data protection gives rise to apprehensions about confidentiality and potential misuse and abuse of patients' health data.

Pakistan is a federal republic. Under the Constitution, legislative powers are divided between the federal legislature, known as the Parliament, and the four provincial assemblies. Health-related matters fall exclusively within the legislative competence of provincial assemblies. This constitutional setup often results in separate legal frameworks for regulating the health sector in the federal capital and the provinces. Consequently, providers of digital health services must ensure compliance with multiple legal frameworks, resulting in enhanced regulatory compliance efforts and costs.

Legislative response to technological advancements in the health sector is very slow and existing laws are mostly incompatible with innovative digital health products, thereby decreasing the effectiveness of these products.

Some digital health technologies, like wearables, may be categorised as medical devices under the Drug Regulatory Authority of Pakistan Act, 2012 ("***DRAP Act***"). To manufacture, import or sell these in Pakistan, compliance with registration and licensing requirements under the DRAP Act is necessary.

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

No official figures are available regarding the size of the digital health market in Pakistan. However, estimates suggest that total healthcare spending in the country now surpasses Rs. 1,500 billion (around USD 5.3 billion) annually, with households being the largest healthcare spenders, contributing approximately Rs. 700 billion (around USD 2.5 billion). A significant portion of this spending is directed towards retail

pharmaceutical purchases and outpatient service fees – both areas being targeted by existing digital health service providers.

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

The digital healthcare industry in Pakistan is in its early stages, with several startups in operation, none of which have fully scaled up yet. Almost all these startups operate as private limited companies. Unlike publicly listed companies, private companies in Pakistan are not obligated to disclose financial information, making it challenging to assess the financial health or revenues of these startups. Limited available data suggests that the five largest digital health companies in Pakistan are Sehat Kahani, Dawaai, Healthwire, Ailaaj and Marham.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

Pakistan currently lacks a dedicated legal framework for regulating digital health, except for the Sindh Province, which has enacted the Sindh Telemedicine Act to regulate certain aspects of digital health. The Sindh Telemedicine Act mandates that medical professionals must practice telemedicine or telehealth after completing an online course and registering themselves with the registry established under said Act. It also emphasises the privacy and security of patients' health information, requiring service providers to implement reasonable security measures for the protection of such information.

Certain federal and provincial laws enacted to regulate healthcare professionals and the manufacture, marketing and sale of therapeutic goods may equally apply to digital health products and services.

The DRAP Act, together with the Drugs Act, 1976 ("***Drugs Act***"), regulates the manufacture, import, export, storage, distribution and sale of therapeutic goods in Pakistan. Both laws are federal legislation and apply uniformly across the entire country.

The DRAP Act ensures, *inter alia*, that therapeutic goods manufactured or imported in Pakistan meet the prescribed standards of quality, safety and efficacy. Therapeutic goods are broadly defined to include medical devices. Some digital health technologies, including wearables, may be categorised as medical devices requiring compliance under the DRAP Act.

The Drugs Act, *inter alia*, prohibits the sale of drugs to the public without obtaining a licence from the respective provincial government.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Other core regulatory schemes that may apply to digital health in Pakistan include the following:

The Pakistan Medical and Dental Council Act, 2022 ("***PMDC Act***") regulates the medical profession and the medical practitioners in Pakistan. The Professional Ethics and Code of Conduct issued by the Pakistan Medical and Dental Council ("***PMDC***"), established under the PMDC Act, contains instructions concerning the practice of medicine through web-based telemedicine sites with a strong emphasis on the privacy of patient information and strictly prohibits the transfer of such information to another jurisdiction without informed consent.

The Electronic Transactions Ordinance, 2002 ("***ETO 2002***") provides legal recognition to electronic signatures, electronic documents and electronic communication. The ETO 2002 also determines the principles for sending and receiving electronic communication. It will apply in respect of any communication or transaction carried out through an online platform.

The Pakistan Telecommunication (Re-organization) Act, 1996 ("***Telecom Act***") regulates the use of frequency spectrum. Any equipment using frequency spectrum requires type approval from the Pakistan Telecommunication Authority ("***PTA***") under the Telecom Act.

The Prevention of Electronic Crimes Act, 2016 ("***PECA 2016***") prohibits unauthorised access to information systems or data. It also regulates certain aspects of online offences such as identity theft, online fraud, etc.

Separate Healthcare Commissions Acts ("***HCCAs***") have been enacted in each province and the federal capital territory to regulate certain aspects of the provision of healthcare services and to provide legal recourse to victims of medical negligence. These HCCAs may apply to certain digital health products, such as telemedicine and telehealth, etc.

Provincial Consumer Protection Acts have been enacted to set up specialised consumer courts for the redressal of grievances of consumers against manufacturers and service providers regarding defective goods and services. The jurisdiction of these consumer courts may extend to certain digital health products and services.

The Competition Act, 2010, aims to promote healthy competition and prohibits misleading or deceptive marketing practices. Any digital health products that may cause consumers to be misled or make misrepresentations about the quality, purpose or efficacy of the product can face inquiry and legal action under the Competition Act.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The DRAP Act, the Medical Devices Rules, 2017, and instructions issued by the Drug Regulatory Authority of Pakistan ("***DRAP***") may apply to any consumer healthcare devices and software that may fall within the definition of medical devices under the DRAP Act.

The term 'medical devices' includes instruments, machines, software and more, serving purposes such as: (i) diagnosis, prevention, monitoring, treatment, or alleviation of disease or injury; (ii) investigation, replacement, modification, or support of the anatomy or of a physiological process; and (iii) supporting or sustaining life. These devices must not primarily act through pharmacological or immunological means in or on the body, although they may be assisted by such means.

Medical devices are classified into four classes using a risk-based classification rule, i.e., the potential of a medical device to cause harm to a patient or user, its intended use and the technology it utilises. Sometimes it becomes challenging, especially for emerging technologies, to determine which products must be registered and the applicable requirements for their manufacture, import, marketing and sale. In such cases, DRAP typically follows the guidelines issued by the Global Harmonization Task Force or the International Medical Device Regulators Forum ("***IMDRF***").

The manufacture, import and sale of medical devices in Pakistan requires an establishment licence from DRAP. In addition, enlistment or registration, as applicable, of medical devices with DRAP is also mandatory.

To the extent that any consumer healthcare devices use radio frequency or spectrum, it may also require type approval from PTA under the Telecom Act.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

DRAP, a federal agency established under the DRAP Act, serves as the primary regulatory authority in Pakistan for therapeutic goods. It enforces the provisions of the DRAP Act, the Drugs Act, and various associated rules and regulations. DRAP is responsible for the registration of therapeutic goods manufactured or imported in Pakistan, ensuring their compliance with applicable quality standards. DRAP is also responsible for licensing and registration of manufacturers and importers of therapeutic goods in Pakistan.

For digital health products using frequency spectrum or falling within the category of terminal equipment under the Telecom Act, PTA is the principal regulatory authority. PTA ensures that these products meet applicable standards under the Telecom Act and enforces certain aspects of the PECA 2016.

Provincial health departments act as principal regulatory authorities for enforcing provincial drugs rules, including the grant, renewal and revocation of drug sale licences within their respective provinces.

The PMDC serves as the principal regulatory authority for health professionals in Pakistan, including those engaged in provision of digital healthcare services such as telemedicine and telehealth.

Provincial Health Care Commissions function as principal regulatory authorities, responsible for licensing and registering healthcare service providers within their respective provinces. They also adjudicate claims related to medical negligence and malpractices.

The Competition Commission of Pakistan is the principal regulatory authority for implementing the Competition Act, 2010. This includes overseeing its provisions that prohibit deceptive marketing practices by businesses.

2.5 What are the key areas of enforcement when it comes to digital health?

As mentioned above, Pakistan lacks a comprehensive legal framework for regulating digital health. Besides, the regulatory authorities are not very proactive in enforcing general laws that may be applicable to digital health products. The primary focus of enforcement is to ensure that:

a) therapeutic goods manufactured or imported in Pakistan are enlisted or registered under the DRAP Act and meet quality standards;
b) healthcare services are provided by qualified and registered professionals;
c) drugs are marketed and sold by licensed establishments; and
d) confidentiality of patients' health information is maintained.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

Software may be installed into a medical device or used standalone as a medical device, i.e., Software as a Medical Device ("***SaMD***"). In either case, it will be regulated under the DRAP Act and the Medical Devices Rules. When software is integrated into a medical device, the Medical Devices Rules stipulate that complete documentation on software validation studies, including the results of all verification, validation and testing conducted prior to the final release, must be submitted with the application for enlistment or registration of the medical device with DRAP. For SaMD, it must be enlisted or registered as an active device and assigned a suitable classification. The DRAP Act and the Medical Devices Rules do not provide sufficient guidance on the registration or risk classification of SaMD. In such cases, DRAP typically relies on the IMDRF's guidance on SaMD.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

As of now, there are no specific regulations for AI/machine learning-powered digital health devices or software solutions. However, the response provided in question 2.6 above equally applies to these devices.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  a) Lack of a comprehensive legal framework.
  b) Registration or licensing, as applicable, under certain laws such as the HCCAs, the Provincial Drugs Rules and/or the Sindh Telemedicine Act.
  c) Whether any devices or software used in providing telemedicine/virtual care services qualify as medical devices, requiring compliance under the DRAP Act and the Medical Devices Rules.
  d) Whether any device uses frequency spectrum or may fall within the definition of terminal equipment requiring type approval from PTA under the Telecom Act.
  e) Establish the legal basis for processing patients' health information and ensure compliance with obligations regarding confidentiality and privacy.
  f) Provision of healthcare services only by registered health professionals in accordance with applicable healthcare standards.
  g) Liability allocation among service providers (digital platform providers, registered health professionals, etc.).
  h) Ownership of data and intellectual property rights.
- **Robotics**
  a) Whether any devices and/or software qualify as medical devices, requiring compliance under the DRAP Act and the Medical Devices Rules.
  b) Whether any device uses frequency spectrum or may fall within the definition of terminal equipment requiring type approval from PTA under the Telecom Act.
  c) Establish the legal basis for processing patients' health information and ensure compliance with obligations regarding confidentiality and privacy.
  d) Liability allocation among service providers (manufacturers, operators, etc.).
  e) Ownership of data and intellectual property rights.
- **Wearables**
  a) Whether any devices and/or software qualify as medical devices, requiring compliance under the DRAP Act and the Medical Devices Rules.

b) Whether any device uses frequency spectrum or may fall within the definition of terminal equipment requiring type approval from PTA under the Telecom Act.
c) Establish the legal basis for processing patients' health information and ensure compliance with obligations regarding confidentiality and privacy.
d) Ownership of data and intellectual property rights.

- **Virtual Assistants (e.g. Alexa)**
  Similar issues as for Telemedicine/Virtual Care.
- **Mobile Apps**
  Similar issues as for Telemedicine/Virtual Care.
- **Software as a Medical Device**
  Similar issues as for Telemedicine/Virtual Care.
- **Clinical Decision Support Software**
  Similar issues as for Telemedicine/Virtual Care.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  Similar issues as for Telemedicine/Virtual Care.
- **IoT (Internet of Things) and Connected Devices**
  Similar issues as for Telemedicine/Virtual Care.
- **3D Printing/Bioprinting**
  Similar issues as for Telemedicine/Virtual Care.
- **Digital Therapeutics**
  Similar issues as for Telemedicine/Virtual Care.
- **Digital Diagnostics**
  Similar issues as for Telemedicine/Virtual Care.
- **Electronic Medical Record Management Solutions**
  Similar issues as for Telemedicine/Virtual Care.
- **Big Data Analytics**
  Similar issues as for Telemedicine/Virtual Care.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Similar issues as for Telemedicine/Virtual Care.
- **Natural Language Processing**
  Similar issues as for Telemedicine/Virtual Care.

3.2 What are the key issues for digital platform providers?

Digital platform providers in Pakistan face a significant challenge due to the absence of a comprehensive legal framework for digital health, resulting in uncertainty and potential liabilities arising from the actions of other suppliers within the platforms. It should be noted that assigning liability through contracts among service providers may prove ineffective for claims based on a statutory liability such as under the consumer protection laws.

Digital platform providers must determine the precise scope of their digital platforms and identify any required licences or registrations for their operation, such as under the Provincial Drugs Rules. Additionally, they must ascertain whether their digital platforms fall within the definition of medical devices, necessitating enlistment or registration under the Medical Devices Rules. Implementing a robust due diligence mechanism is essential to ensure that digital health services through digital platforms are delivered exclusively by registered healthcare professionals.

Another pressing concern is the absence of data protection legislation, making explicit consent the sole legal foundation for processing personal data. Providers must ensure that this consent adequately covers all types of data processing on their platform and, when necessary, its disclosure to third parties. They must also prioritise the privacy and security of data generated, processed or stored on their platform. Clear provisions addressing the ownership of intellectual property rights in information generated through the platform should be expressly outlined.

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

The right to privacy of information is considered a fundamental right of citizens under Articles 9 and 14 of the Constitution of Pakistan. Additionally, unauthorised access to data and unauthorised transmission of data with a dishonest intent constitute offences under the PECA 2016 punishable with corporal punishments. However, at present, Pakistan does not have comprehensive personal data protection legislation. In these circumstances, the fundamental issue to be considered is the legal basis for use of personal data.

It is noteworthy that the federal government has prepared a draft Personal Data Protection Act, 2023 ("***Draft PDP Act***"), but it is yet to be voted on by the Parliament. The Draft PDP Act, in its current form, is based on the European Union's General Data Protection Regulation ("***EU GDPR***"). However, in certain aspects, its requirements significantly differ from those laid down in the EU GDPR.

4.2 How do such considerations change depending on the nature of the entities involved?

The considerations outlined in our response to question 4.1 do not depend on the nature of the entities involved and remain consistent. However, for entities operating in the healthcare sector, stringent requirements regarding the confidentiality and security of patients' health information will apply. However, where government entities are involved in the use of personal data, the requirements may not be strictly enforced.

The Draft PDP Act permits the use of sensitive personal data, including health data, under specific circumstances without the consent of the data subject. This exception applies when such use is for medical purposes by a healthcare professional or an individual with a duty of confidentiality equivalent to a healthcare professional. Consequently, if the Draft PDP Act is enacted in its current form, use of sensitive personal data by healthcare professionals would be exempt from the requirement of informed consent. Also, the Draft PDP Act imposes less stringent requirements on data processors compared to data controllers.

4.3 Which key regulatory requirements apply?

As explained in our response to question 4.1, currently, Pakistan does not have data protection legislation. Therefore, there is no clarity regarding the regulatory requirements applicable to the use of personal data. In these circumstances, it must be ensured that explicit and informed consent from the data subject is obtained concerning the use and processing of their personal data. Such consent should be properly scoped to include all types of uses of personal data. Furthermore, compliance with the regulatory requirements applicable to the healthcare industry regarding protection and confidentiality of personal data, as explained in our response to question 2.1 above, should be ensured.

If the Draft PDP Act is enacted in its current form, data controllers will bear significant responsibilities. They must ensure the legality of personal data collection through consent or other specified lawful purposes. Data subjects must be informed about the purpose, legal basis, usage and sharing of collected data. The processing of personal data must be confined to lawful and directly related activities. Disclosure for purposes

beyond the specified or directly related ones must be made with explicit consent from data subjects. Collected personal data must be adequate and not excessive for its intended purposes. Accuracy, completeness and regular updates must be ensured. Personal data should not be retained beyond the necessary duration. Applicable standards to protect personal data must be strictly followed, with any breaches promptly reported.

Under the Draft PDP Act, data subjects have the right to avoid decisions based solely on automated processing leading to legal obligations or significant harm without explicit consent. They also have the right to receive specific information about automated decision-making and human intervention from the data controller. However, this does not apply to decisions made in the public interest.

4.4 Do the regulations define the scope of data use?

Currently, there are no regulations defining the scope of data use.

However, this is expected to change if the Draft PDP Act is enacted in its current form. According to the Draft PDP Act, personal data must be collected for a specified, explicit and legitimate purpose, and should not be processed in ways incompatible with that purpose. The use of sensitive personal data, including health data, without the prior informed consent of the data subject is prohibited under the Draft PDP Act. Nevertheless, there are exceptions to this rule. For example, healthcare professionals or individuals with a duty of confidentiality equivalent to a healthcare professional can use sensitive personal data for medical purposes without consent. Additionally, the use of sensitive personal data without consent is permitted if necessary for treatment, public health, medical or research purposes, or to respond to a medical emergency involving a threat to the life or health of the data subject or another individual.

4.5 What are the key contractual considerations?

In the absence of data protection legislation providing a legal basis for the use and processing of personal data, explicit consent alone can serve as the legal foundation. It is crucial that relevant contracts accurately document informed explicit consent, clearly outlining the nature of personal data to be collected and disclosed, the intended purposes and the involved parties. These considerations are equally important when entering contracts with third parties, especially data controllers or processors abroad, who may be regulated under different data protection regimes providing additional legal basis for the processing of personal data.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

The absence of a legal framework concerning the processing of personal data creates uncertainty about securing comprehensive rights, especially for sensitive data. It remains unclear to what extent courts will allow data controllers to assert rights over such data, even if collected or used with explicit consent. It is generally advised that contractual arrangements regarding the collection and use of personal data should include clear provisions about the ownership of the data used or collected. These provisions should be reasonable in scope and should not result in harm to the data subject or put them at a disadvantage.

If the Draft PDP Act is enacted in its current form, data controllers will not be permitted to use collected data beyond what is necessary for providing the relevant service or product, regardless of the data subject's consent. Additionally, when entering contractual arrangements, due consideration must be given to the provisions of the Draft PDP Act concerning an individual's right to withdraw consent and the right to erasure of personal data, as these provisions are likely to impact securing comprehensive rights to data that is used or collected.

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

The current legal framework in Pakistan does not address issues such as data inaccuracy, bias and/or discrimination in relation to the processing of personal data. Regarding healthcare products classified as medical devices, DRAP may intervene to address issues of data inaccuracy, bias and discrimination if these issues pose risks of errors or safety concerns. In such cases, DRAP may refuse to enlist or register the relevant medical devices and, if already registered, may issue a recall order.

If the Draft PDP Act is enacted in its current form, data controllers will be obligated to take adequate steps to ensure that the required personal data is accurate, complete, not misleading and kept up to date. Thus, data inaccuracy may potentially constitute a breach of the obligation under the Draft PDP Act. Additionally, while the Draft PDP Act does not expressly address issues such as bias and discrimination, it generally requires that data subjects shall not, without explicit consent, be subjected to a decision based solely on automated processing, including profiling, that results in legal obligations or significantly harms the data subject.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

The current regulatory framework in Pakistan does not address legal issues concerning data usage by generative-AI companies. It is expected that certain concerns related to generative-AI companies, such as the use and sharing of data, data privacy and security, automated decision-making and bias, will be addressed in the Draft PDP Act or the regulations to be made thereunder. However, there is no guidance on how complex issues, such as the infringement of intellectual property rights by AI-generated content and liability in the case of AI-generated content causing harm, will be handled by local regulators.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The fundamental considerations when sharing personal data include assessing whether the relevant individual has expressly consented to the sharing and whether such consent is adequate. This is particularly important for health data, which must be kept confidential under healthcare industry regulations.

Another important aspect to consider is the potential liability in case of misuse of personal data by the party with whom it is shared or if that party fails to ensure the privacy of the shared data. It is essential to contemplate the consequences of these risks, and any contractual arrangement regarding data sharing should incorporate adequate protection against liability.

If the Draft PDP Act is enacted in its current form, it will introduce additional grounds for the use and processing of personal data beyond explicit consent. Concerning the sharing of personal data, especially health data, it will be important to determine beforehand whether such sharing is covered by any of the grounds provided in the Draft PDP Act.

5.2 How do such considerations change depending on the nature of the entities involved?

While the considerations related to sharing personal data remain independent of the nature of involved entities, the requirements for data sharing are generally either less stringent or not strictly enforced against public-sector entities.

Moreover, more stringent requirements and additional restrictions may be imposed on national security grounds when sharing data with entities from specific jurisdictions.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The key regulatory requirements applicable to data sharing have been outlined in our responses to the preceding questions 5.1 and 5.2. The primary requirement is to obtain explicit consent from relevant individuals for such sharing. The document recording this consent must clearly state the purpose for which personal data is shared and can be utilised. It is particularly advisable for health data, which is required to be kept confidential under applicable healthcare regulations, to ensure that such data is not shared for any purpose unrelated to its initial collection.

If the Draft PDP Act is enacted in its current form, the cross-border transfer of critical personal data will be prohibited. Additional conditions will apply to the cross-border transfer of personal data, including the provision of a copy of any sensitive personal data kept outside Pakistan to the government within specified timelines.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

The NDH Framework delineates five strategic objectives to advance the use of modern digital technologies in the healthcare sector. These objectives include the establishment of a national interoperable digital health ecosystem by defining standards for safety, privacy, interoperability, confidentiality and ethical use of data. The recommended steps involve digitising data entry at the first point of contact between healthcare providers and patients and introducing electronic medical records at the tertiary care facility level. Mandatory reporting of such data through provincial healthcare commissions or regulatory authorities is also envisaged. However, the NDH Framework is currently in the initial implementation stage, and the applicable standards are yet to be issued.

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

As explained in our response to question 1.3 above, Pakistan is a federal republic, where, according to the Constitution, the authority to enact laws pertaining to health lies with the provincial legislatures, unless they jointly request the Parliament to formulate a law applicable nationwide. Laws passed by provincial legislatures may not always be identical, leading to potential inconsistencies among them. Ensuring compliance with applicable legal requirements for healthcare data sharing and the privacy and protection of shared healthcare under respective provincial laws poses a significant challenge.

Another significant challenge arises from the lack of standardisation in data practices and interoperability due to varying approaches to healthcare data collection across provinces. The NDH Framework aims to address these challenges and establish a uniform legal framework at the national level for digital healthcare, with the consent and support of all provincial legislatures. However, progress on the implementation of this initiative has been slow.

Additionally, if the draft PDP Act is enacted in its current form, it will also address some of the issues concerning the collection, use and sharing of healthcare data.

6 Intellectual Property

6.1 What is the scope of patent protection for digital health technologies?

The Patents Ordinance, 2000 ("***Patents Ordinance***"), governs the grant and renewal of patents in Pakistan. This ordinance aligns with the requirements of the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights.

To qualify for a patent, an invention must be new, involve an inventive step and be capable of industrial application. The Patents Ordinance does not recognise computer software as an invention. Additionally, the Patents Ordinance prohibits the grant of patents, *inter alia*, for diagnostic, therapeutic and surgical methods for the treatment of humans or animals.

As a result, patent protection under the Patents Ordinance cannot be obtained for digital health technologies that consist of computer software alone. However, when digital health technology involves a combination of software and hardware, patent protection can be claimed for it.

The term of a patent is 20 years.

6.2 What is the scope of copyright protection for digital health technologies?

The scope of copyright protection for digital health technologies is defined by the Copyright Ordinance, 1962 ("***Copyright Ordinance***").

According to this ordinance, copyright extends throughout Pakistan to various classes of works, including original literary, dramatic, musical and artistic works. For literary works, copyright subsists for the life of the author until 50 years from the beginning of the calendar year following the author's death.

Although copyright may be registered under the Copyrights Act, registration is not mandatory for claiming protection.

Computer programs and software fall within the definition of literary work and can be protected under the Copyright Ordinance. Consequently, copyright protection may be claimed for digital health technologies that consist of software.

It is important to note that different rules apply to determine the ownership of any literary works created under a 'contract for service' and a 'contractor of service.' Additionally, the Copyright Ordinance imposes certain restrictions on the assignment of copyrights in certain situations.

6.3 What is the scope of trade secret protection for digital health technologies?

In Pakistan, confidentiality and trade secret protection are

commonly addressed through contractual arrangements, incorporating confidentiality, non-disclosure and similar restrictive covenants. It is essential to acknowledge, however, that the courts do not always enforce such contractual arrangements. When seeking enforcement, the party must provide a clear rationale, demonstrating a legitimate need rather than using the covenant solely for punitive measures or to stifle competition. In certain situations, trade secret protection may also be pursued through legal provisions concerning breach of trust and the common law principle of breach of confidence.

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

There are no specific rules or laws that govern academic technology transfers. Generally, these matters are addressed through contractual arrangements. Regarding technology developed in academic institutions, considerations of ownership, licensing and assignment of intellectual property rights are determined in accordance with applicable intellectual property legislation and contract law.

6.5 What is the scope of intellectual property protection for software as a medical device?

SaMD are classified as computer programs, falling within the definition of 'literary work', making them eligible for protection through copyright. The Intellectual Property Organization of Pakistan's Patent Office maintains the stance that computer programs cannot be protected through patents. However, the absolute nature of this exclusion remains unclear, particularly whether computer programs with a 'technical character' can be granted patent protection. So far there is no reported judgment on this matter.

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

There is no formal adjudication on this matter. However, under the Patents Act, an application for a patent can only be filed by a natural person, a judicial person, or an association or body of individuals. An AI device does not qualify as any of these.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

There are no specific rules or laws related to government-funded inventions in Pakistan. Government funding to support innovation is available on a very limited scale and is typically regulated through contractual arrangements.

7 Commercial Agreements

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

The primary focus when engaging in collaborative improvements should be to establish a clear and transparent contractual framework that governs the utilisation, assignment and ownership of intellectual property rights connected to these enhancements. These contractual arrangements must align with the provisions of intellectual property laws, particularly those addressing ownership and assignment issues. Additionally, aspects related to the use and licensing of any existing or background technology, along with associated royalty payments, should be carefully addressed. In cross-border collaborations, it is essential to consider restrictions on outbound royalty payments. Ensuring confidentiality is paramount. Furthermore, it is important to verify that the collaborative arrangement does not fall within a 'prohibited agreement' under competition law.

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

When dealing with agreements between healthcare and non-healthcare companies, it must be ensured that such agreements do not lead to a breach of regulatory requirements applicable to healthcare companies, especially those concerning the confidentiality of patients' health information, as well as any relevant healthcare codes and standards.

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

There is currently no official guidance regarding federated learning healthcare data-sharing arrangements between companies, contributing to increased compliance-related risks. It is expected that this inadequacy will be addressed once the NDH Framework is implemented, and necessary regulations are issued thereunder.

When entering into federated learning healthcare data-sharing agreements, key considerations include privacy, security and data protection. Additionally, it should be ensured that the consent of data subjects is appropriately scoped to include such sharing. Shared data should be interoperable.

In light of legal obligations concerning the confidentiality of patient records, where applicable, the information to be shared should be anonymised before any sharing takes place. Matters concerning the ownership of shared data should be explicitly addressed, and adequate mechanisms should be implemented to control access to shared data.

The contractual arrangement concerning federated learning healthcare data sharing should expressly outline the consequences of breaching these obligations. Appropriate indemnities to protect the innocent party may also be included.

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

No official guidance is currently available regarding the use of generative AI in the provision of digital health solutions. It is expected that regulations, pursuant to the NDH Framework and the Draft PDP Act, will include guiding principles on these matters. Broadly, the considerations include ensuring transparency in data processing, obtaining informed consent from individuals before utilising their data in AI models, diversifying training datasets to ensure unbiased outcomes, implementing continuous monitoring through robust human oversight mechanisms, and providing proper warnings and disclaimers outlining the capabilities of the generative-AI systems in use.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

At present, the use of machine learning in Pakistan's health sector is limited, and is characterised by fragmented research efforts. Nevertheless, the government is actively advocating the integration of machine learning and other digital technologies in healthcare to improve administrative efficiency in hospitals, address infectious diseases through mapping and treatment, and personalise medical treatments. The recently adopted NDH Framework aims to promote the utilisation of machine learning across various facets of the health sector, fostering research and innovation in machine learning for healthcare, digitising healthcare data and employing data for disease modelling.

8.2 How is training data licensed?

There are currently no specific regulations governing the licensing of training data. Licensing of training data can be facilitated through contractual agreements; however, such contracts must align with the applicable regulatory framework. Moreover, the contract should explicitly address matters concerning the permitted use and disclosure of licensed data, as well as establish ownership rights for any work or product resulting from the use of the licensed data.

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

Under the Copyright Ordinance, as a rule, the author of a work is considered the first owner of copyright in that work. Therefore, in the case of algorithms created by a human, that human will be deemed the author and the first owner of intellectual property in the algorithm (unless it was created under a contract of service). The position concerning algorithms created by machine learning without active human involvement is unclear. The Copyright Ordinance envisages only a natural person as the author of a work. As of now, there is no reported judgment addressing this issue.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Key commercial considerations for licensing data for use in machine learning include the accuracy and value of the licensed data, the scope of its use, sharing, disclosure and retention protocols, the financial model for licensing, liability caps, ownership rights in any developments arising from its use, compliance with applicable regulatory requirements and termination procedures.

9 Liability

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

In Pakistan, the liability for adverse outcomes in digital healthcare solutions depends on the nature of the healthcare product and the severity of adverse outcomes. This liability may encompass both civil and criminal aspects, determined by the nature and seriousness of the adverse outcomes.

Typically, civil liability originates from common law principles of tort. Additionally, if adverse outcomes result from a breach of contract, the law of contract becomes relevant. The consumer protection laws also define liability for defective products or services, and such liability cannot be limited or excluded by contract.

In specific situations, special remedies under regulatory frameworks applicable to the healthcare sector may be pursued. For instance, in cases of medical negligence, complaints can be directed to the respective provincial healthcare commissions or the PMDC depending on the sought remedy. In the context of defective healthcare products, complaints can be lodged under the DRAP Act.

In serious situations where adverse outcomes involve bodily harm or injury, they may constitute a criminal offence, attracting punishment under the national penal code.

9.2 What cross-border considerations are there?

For a product manufactured abroad and sold to consumers in Pakistan, the relevant statutory regime in Pakistan applies to non-contractual claims (e.g. product liability, personal injury, etc.). This principle extends to digital healthcare services provided to Pakistani consumers from abroad, although enforcing liability against a foreign manufacturer or service provider typically poses challenges.

Concerning contractual claims, local courts usually uphold a choice of applicable law clauses. Additionally, liability caps are commonly included in cross-border contracts to mitigate exposure.

9.3 What are best practices to minimise liability risks posed by the use of generative AI in the provisioning of digital health solutions?

No official guidance is currently available regarding the best practices to minimise liability risks associated with the use of generative AI in the provision of digital health solutions. It is expected that regulations, pursuant to the NDH Framework and the Draft PDP Act, will include guiding principles on these matters. The best practices generally involve ensuring transparency in data processing, obtaining informed consent from individuals before utilising their data in AI models, diversifying training datasets to ensure unbiased outcomes, implementing continuous monitoring through robust human oversight mechanisms, and providing proper warnings and disclaimers outlining the capabilities of the generative-AI systems in use.

10 General

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

The key issues in Cloud-based services for digital health include data protection and privacy. The lack of a formal regulatory framework governing data protection creates uncertainty about the adequacy of compliance in these matters. Therefore, robust contractual arrangements must be put in place for the protection and privacy of stored data. Additionally, issues concerning the use of data by Cloud service providers and its erasure must be specifically addressed. Data should not be stored in certain locations outside Pakistan. In transactions with public-sector

entities, compliance with the government's Cloud Computing Policy should be ensured. Another important issue is the absence of reliable local Cloud service providers, which often results in increased costs.

If the Draft PDP Act is enacted in its current form, it will regulate the processing and protection of health data, as well as its cross-border transfer and storage.

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

While there are currently no specific regulations governing the digital healthcare market, the healthcare industry in Pakistan is subject to comprehensive regulation through various regulators and frameworks. Non-healthcare companies intending to enter the digital healthcare market must carefully assess the costs and efforts associated with achieving regulatory compliance. It is crucial for them to recognise that the regulatory framework is continuously evolving, necessitating a proactive approach to stay abreast of regulatory changes.

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

Before investing in digital healthcare ventures in Pakistan, venture capital and private equity firms should seek expert advice to fully understand the relevant legal frameworks governing the digital healthcare industry in the country. They must also ensure that the target is in compliance with applicable regulatory requirements and establish the target's ownership of intellectual property rights in the digital healthcare product.

A comprehensive understanding of local market dynamics and opportunities, coupled with an assessment of the target's business strategy and the success rate of similar ventures in the past, is imperative. Extreme care should be exercised during valuations, accounting for all potential risks. Additionally, a thorough understanding of the local company and foreign exchange laws is essential, and the transaction should be structured in compliance with these regulations.

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

Several factors hinder the widespread clinical adoption of digital health solutions in Pakistan. These include the absence of a comprehensive national-level legal framework for regulating digital healthcare services, as well as legal uncertainty stemming from laws that govern the conventional healthcare sector. These laws traditionally follow a premises-based approach and are not fully updated to address the use of technology in healthcare delivery. Another crucial factor is the absence of a legal framework for the processing and protection of personal data. Additional contributing factors include the unavailability of digital health records, a low literacy rate among citizens and widespread poverty.

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 in Pakistan that can influence the clinical adoption of digital health solutions are the PMDC and the Pakistan College of Physicians and Surgeons. However, these certification bodies exhibit limited proactivity in advocating for the adoption of digital healthcare solutions. The GOP's Ministry of National Health Services Regulations and Coordination serves as the leading agency, collaborating with provincial health departments and international agencies to cultivate an environment conducive to accelerating the clinical adoption of digital health solutions at the national level.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

There is currently no government scheme in place to reimburse patients utilising digital healthcare solutions. However, in response to the COVID-19 pandemic, the government entered contractual arrangements with specific digital healthcare providers to address gaps in the public-sector health-delivery system. Under these agreements, the digital health provider offered specified healthcare services to patients, with the government serving as the buyer of these services instead of the patient paying directly.

Reimbursement by private insurers for digital health solutions used by patients depends on the terms outlined in the applicable insurance policy and the contractual arrangements between the digital healthcare provider and the private insurer.

10.7 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 adoption and development of digital health technologies in Pakistan largely depend on the enabling regulatory environment. Acknowledging the potential of digital health technologies for bringing transparency and improving service delivery in the healthcare sector and extending the reach of healthcare facilities to far-flung areas, the government has undertaken several initiatives aiming to create a conducive regulatory environment for the digital health sector. However, the implementation pace of these initiatives is slow, attributed to multiple factors, including political instability.

As 2024 marks an election year, there are expectations that it will bring political stability to the country. It is anticipated that the elected government will progress with the agenda regarding the digital health sector, and the data protection legislation will be enacted soon. Furthermore, the government is expected to swiftly proceed with the implementation of measures outlined in the NDH Framework, particularly focusing on the standardisation and digitisation of health records, including mandatory reporting at the national level.

The IT sector is expected to remain a key area of the government's focus, with various financial incentives to tech companies with innovative business models and ideas expected to continue and increase. Additionally, it is expected that the government will soon proceed with its plan to allocate frequency spectrum for 5G technology, with a rapid rollout of the 5G network following it. These measures are expected to disrupt the healthcare ecosystem. Given Pakistan's robust IT sector, it is anticipated that several digital health startups will enter the local market after these actions are implemented, with the potential to expand into other markets.

Saqib Majeed specialises in banking and finance, corporate, regulatory and public procurement, and is also involved in our litigation and employment groups. He has worked on several preeminent and high-profile transactions in Pakistan.
Saqib has significant experience in Pakistani corporate and commercial laws and is a specialist in cross-border commercial transactions, including restructurings, acquisitions, joint ventures, business alliances, etc.
Saqib has significant litigation experience. He frequently advises foreign clients on litigation matters before courts in Pakistan, as well as in court and arbitration proceedings abroad on matters governed by Pakistani law.
Saqib is a frequent author and has contributed to magazines and international publications on mergers and acquisitions, enforcement of foreign arbitral awards, employment law, trans-national litigation, public procurement, and doing business in Pakistan.

Majeed & Partners, Advocates & Counsellors at Law
554-B, Street 14, Askari 10, New Airport Road
Lahore-58810
Pakistan

Tel: +92 321 442 5310
Email: smajeed@mplaw.com.pk
LinkedIn: www.linkedin.com/in/saqib-majeed-71b81815

Majeed & Partners, Advocates & Counsellors at Law, is a full-service boutique law firm based in Lahore, Pakistan, offering a wide range of high-quality legal services to businesses operating in all major sectors and industries across Pakistan. We have a committed team of experienced lawyers and subject-matter specialists ready to provide client-focused legal solutions. We endeavour to exceed expectations by offering practical advice and help on the path to achieving results.
We offer a broad spectrum of legal services, covering all practice areas essential for clients managing and growing businesses in Pakistan. Our practice is built on our deeply held values of being bold, trustworthy and ethical, collaborative and supportive, which form the foundation of our distinctive culture. These values shape how we conduct business and are essential to the success of our law firm.

Majeed & Partners is the exclusive TerraLex® firm in Pakistan. This prestigious connection gives our clients immediate and seamless access to high-quality, client-focused affiliated attorneys worldwide.

www.mplaw.com.pk

MAJEED & PARTNERS
ADVOCATES & COUNSELLORS AT LAW

Portugal


Eduardo Nogueira Pinto


Hugo Monteiro de Queirós


Tiago Linhares Carneiro


Bartolomeu Soares de Oliveira

PLMJ

1 Digital Health

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

Portuguese law does not provide a specific definition of "digital health". Regulations for digital health matters – understood as the provision of healthcare using digital resources – are usually associated with the laws and regulations on medical devices and statutes and/or professional ethics codes of the relevant professional associations.

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

1. Telemedicine
Telemedicine has reached in the last years a prominence that had never been seen before, although it is not new in Portugal. In 2006, an attempt was made to regulate teleconsultations by defining the concept and establishing the price list for telemedicine services in *Serviço Nacional de Saúde* ("**SNS**"). The pandemic period has clearly evidenced the advantages of telemedicine: greater efficiency; reduction of financial costs; and better access to health services.

2. Medical software
Medical software has come to stay and is progressively being used in healthcare to help doctors to make clinical decisions and establish and develop therapeutic programs.

3. Health apps
Health-related apps are becoming increasingly widespread in society and have a very important role in increasing health literacy and raising awareness of healthy lifestyles. Several entities – both public and private – made available tailor-made apps allowing access to digital health services on mobile devices, including teleconsultation, medicines history, prescriptions, therapeutic programs and monitoring of health parameters.

4. Wearables
Portugal has seen exponential growth in the use of wearables in recent years. Those products are also very relevant from a digital health point of view. These devices often include heart-rate sensors, fitness trackers, sweat meters and oximeters. It is highly expected that wearables will become increasingly important in the coming years.

1.3 What are the core legal issues in digital health for your jurisdiction?

The main issues are related to safety, privacy, information security and personal data protection. The use of digital health devices can lead to self-diagnosis and self-medication by users who do not have the necessary knowledge to decide the treatment for their putative illness.

For matters relating to privacy, information security and data protection, please see section 4 below.

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

Despite having no official data on this matter, some projections to the future of digital health in Portugal point to a marker evaluated up to €470 million by 2027.

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

This information is not publicly available, even though some important companies are operating in Portugal in the digital health market.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The legal framework arises from Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices ("**MDR**") and Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in-vitro* diagnostic medical devices ("**MDIVR**"). There are also the regulations of professional associations addressing professional ethics issues.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, the General Data Protection Regulation ("**GDPR**").
- Decree-Law 7/2004 of 7 January on the legal framework for electronic commerce.

- Decree-Law 383/89 of 6 November on liability for defective products.
- Decree-Law 145/2009 of 17 June on the national provisions applicable to the advertisement of medical devices and governing the relationship between healthcare providers and medical device manufacturers.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Apart from the Regulations on medical devices and *in-vitro* medical devices, the following consumer protection laws are applicable:

- Law 24/96 of 31 July, the Portuguese Consumer Protection.
- Decree-Law 57/2008 of 26 March on Unfair Commercial Practices.
- Decree-Law 330/90 of 23 October, the Portuguese Advertising Code.
- Decree-Law 69/2005 of 17 March on the General Product Safety Law, transposing Directive 2001/95/EC into Portuguese law.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

- The Ministry of Health, as responsible for the definition of the national health policy and for the SNS.
- *Entidade Reguladora da Saúde* ("**ERS**"), which supervises all entities providing healthcare services, except pharmacies.
- Infarmed – *Autoridade Nacional do Medicamento e Produtos de Saúde I.P.*, the regulatory body supervising medicines and health products ("**Infarmed**").
- *Comissão Nacional de Proteção de Dados* ("**CNPD**"), the Portuguese Data Protection Agency.

2.5 What are the key areas of enforcement when it comes to digital health?

- ERS ensures that healthcare providers comply with the requirements for engaging in licensed activities.
- Infarmed supervises the placing of medicines and medical devices on the market, and it enforces conformity with the applicable laws and regulations.
- CNPD, if processing of personal data is required.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

Software classified as a medical device is subject to the MDR or MDIVR, as applicable.

From a domestic law point of view:

i) Decree-Law 145/2009 of 17 June, without prejudice to the MDR.

ii) Decree-Law 189/2000 of 12 August on *in-vitro* diagnostic medical devices, without prejudice to the MDIVR.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

There is currently no specific legislation regarding artificial intelligence ("**AI**") in digital health devices. There is a proposal from the European Commission to harmonise the legislation on AI in the Member States currently under discussion.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  Legal and regulatory challenges in telemedicine and virtual care are mostly related with privacy and data protection.
  The inclusion of digital health implies the redesign of working processes, as well as the integration of new technological systems with existing ones, which also implies adapting several regulations applicable to such activities.
  The confidentiality and security of patients and health professionals must be preserved, with the respective legal challenges, mainly from privacy and data protection points of view.
- **Robotics**
  The use of robotics in healthcare must ensure the safety of patients and the quality of the healthcare provided. Questions regarding liability for accidents and/or medical negligence can also arise.
  The risk of technical errors and failures is also significant when it comes to the use of robotics, being necessary to clarify the legal and regulatory framework applicable to those matters.
- **Wearables**
  Qualification and the requirements to put them on the market are probably the most important issues regarding wearables and mobile apps. Qualification as a medical device is highly important considering that the requirements for the placement on the market differ significantly. As the line between medical devices and non-medical or fitness apps is thin, it is important to ensure the safety of the users without harming the innovation and development of new technological solutions.
  Those technologies can also induce misdiagnosis by users, with the associated danger to the health and safety of the patients.
  Additionally, there are also legal challenges regarding the security of patient data and privacy, namely from the data protection point of view.
- **Virtual Assistants (e.g. Alexa)**
  The safety and the possible illegal practice of health procedures by unqualified "entities" is a very significant risk when it comes to virtual assistants in healthcare. It would be important to evaluate whether virtual assistants might breach the applicable laws and regulations in what relates to healthcare providers.
- **Mobile Apps**
  Please see "Wearables" above.
- **Software as a Medical Device**
  Software can induce overconfidence in patients with the information provided, which may be subject to errors. The qualification of software as a medical device is complex, as it depends primarily on the purpose attributed by the manufacturer. As such, it is essential to ensure that the use of software as a medical device is properly supervised by a healthcare professional to avoid risks and misinterpretation of results. The problem of qualification of the healthcare services providers is also present in this field.

- **Clinical Decision Support Software**
  As support software, this kind of tool should be used to support decision-making by healthcare professionals and not as the final decision-maker. Healthcare professionals should critically analyse the results of software and evaluate whether the suggested decision is correct and suitable for the specific pathology.
  If not, technical errors can compromise the result and the health and safety of the patient. This could then lead to an error in the final diagnosis or in the choice of the most suitable treatment, with legal consequences.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  As a technology based on algorithms, it is essential that the algorithm is tested to be fully reliable and safe. A validation system would be essential to ensure the safety and the suitability of those systems. Healthcare professionals must be specifically trained and educated to apply those technologies to their healthcare activities.
  Another issue is the trust of the patients in those tools. It is necessary to provide accurate information on the benefits of AI in healthcare, and to adopt a fully transparent policy and communicate all the risks involved.
  Inappropriate use of these tools can also lead to responsibility to the relevant players.
- **IoT (Internet of Things) and Connected Devices**
  Privacy and safety of patients are the central topics. There is a risk of cyber-attacks that compromise the privacy and safety of the patients and of a lack of trust in the results obtained by those tools.
- **3D Printing/Bioprinting**
  Quality, safety and suitability of these products are the main concerns regarding 3D printing and bioprinting when applied in the field of healthcare, as well as qualification and certification of those products as medical devices.
- **Digital Therapeutics**
  There is a high risk regarding patient data, especially because it may involve very sensitive data, with the privacy and data protection associated concerns.
- **Digital Diagnostics**
  The main legal and regulatory issues applicable to digital diagnostics are misdiagnosis and the possibility of non-authorised entities providing healthcare services.
- **Electronic Medical Record Management Solutions**
  As in most technological systems applied to health, the major concerns are the privacy of data and possible data breaches, with the inherent legal and regulatory consequences.
- **Big Data Analytics**
  Legal and regulatory challenges are also mainly regarding privacy matters. Using databases implies the use of personal data, which should be kept confidential under the applicable laws. As such, the big risks associated with the use of big data analytics are the possibility of data breaches and the violation of privacy rights.
- **Blockchain-based Healthcare Data Sharing Solutions**
  As in other technology solutions, the prime challenges regarding blockchain-based healthcare data sharing solutions are related to privacy and safe access to the data. Another sensitive aspect is the need to ensure that only permitted persons have access to the data. Finally, due to the nature of this technology, it can be exposed to digital attacks by hackers, having as a consequence a possible data breach.
- **Natural Language Processing**
  The main concerns are privacy and data protection and the capacity of the systems to correctly interpret messages which may lead to contradictory and meaningless communications. In turn, this could cause the unreliability of the system and risk the safety of patients.

3.2 What are the key issues for digital platform providers?

The key issues for digital platform providers are the need to (i) ensure that no illegal content is transferred to the digital platform, (ii) ensure the safety of the patients' data, (iii) ensure that the use of digital platforms is safe, efficient and improves the quality of the healthcare, (iv) design tools that enable a smooth transition to the use of digital platforms and, finally, (v) train and educate healthcare professionals to confidently use those digital tools in their practices.

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

The processing of personal data must consider the nature of the data, as information that relates to an identified or identifiable person, the process of anonymisation, in compliance with the principle of storage limitation, the process of pseudonymisation, to enhance data protection and authentication procedures. Article 9 of the GDPR prohibits the "processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" ("**Health Data**").

This prohibition may not apply under the exceptions in article 9(2), particularly when the data subject gives explicit consent, the processing relates to personal data which are manifestly made public by the data subject, or the processing is necessary for reasons of public interest in public health.

The controller should comply with the duty of information as set forth in articles 12 to 14 of the GDPR.

4.2 How do such considerations change depending on the nature of the entities involved?

Pursuant to article 7 of the GDPR, when processing is based on consent, the controller must be able to demonstrate that the data subject has consented to the processing of their personal data. The consent must be freely given, informed, specific and unambiguous, and the data subject must be able to withdraw it at any time.

Public authorities may process health data when this processing is necessary for reasons of public safety, regardless of consent. In these cases, the processing of health data must be properly justified to ensure the pursuit of a public interest that cannot otherwise be safeguarded. The processing of health data must be carried out by a person bound by duties of confidentiality, and appropriate security measures must be guaranteed to safeguard the security of the information, as defined in Law 58/2019 of 8 August.

4.3 Which key regulatory requirements apply?

Article 5 of the GDPR sets out the principles governing the processing of personal data: lawfulness; fairness and transparency; purpose limitation; data minimisation; data accuracy; storage limitation; integrity; and confidentiality. Exemptions or restrictions to these principles must be provided for by law, pursue a legitimate aim and be necessary and proportional.

Even in cases where the public interest allows for the processing of health data, confidentiality obligations, requirements of proportionality and appropriate security measures must be guaranteed. Access to personal data should be notified to the data subject. Access may be processed on a need-to-know basis and made through electronic means, unless there is technical impossibility or under express instructions contrary from the data subject, if the processing is necessary for (i) preventive or occupational medicine, medical diagnosis, the provision of medical care or treatment, and (ii) reasons of public interest in public health.

4.4 Do the regulations define the scope of data use?

Law 12/2005 of 26 January ("**Law 12/2005**") defines health information as all types of information directly or indirectly linked to the present or future health of a person, whether living or deceased, as well as their medical and family history. Law 12/2005 stipulates that such information may only be used by the health system under the conditions expressed in the written authorisation of the data subject or their representative. Access to health information can be provided for research purposes on the condition that it is anonymised.

Article 6 of Decree-Law 131/2014 of 29 August provides that the processing of genetic information and the creation of genetic databases are allowed exclusively for the provision of healthcare or health research, including epidemiological and population studies.

4.5 What are the key contractual considerations?

Pursuant to article 24 of the GDPR, the controller must implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation. Article 32 of the GDPR provides that such measures include (i) the pseudonymisation and encryption of personal data, (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. The controller and the processor should also take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

When using or collecting personal data, it is vital that the data subject has the rights to be informed, to access the data, to rectify inaccurate data, to erase data, to be forgotten, to restrict the use of the data, to enjoy data portability and to object to the processing. Law 12/2005 defines a genetic database as any record, whether computerised or not, which contains genetic information about a set of persons or families. Regarding such databases, the law establishes that any person may request and have access to information about themselves contained in files containing personal data.

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

Under article 6(2) of Law 59/2019 of 8 August, profiling activities leading to discrimination of natural persons based on special categories of personal data, such as health data, should be prohibited. Article 11 of Law 12/2005 establishes that (i) no one may be prejudiced in any way on the basis of a genetic disease or of their genetic heritage, (ii) no one may be discriminated against in any way on the basis of the results of a genetic test diagnostic, including for the purpose of obtaining or retaining employment, obtaining life and health insurance, access to education and for the purpose of adoption, (iii) no one may be discriminated against in any form, including in their right to medical and psychosocial follow-up and genetic counselling, for refusal to undergo a genetic test, and (iv) everyone is guaranteed equitable access to genetic counselling and genetic testing, with due safeguarding of the needs of the populations most severely affected by a given disease.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

Generative AI companies require a robust data strategy used in the stages of the AI lifecycle, ensuring its quality for data-mining purposes, its sources and processing purposes. These companies must provide clear information to stakeholders, including based on the reporting obligations of the Artificial Intelligence Act Proposal ("**AIA**"). Generative AI companies must provide accountability mechanisms to promote the auditability of AI outputs and the responsibility of the various stakeholders for any damages caused due to errors and biases of the AI system, including the obligation to provide evidence to support or refute claims.

In 2019, the Portuguese Government published its AI Portugal 2030 Strategy with the aims of boosting innovation and investment in AI. Decree-Law 67/2021 and Resolution 29/2020 of the Council of Ministers were enacted, establishing the legislative framework for Technological Free Zones (*Zonas Livres Tecnológicas* – "**ZLTs**"). ZLTs are real-life geographical areas set up as regulatory sandboxes aimed at promoting and facilitating research, development and testing activities.

In 2022, the Agency for Administrative Modernisation (*Agência para a Modernização Administrativa*) published its Guide to ethical, transparent and responsible Artificial Intelligence in the Public Administration. In 2023, the Ibero-American Network reuniting supervisory authorities from Spanish and Portuguese-speaking countries announced that it initiated a coordinated action in relation to ChatGPT.

Since the AIA is yet to be finalised, there have been no developments regarding its implementation in Portugal, particularly as to which national authority will be tasked with monitoring compliance with the AIA obligations or whether regulatory sandboxes will operate as part of the ZLT initiatives.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

GDPR provides for the free flow of data within the EU. There are specific requirements regarding the transfer of personal

data to third countries outside the EU and international organisations, such as adequacy decisions, standard contractual clauses, binding corporate rules, certification mechanisms and codes of conduct. The primary purpose of these requirements is to offer the same level of protection when the personal data of EU citizens is transferred abroad.

5.2 How do such considerations change depending on the nature of the entities involved?

Pursuant to Directive 2016/680, competent authorities may exchange personal data within the EU. The exchange of personal data in these cases is neither restricted nor prohibited for data protection reasons.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Articles 45 and 46 of GDPR provide for two ways of allowing the transfer of personal data to third countries and international organisations: an adequacy decision; or, in the absence of an adequacy decision, a controller or processor may transfer personal data by providing appropriate safeguards, including enforceable rights and legal remedies for the data subject.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

There are key governmental initiatives to establish standards for processing healthcare data in Portugal, namely:

- **Shared Services of the Ministry of Health** (*Serviços Partilhados do Ministério da Saúde* – "**SPMS**") is responsible for developing and managing national health information systems and services. SPMS has been working on various initiatives, such as creating a National Health Surveillance System (*Sistema Nacional de Vigilância Epidemiológica*) for health surveillance and epidemiological monitoring, contributing to public health initiatives and data sharing.
- **Electronic Health Record** (*Registo de Saúde Eletrónico*), including the standardisation of healthcare data to ensure sharing and accessibility of patient information among citizens and healthcare professionals.
- **National Strategy for the Health Information Ecosystem** (*Enesis 2022*) promotes access to health data portability and develops cross-border aspects.

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

Federated models of healthcare data sharing provide a decentralised approach in which data is stored locally and aim to improve health research and clinical practice. When implementing these models, it is important to consider (i) data privacy and security issues, namely integration of IT infrastructures and security policies across healthcare organisations is recommended; (ii) interoperability of healthcare data sharing, including the standardisation of data formats and systems; (iii) provide patients with clear consent mechanisms to determine who can access and share healthcare data; (iv) accountability and data scalability to keep up with the increasing volume and complexity of data; and (v) resource allocation in healthcare organisations, namely infrastructure, training and personnel with expertise in medical and data analytical fields.

6 Intellectual Property

6.1 What is the scope of patent protection for digital health technologies?

A patent confers to its owner the exclusive right to exploit an invention, and to prevent third parties from exploiting such invention without consent.

An invention may be defined, broadly, as a new way of doing something, or a technical solution to a problem in the field of technology. Patent types may amount to a new product, may consist of a new process to obtain a new or an already known product, or to a new use/application of such product.

Patents shall be granted for inventions in all fields of technology, provided that they are new, involve an inventive step and are susceptible of industrial application.

Although digital health technologies can incorporate different innovations, not all of them can be protected by a patent. General patent exclusions exist, for example, with regard to the protection of software without technical character, or to methods for treatment of the human body by surgery or therapy and diagnostic methods practised on the human body (this exclusion shall not apply to products for use in any of these methods). On the other hand, in the digital health technologies sector, patents may (and are often) used to protect inventions relating to hardware, software components of digital health products with a technical effect, and methods and protocols used in digital health products.

6.2 What is the scope of copyright protection for digital health technologies?

In broad terms, copyright, referred to in Portugal as authors' rights, grants protection over externalised expressive intellectual creations, designated as "works", and covers artistic and literary works.

Originality and creativity are the general requirements for a work to be protected by copyright. This means that the work must be the author's own intellectual creation, and that at least some creative aspect is required.

Copyright protection is independent of the registration, disclosure, publication, use or exploitation of the protected work.

Under Decree-Law 252/94 of 20 October, computer programs with a creative character are entitled to protection analogous to that provided for literary works, that is, they are protected in their expression. The protection of software by copyright in Portugal does not affect the freedom of the ideas and principles underlying any element of the program or its interoperability, such as logic, algorithms or programming language.

6.3 What is the scope of trade secret protection for digital health technologies?

Portuguese Industrial Property Code ("**CPI**") provides that trade secrets are protected and that information will be considered as a trade secret if it meets the following requirements: (i) it is secret, in that it is not generally known or easily accessible to persons in the circles that normally deal with this type of information; (ii) it has commercial value by virtue of being secret; and (iii) it is subject to reasonable diligence in order to keep it secret. Articles 314 and 315 of the CPI identify the acts that constitute a legal or illegal use, acquisition or disclosure of the trade secret.

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

Pursuant to article 59 of the CPI, inventions made by employees or collaborators due to their research activities belong to the legal entity under whose statutory scope the research and development activities are carried out.

The inventor will reserve the right to participate in the economic benefits arising from the exploitation or transfer of the patent rights.

The terms of this participation and further issues regarding academic technology transfers are defined in the articles of association and the intellectual property regulations of the legal entity in question.

6.5 What is the scope of intellectual property protection for software as a medical device?

Under the CPI, software *per se* cannot be subject to patent protection. However, patent protection may be granted to software which exhibits a technical effect. The European Patent Office has held that computer software can be patented in certain circumstances: (i) when the software affects the execution of processes which take place outside the software or the computerised system; or (ii) when the software leads the computer/hardware to operate in a new manner. Furthermore, software can be protected by copyright under Decree-Law 252/94 of 20 October, which grants software protection analogous to that conferred on literary works.

The source code of a piece of software may also be protected under the trade secrets rules provided that the necessary requirements are met.

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

There are no specific rules on AI devices being named as inventors in Portugal. When referencing the inventor and "his/her successors in title", article 57 of the CPI appears to be construed around the concept of the inventor being a natural person. Therefore, it seems to exclude legal persons and AI devices from being named as the inventor.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

There are no specific rules on Government-funded inventions. These are subject to the general principles of contractual freedom. The parties can draft the terms of ownership of any IP right and, in the absence of such terms, any supplementary rules will apply.

7 Commercial Agreements

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

There is no specific regulation on collaborative improvements in Portugal. These collaborations are accepted depending on the organisations and professionals involved. The regulatory and legal framework must be observed, particularly regarding interactions between healthcare companies or pharmaceutical industry companies and healthcare professionals, healthcare organisations or patient associations. Under Portuguese law, an "interaction" includes granting benefits to any of the above professionals and organisations, supporting events, granting scholarships and any other interaction that results in the concession of a benefit.

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

It is advisable for these agreements to be concluded in a written instrument where key issues are addressed. Intellectual property rights, data protection and confidentiality are the main issues to be considered. When concluding agreements with public healthcare entities, legal regulations should be considered to prevent distortions to competition and undue influence of healthcare professionals and organisations.

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

A federated learning ("**FL**") model in healthcare data sharing agreements is pivotal in shaping healthcare data platforms and defining common standards. Initiatives such as Gaia-X and funding through the Digital Europe Programme promote an open data infrastructure.

Moreover, FL enables machine learning at scale while preserving data privacy. This approach allows models to learn from decentralised devices without transferring sensitive information, promoting robust algorithms with wider applicability. Thus, FL fosters collaboration among competitive companies since they do not require the exposure of proprietary data. One important initiative is the Mellody project aiming to deploy FL in drug discovery, where multiple life sciences companies collaborate, leveraging each other's data to improve predictive models without compromising confidentiality and revealing their highly valuable in-house data.

While training algorithms collaboratively, FL healthcare data sharing agreements aim to bridge the gap between data governance, privacy and the advancement of AI-driven healthcare solutions.

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

Although there is no specific regulation to this effect, the use of AI must be guided by the respect for fundamental rights, guaranteeing a fair balance between the principles of security, transparency and responsibility, taking into account the circumstances of each specific case and establishing processes aimed at avoiding any prejudice and forms of discrimination, in accordance with the Portuguese Charter on Human Rights in the Digital Age (Law 27/2021, of 17 May).

In addition, decisions with a significant impact on the sphere of recipients that are taken using algorithms must be communicated to those concerned, and be subject to appeal, as well as audits, if necessary.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

As part of AI, machine learning can have a very important role in healthcare. However, this role must respect the patient, his/her safety and privacy.

8.2 How is training data licensed?

Training data may fall under the scope of Decree-Law 122/2000 of 4 July, which incorporated into Portuguese law Directive 96/9/EC regarding the protection of database rights. In such cases, the licensing of training data is subject to the general provisions regarding the licensing of intellectual property rights. If it includes personal health data, the limitations imposed by the GDPR should also be considered in the context of licensing.

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

Pursuant to article 11 of the Portuguese Copyright and Related Rights Code, copyright belongs to the intellectual creator of the work, unless expressly provided otherwise. To date, there are no specific rules for the intellectual property rights resulting from machine learning improvements. Portuguese law does not recognise machine learning or AI as "authors" for copyright purposes. In Portugal, the creation of intellectual works is strictly associated with human beings.

8.4 What commercial considerations apply to licensing data for use in machine learning?

If the licensed data consists of health data, the commercialisation of sensitive information must always comply with the GDPR rules, in particular, the ones in articles 7, 9 and 32. Contractual provisions regarding indemnifications and liability for the use of data in violation of the GDPR should also be implemented by the parties, as should the customary representations and warranties regarding the ownership of the rights over the licensed data. Further issues regarding the definition of ownership of rights relating to that data should also be considered, including the ownership of any future works based on the licensed data, and the conditions and scope of use of that derivative data.

9 Liability

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

Depending on the specific service provided, contractual liability may be applicable. This liability is governed by the law chosen by the parties in the contract or the law where the service is provided.

Non-contractual civil liability may be applicable if the legal criteria are met. Law 24/96 of 31 July establishes an objective liability of the manufacturer for any damage caused by defects in the product or service placed on the market. Other bases of liability may be applicable depending on the nature of the event that led to the adverse outcome.

9.2 What cross-border considerations are there?

When it comes to liability in cross-border interactions, B2B relations must be distinguished from B2C relations:

i) In B2C relations, the parties' choice of the applicable law may not always be the prevalent criteria. Under the Rome Convention on the Law applicable to Contractual Obligations ("**Rome Convention**"), other criteria may be adopted to determine the applicable law depending on the specific circumstances of the case. In these cases, the parties may be able to choose the applicable law. However, if mandatory provisions exist in the country where the consumer has their habitual residency, these provisions will prevail. Under the Rome Convention, the applicable law is the law of the habitual residence of the consumer. As regards non-contractual liability, the Rome Convention determines, as a rule, that the applicable law is the one of the countries where the damage occurs, regardless of where the event giving rise to the damage occurred and the country where the indirect consequences of that event occur. However, there are other criteria depending on the specific circumstances of each case.

ii) In B2B relationships, under the Rome Convention, the law applicable to a non-contractual obligation arising from an infringement of an intellectual property right will be the law of the country where protection is claimed. In the case of a non-contractual obligation arising from an infringement of a unitary EU intellectual property right, the applicable law will be the law of the country where the infringement was committed, except for questions that are not governed by any relevant EU instrument.

9.3 What are best practices to minimise liability risks posed by the use of generative AI in the provisioning of digital health solutions?

Several measures should be taken to minimise the risk to patients:

- Development of a code of ethics for healthcare providers.
- Provision of training on how to use and develop AI systems for all healthcare providers.
- Ensure compliance with data protection regulations, addressing patients' privacy concerns.
- Use of high-quality datasets and representative databases, ensuring the AI system does not discriminate against individuals or groups.
- Establishment of quality-control oversight and inspections.

10 General

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

Issues raised by Cloud-based services relate mainly to data protection, data transmission and privacy. It is essential to be aware that data treatment and data transfer by Cloud service providers raise additional legal issues.

Healthcare organisations must ensure that their Cloud-based systems are reliable, robust and legally compliant. The most frequent risks of Cloud computing are improper access, data leaks, data loss, power failures, loss of control over data

and low security standards. Many of these risks are caused by configuration errors, lack of security updates, insufficient data governance and weak defence mechanisms.

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

The healthcare sector is a heavily regulated sector. EU instruments and national laws establish a framework that must be properly acknowledged by any company before entering the market. Other issues may be raised, particularly regarding intellectual property and data protection.

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

Considering the level of regulation of the health sector, the compliance check is one of the most important requirements any firm should consider when approaching a target firm. The position of the target company in the relevant market, manufacturing costs and distribution channels, intellectual property rights and commercial agreements are key issues to check when entering the market. Possible partnerships with governments in countries with public health systems as well as reimbursement agreements are also important issues that must be addressed before investing in a digital healthcare venture.

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

The key barriers are the legal frameworks, the lack of investment from governments in digital health technologies and the lack of adequate regulation regarding some specific technologies.

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?

Public entities such as the Central Administration of the Health Services, Health Authorities or the Shared Services of the Health Ministry perform an important role in this field. Depending on the type of technology, associations representing manufacturers and other stakeholders can influence clinical adoption of digital health solutions. Associations such as the Portuguese Association of Medical Devices, Portuguese Association of Health Engineering and Management and the Portuguese Telemedicine Association may be able to influence such decisions. Professional associations that regulate healthcare professions are also able to influence the clinical adoption of health solution from the perspective of the healthcare professionals.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

Reimbursements by the Government depend on the product itself and are subject to specific regulation. Requirements for reimbursement are settled by law or administrative order. Solutions focused on efficiency are more likely to be subject to reimbursement rather than solutions focused on preventive health. Reimbursements by private insurers depend on the type of technology and the insurance policy.

10.7 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 Deloitte study "Shaping the future of European Healthcare" (2020), the current main challenges identified in the health digitalisation process in Portugal are bureaucracy, the choice of the most appropriate digital solution and training of healthcare workers. Moreover, adjustments in the regulatory framework are said to be needed to increase patient confidence in the use of digital solutions in healthcare. Inclusion of digital health in the education of healthcare professionals and patient literacy in digital health are also identified as key issues to be developed to allow the advancement of the digital transformation.

The Portuguese Government is engaged in the digital transformation of the healthcare sector and the Portuguese eHealth strategy has been referred to as exemplary by the WHO since 2015.

The Portuguese National Centre for Telehealth was launched in 2016 and was the first centre of this kind in the world. Its mission is to facilitate citizens' access to healthcare, ensure its fairness and increase the efficiency of national resources by taking advantage of ICT. Furthermore, the National Strategic Telehealth Plan of 2019 demonstrates the engagement of the Portuguese Government in the digital transformation of the healthcare sector.

The National Strategy for the Health Information Ecosystem also performs an important role in fostering the digital transformation of the health sector in Portugal. The COVID-19 pandemic allowed some barriers to be broken down as it created an environment that was even more receptive to the implementation of digital solutions in the health sector in Portugal.

It is also relevant to mention the Resolution of the Council of Ministers no. 131/2021 approving the Strategy for the Digital Transformation of Public Administration 2021–2026 and the respective Transversal Action Plan for the legislature. This plan is designed to upgrade services through digital technologies towards simplicity, integration, efficiency and transparency. Six strategic lines can be outlined: 1) digital public services; 2) valuing data; 3) reference architectures; 4) ICT skills; 5) ICT infrastructures and services; and 6) security and trust.

Eduardo Nogueira Pinto is the partner who heads the Healthcare, Life Sciences & Pharmaceuticals practice. He has 20 years' experience in advising Portuguese and foreign companies, and he has worked on many projects in the areas of healthcare and pharmaceuticals.
Eduardo focuses on regulatory matters, licensing, compliance, advertising, prices and reimbursements, contracts and market access.
He has a law degree from the Faculty of Law of Universidade Católica Portuguesa.

PLMJ
Av. Fontes Pereira de Melo, 43, 1050 119
Lisbon
Portugal

Tel: +351 213 197 300
Email: eduardo.nogueirapinto@plmj.pt
LinkedIn: www.linkedin.com/in/eduardo-nogueira-pinto-71458a2b

Hugo Monteiro de Queirós is a partner and head of the Intellectual Property practice, who has more than 15 years' professional experience. He advises on patents, trademarks, designs, copyright, software licensing, information technologies, data protection and advertising. Hugo has also focused on litigation in the area of intellectual property, with an emphasis on dealing with arbitration and court cases involving industrial property rights relating to medicines and trademarks. He also drafts opinions and contracts in the area of intellectual property.
Hugo has been an Official Industrial Property Agent since 2012 and a European Trademark and Design Attorney since 2016.
With a Master's degree in private legal sciences from the Faculty of Law of the University of Porto, he also completed a postgraduate course in arbitration at the Faculty of Law of Universidade NOVA de Lisboa.
Hugo is a frequent speaker at universities and at Portuguese and international congresses and seminars.
Before joining PLMJ, he was a lawyer at BMA, ABBC and CMS Rui Pena & Arnaut.

PLMJ
Av. Fontes Pereira de Melo, 43, 1050 119
Lisbon
Portugal

Tel: +351 213 197 300
Email: hugo.monteiroqueiros@plmj.pt
LinkedIn: www.linkedin.com/in/hugo-monteiro-de-queir%C3%B3s-4a18055

Tiago Linhares Carneiro is an associate lawyer in the Healthcare, Life Sciences and Pharmaceuticals practice and has a law degree from the Faculty of Law of the University of Lisbon.
He is director of the Biosecurity Unit of the Gulbenkian Science Institute and, before joining PLMJ, he was a post-doctorate researcher at this institute and a senior researcher at Medipolis GMP Oy, in Finland. Besides having a degree in law, Tiago has a degree in applied biochemistry from the University of Porto and a PhD in biomedical sciences from the Faculty of Medicine of the University of Lisbon.

PLMJ
Av. Fontes Pereira de Melo, 43, 1050 119
Lisbon
Portugal

Tel: +351 213 197 300
Email: tiago.linharescarneiro@plmj.pt
LinkedIn: www.linkedin.com/in/carneirotiago

Bartolomeu Soares de Oliveira holds a law degree from the Faculty of Law of the University of Lisbon and attended a postgraduate course in pharmacy, medicine and new technologies law at the Biomedical Law Centre of the Faculty of Law of the University of Coimbra.

PLMJ
Av. Fontes Pereira de Melo, 43, 1050 119
Lisbon
Portugal

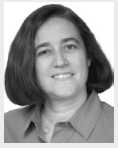
Tel: +351 213 197 300
Email: bartolomeu.soaresoliveira@plmj.pt
LinkedIn: www.linkedin.com/in/bartolomeu-soares-de-oliveira-b64717139

PLMJ is a law firm based in Portugal that combines a full service with bespoke legal craftsmanship. For more than 50 years, the firm has taken an innovative and creative approach to produce tailor-made solutions to effectively defend the interests of its clients. The firm supports its clients in all areas of the law, often with multidisciplinary teams, and always acts as a business partner in the most strategic decision-making processes.
With the aim of being close to its clients, the firm created PLMJ Colab, its collaborative network of law firms spread across Portugal and other countries with which it has cultural and strategic ties. PLMJ Colab makes the best use of resources and provides a concerted response to the international challenges of its clients, wherever they are. International collaboration is ensured through firms specialising in the legal systems and local cultures of Angola, Cape Verde, China/Macao, Mozambique, São Tome and Príncipe and Timor-Leste.

www.plmj.com

PLMJ Transformative Legal Experts

Spain



Montserrat Llopart Vidal

David Molina Moya

Baker McKenzie

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 Spain. According to the *Fundación Tecnología y Salud*, a foundation set up by the Spanish Federation of Healthcare Technology Companies (FENIN), digital health refers to the set of Information and Communication Technologies used in a medical setting in areas related to the prevention, diagnosis, treatment, monitoring and management of health, acting as an agent of change that enables cost savings and improves efficiency.

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

This year has seen a boom in all kinds of projects related to artificial intelligence (AI) in healthcare. From telemedicine applications that use AI to predict possible medical relapses (comparing personal health data collected in real time with the past evolution of previous patients and also enriching it with other scientific knowledge), to projects that seek to use real patient data to "train" algorithms that will be able to better predict diagnoses and/or personalised treatment, to new and better ways for certain companies to communicate with healthcare professionals based on their type of profile.

1.3 What are the core legal issues in digital health for your jurisdiction?

The core legal issues are data privacy, quality of data, cybersecurity and the interoperability of IT systems as well as IP rights. Regulatory issues (product classification as medical device) and financing are also key for the development of digital health.

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

Spain has relatively well-developed digital healthcare and has focused its efforts on advancing its National Health System Digital Health Strategy, seeking to maintain the health of the population through digital transformation involving the entire healthcare ecosystem: patients; professionals; and industrialists.

According to Statista, in 2023 the revenue in the Digital Health market is projected to reach US$ 2.08 bn, showing an annual growth rate (CAGR 2023–2028) of 8.93%, resulting in a projected market volume of US$ 3.19 bn by 2028.

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

The Spanish market continues to develop from multiple players who bet on the digital development of health. The industries of medical supplies, pharmaceuticals, health technology systems, among others, are responsible for accelerating the growth of the sector.

More and more transactional operations between companies, as well as bets on the development of AI and machine learning, robotics and mobile user experience are gaining relevance.

The market is changing and is increasingly directed towards wellness, fitness and sports performance with companies that increasingly invest resources such as Healthia, Doctoralia, Grupo R Queraltó, Sha Wellness Clinic, including from platform development services to increase competitiveness, suppliers of orthopaedic products, to specialised treatments that manage to increase productivity. Activity has also been observed in companies that provide knowledge and include a portfolio of services that connect users with health professionals, such as iSalud and Multiestetica, to name a few.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

Spain does not have specific legislation relating to digital health, but the following schemes apply:

- Royal Legislative Decree 1/2015, approving the revised text of Law 29/2006 on Guarantees and the Rational Use of Medicines and Medical Devices.
- Regulation (EU) 2017/745 on medical devices and Regulation (EU) 2017/746 on *in vitro* diagnostic medical devices.
- Royal Decree 192/2023 on the regulation of medical devices; Royal Decree 1591/2009 on medical devices (partially repealed); Royal Decree 1616/2009 on active implantable medical devices (partially repealed); Royal Decree 1662/2000 on *in vitro* diagnostic medical devices (currently, this last regulation is under review to adapt it to the above EU Regulations).
- Law 34/1988 on Advertising.
- Law 3/1991 on Unfair Competition.

- Guide for Advertising of Medical Devices to the General Public of the Catalonia region – January 2017, fourth edition.
- Code of Ethics of the Spanish Board of Medical Associations (OMC).

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The following regulatory schemes apply to digital health in Spain:

- The General Data Protection Regulation (EU) 2016/679 (GDPR).
- Organic Law 3/2018 of 5 December on Data Protection and Guarantee of Digital Rights.
- Law 34/2002 on Information society services and electronic commerce.
- Royal Decree 3/2010 regulating the National Security Framework in the field of e-government.

Similarly, by October 2024 at the latest, Spain will have to implement the NIS 2 Cybersecurity Directive, which will have a significant impact on the healthcare sector in general and on Digital Health in particular. To a lesser extent, the European Union (EU) regulation known as the Digital Service Act (which will be fully applicable throughout the EU in February 2024) could be applicable to some digital health projects, depending on whether they include certain intermediation features.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

In addition to the regulations mentioned in the answers to questions 2.2 and 2.1 (in the latter case especially if the software is considered to be, or to be integrated in, a Medical Device), the following regulatory schemes apply to consumer healthcare devices/software in Spain:

- Royal Legislative Decree 1/2007 approving the revised text of the general law for the protection of consumers and users (GLPCU).
- Royal Decree 1801/2003 on general product safety.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The Ministry of Health is responsible for the financing of medical devices and establishes the framework for the provision of health services. It is also responsible for consumer protection legislation. The Spanish Agency for Medicines and Medical Devices, attached to the Ministry of Health, supervises the whole lifecycle of medical devices.

The regional authorities are responsible for the provision of healthcare services, supervision of promotional activities, enforcement of consumer protection and market surveillance in general.

The Spanish Data Protection Agency is the national supervisory authority under the GDPR and ensures that data privacy principles and regulations are respected.

The OMC is responsible for supervising doctors, including telemedicine practices.

2.5 What are the key areas of enforcement when it comes to digital health?

The key areas of enforcement for digital health in Spain are the following:

- Regulatory authorities' actions against digital health and healthcare IT that meet the definition of medical devices but have not obtained the CE mark.
- The Spanish Data Protection Agency's actions in the event of breaches of data protection legislation and data security.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

In addition to the regulations mentioned in the answers to the previous questions, software that qualifies as a medical device must follow the provisions relating to medical devices, which vary depending on the kind of medical device.

EU Regulation 2017/745 and EU Regulation 2017/746 apply. At Spanish level: Royal Decree 192/2023 on the regulation of medical devices; Royal Decree 1591/2009 on medical devices (partially repealed); Royal Decree 1616/2009 on active implantable medical devices (partially repealed); and Royal Decree 1662/2000 on *in vitro* diagnostic medical devices (currently this last regulation is under review to adapt it to the above EU Regulations).

The European Commission has issued guidelines on the classification of medical devices and, in particular, on the Qualification and Classification of stand-alone software used in healthcare (MDCG 2019-11).

Digital solutions to be adopted by the national health service are checked to ensure that the security standards required for the public administration are met.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

AI in healthcare is mainly regulated by the EU Medical Devices Regulation 2017/745 (MDR) and *In-vitro* Diagnostic Medical Devices Regulation 2017/746 (IVDR) in combination with the GDPR. Medical devices are often either developed using AI or they have an AI component. The GDPR applies since the application of AI implies the collection or processing of data, and, specifically health data, which is considered as special-category data and is subject to strict privacy and data protection obligations. The MDR and IVDR contain both *ex ante* and *ex post* requirements for AI in healthcare to be safe and performant throughout their entire lifecycle.

Moreover, the Ethics Guidelines for Trustworthy AI, published by the European Commission (2019) highlighted that AI applications should not only be consistent with the law, but they must also adhere to ethical principles and ensure their implementations avoid unintended harm. Since then, the guidelines on this issue have been reiterated. Among the many publications, we can especially highlight the "Regulatory considerations on artificial intelligence for health" guide of the World Health Organization.

On a European level, the EU has presented a Proposal for Regulation, laying down harmonised rules on AI (the AI Act), that will impact medical device and diagnostic companies.

Regulation classifies medical devices and *in vitro* diagnostics as high-risk AI systems; therefore, those AI systems will have to comply with a set of horizontal mandatory requirements for trustworthy AI and follow conformity assessment procedures before those systems can be placed on the EU market. Predictable, proportionate and clear obligations are also placed on providers and users of those systems to ensure safety and respect of existing legislation protecting fundamental rights throughout the whole AI systems' lifecycle. The importance of this Regulation also lies in the fines for non-compliance, some of them up to €30 million or up to 6% of the total worldwide annual turnover for the preceding financial year.

In Spain, following the European scheme, the applicable legislation would be the Royal Decrees regulating medical devices, implantable medical devices and *in vitro* diagnostic medical devices, as well as Organic Law 3/2018 on the Protection of Personal Data.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  There is no specific telemedicine regulation in Spain. The legislation governing healthcare professions refers this issue to the medical profession's deontological rules. The Code of Ethics of the OMC allows telemedicine, if the parties involved are identified, and the confidentiality and security of the communication is ensured. Privacy is another important concern, especially consent, data minimisation and data security. The Code of Ethics of the OMC also states that the use of digital health technologies by the medical profession is not a substitute for the good medical practices and shall ensure the patients' safety.
  As for virtual care, covering both clinical and non-clinical applications, key issues relate to privacy and cybersecurity.
- **Robotics**
  The core issues are product qualification, security, cross-border remote control and liability. Avoiding the risk of hacking is critical. Cross-border remote control raises issues relating to differences in the qualifications of the persons located outside of Spain controlling robotic devices. Finally, it may become difficult to determine whether product defects or incorrect use are to blame when loss or damage occurs.
- **Wearables**
  The core issues are the reliability of data, privacy concerns and data security. To the extent that an app tracks medical conditions, product qualification and liability issues may also arise.
- **Virtual Assistants (e.g. Alexa)**
  The core issues are first data security and the risk of cyberattacks and then the reliability of data, together with privacy concerns. Additional concerns relate to the illegal non-licensed practice of medicine if enforcement authorities consider that the virtual assistant is giving medical advice.
- **Mobile Apps**
  The same issues apply as for wearables – see above.
- **Software as a Medical Device**
  Software that will meet the definition of medical devices needs to be developed according to the requirements set out in medical device regulations in order to obtain the CE mark.
- **Clinical Decision Support Software**
  The core issues are lack of interoperability between different systems and the difficulty to pool information from many and diverse clinical sources. Moreover, product classification, privacy issues and IT law contracts.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  Privacy issues, cybersecurity issues and IT law contracts of all the stakeholders. Additionally, product qualification and liability issues in the event that the algorithm fails and triggers a faulty clinical decision. In addition, in contradictory situations or where there is a lack of interpretation, an algorithm may not work properly. As long as the product liability framework is not amended, the chances to find a developer of a standalone software liable for a defective product are limited. In this regard, the new European Commission Proposal for regulating the liability of AI systems is still at a premature stage. Finally, the AI Act of the EU would require a lot of efforts to be implemented in a regulated sector such as healthcare and has not yet been approved.
- **IoT (Internet of Things) and Connected Devices**
  The core issues are cyberattacks, data security, the value and reliability of the data obtained and privacy issues. Interoperability with healthcare providers' IT systems also needs to be addressed.
  Virtual reality, augmented reality and mixed reality, with their potential for treating patients and affecting their behaviour, may pose additional security and regulatory issues.
- **3D Printing/Bioprinting**
  The core issue is product qualification of the resulting product. The collection of biological samples intended to be used for 3D printing/bioprinting in the framework of biomedical research is subject to Law 14/2007, especially with regard to informed consent, confidentiality and personal data protection. In addition, liability issues could arise with regard to implanted bio-artificial organs or tissues.
- **Digital Therapeutics**
  Sound evidence of performance and clinical evidence is key for digital therapeutics (DTx) to receive conformity assessment under the MDR. Furthermore, risks pertaining to data protection refer to the profiling of patients and the serious security threats and major consequences in the event of a data breach.
- **Digital Diagnostics**
  Personal data protection, cybersecurity, AI, civil liability and IT contracts are the key issues. The vast majority of these technologies are marketed under conditions of use that emphasise that they should not be used to obtain a diagnosis without the intervention of a human doctor (whom the technology will only support). The problem is the automation bias whereby if technology is present, human intervention tends to be increasingly reduced and the human tends to coincide more and more with the machine (so that technology complements less and less and decides more and more).
- **Electronic Medical Record Management Solutions**
  Personal data protection, cybersecurity, interoperability and the regulation of medical records.
- **Big Data Analytics**
  Personal data protection, cybersecurity, AI and IT contracts are the key issues.
- **Blockchain-based Healthcare Data Sharing Solutions**
  The blockchain technology itself has significant problems with data subjects being able to have some of their rights under the GDPR (for example, erasure and rectification) well satisfied. Blockchain-based medical technologies must deal with this issue or they are not "Privacy by design".

- **Natural Language Processing**
  The core issue is the existence of various official languages in Spain, some spoken by small populations. Availability of digital health technologies in several of those languages may be key to their adoption by Spanish regional healthcare authorities.

3.2 What are the key issues for digital platform providers?

The key issues for digital platform providers are as follows:

- Interoperability of digital platforms with apps, wearables, IoT, medical devices and other digital healthcare technologies without compromising the integrity of the platforms.
- Market access issues due to the need for validation before connecting with public healthcare IT systems.
- Business models that favour the creation of value and potential savings for healthcare providers and sustainable financing models.
- Personal data protection, cybersecurity, AI, civil liability and contracts are key issues.
- Depending on the case, they may need to comply with the wide range of DSA obligations (they would have more or less obligations depending on the definition of the DSA in which the platform fits).

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

The main issue to consider is that genetic data, biometric data uniquely identifying natural persons, and health data are considered to be special categories of personal data (art. 9 of the GDPR) and that the GPDR prohibits the processing of special categories of personal data. However, there are some exceptions, such as the explicit consent of the data subject.

The first step when using personal health-related data is to clearly define for which purposes the personal data will be used, in order to check if any of the exceptions foreseen in art. 9 of the GDPR apply and to be compliant with the transparency principle. In this regard, the most commonly used exception is to obtain the explicit consent of the data subject to process personal data concerning health, without such personal data being collected for a purpose other than that for which the data subject gave their consent.

Operators shall limit the purposes for which personal data is collected and provide transparent and granular information on how and by whom personal data is going to be processed. Extending the types of processing in the future to purposes not foreseen at the outset or that could have appeared with the evolution of the market may not be compliant with the transparency principles of the GDPR, and the obligations of privacy by design and should be avoided.

4.2 How do such considerations change depending on the nature of the entities involved?

The Spanish Data Protection Agency (*Agencia Española de Protección de Datos*) has a clear tendency not to give as much relevance to whether it is a public or private entity for the purposes of the GDPR (for example, for the application of different legal bases of the processing). However, in Spain, public entities (strictly speaking) are not fined for not complying with the GDPR, whereas private entities are, so private entities always have certain incentives to comply more scrupulously with the GDPR.

4.3 Which key regulatory requirements apply?

When using personal health-related data, appropriate safeguards are required. These include, for example: (i) correctly identifying the purposes for which the personal data is going to be processed and only processing personal data that is strictly necessary for the identified purposes (data minimisation); (ii) applying the privacy-by-default and privacy-by-design principles; (iii) conducting a privacy impact assessment and analysis of the risks for the rights and freedoms of the data subjects prior to the processing of data; (iv) guaranteeing the confidentiality, integrity and availability of the personal data processed; (v) anonymising personal data or, at least, pseudonymising the same and prohibiting third parties with whom personal data may be shared from reverting the pseudonymised data; (vi) obtaining separate consent for each purpose; (vii) providing clear information to data subjects, using plain language and providing information about the identity of the data controller, and specifying whether personal data is shared and with whom and if it will be re-used and for which purposes; (viii) designing user-friendly settings options, so that data subjects can easily decide whether they want to share personal data or not; and lastly (ix) taking into account that profiling is only permitted under very specific circumstances and, if done, explicit consent of the data subject needs to be obtained.

Pursuant to art. 37 of the GDPR, the controller and the processor shall designate a data protection officer in the following events. In addition, art. 34.1 l) of the Spanish Data Protection Act (*LOPDGDD*) complements the provisions of the GDPR and stipulates that healthcare facilities must appoint a Data Protection Officer (there are some nuances and exceptions but this is the general rule). Digital health providers should generally process personal health data on a large scale, and therefore they will be obliged to designate a data protection officer too.

In addition to the above, other regulatory requirements, which stem from the processing of personal health data, are the following: (i) regardless of the size of the entity, the controller, or, if applicable, the processor who processes health data on behalf of the controller, shall keep a record of processing activities pursuant to art. 30 of the GDPR; and (ii) by default, when there is large-scale processing of health data, the controller shall carry out a data protection impact assessment pursuant to art. 35.3 of the GDPR.

4.4 Do the regulations define the scope of data use?

The regulation prevents almost no use, but establishes strict "procedural" rules on how to manage this issue. The purposes must be clearly communicated to the data subject (the physical person to whom the personal data refers) and very rarely can this rule be waived. Often the difficulty arises when the entity thinks of purposes not foreseen up to that moment with personal data it already has at its disposal. In addition, the legal bases issue is mixed with this problem; for example, if the purpose of the processing is medical assistance, consent may not be necessary, but it may be required for medical research (although in Spain, in fact, more and more work is being done to carry out medical research with bases of legitimacy for processing other than consent).

4.5 What are the key contractual considerations?

(a) Privacy contractual considerations with data subjects (users) in apps: according to the Spanish Data Protection Agency's guidelines, information with regard to the processing of personal data (privacy policy) must be available both in the application itself and in the application store, so that the user can consult it before installing the application or at any time during its use. The language used in the privacy policies must be clear, taking into account the target user of the application. For example, applications available in Spanish and therefore aimed at Spanish-speaking users must provide the privacy policy in Spanish. In addition, the permissions that the application can request for access to data and resources should be indicated in the privacy policy. For example, it must explain if the application will process personal data only when it is being used by the user in the foreground or also when it is running in the background.

(b) Privacy contractual considerations with data processors (normally, providers): the processing by the processor shall be governed by a binding contract that sets out the subject matter and duration of the processing, its nature and purpose, the type of personal data and categories of data subjects and the obligations and rights of the controller; the security measures; and that the data processor can only process the personal data according to the data instructions of the data controller, etc.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

In recent years, there has been a lot of controversy about the transparency of information and, for example, whether data subjects were sufficiently well informed about each differentiated processing for which differentiated purpose and on what differentiated legal basis (for example, the emphasis has been on "unbundling" consents and purposes). Aspects related to the legal basis other than consent have also generated a lot of interest (both in sanctions and in reports of the Spanish Data Protection Agency analysing it, for example, in the field of medical research). Security measures, the need for privacy impact assessments, etc. have also been much discussed and lately there is a growing interest in data minimisation in all areas.

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

It is worth highlighting the role of the Spanish Data Protection Agency, which is responsible for publishing guides, reports and other documents on how personal data should be processed by companies and public administrations.

In both cases, guidelines are offered that provide support and enable the needs of the public and private sectors to be met with regard to the correct processing of data. It also provides resources and tools to facilitate compliance with the GDPR. Finally, it is also possible to consult the Agency on the application of the data protection regulation.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

Especially the problems of (i) "hallucination" (a computer science term referring to when the AI "makes things up" and even denies having done so); (ii) deduction of personal data of all kinds (which cannot always be expected to be deduced); and (iii) the problems of explainability of AI reasoning (especially if used in a way that involves automated decision making). Also problematic is the access and commercialisation of data sets to train such AI. For the time being, the Spanish Data Protection Agency has been harsh on some occasions in terms of sanctions but, for example, there are indications that it is open to interpretations of the GDPR that favour medical research in this type of project. We will have to see how the situation evolves and be especially attentive to possible sanctions that may be even more focused on these aspects than it has been so far.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

The main issue when sharing personal data in the context of digital health is that it is a market with many different players (app developers, device manufacturers, app stores, etc.). As the European Data Protection Supervisor established in its Opinion 1/2015 on Mobile Health, this makes it difficult to identify which parties act as data controllers or processors and to ensure an appropriate allocation of responsibilities, as well as ensuring user empowerment.

Therefore, it is important to respect the principle of transparency and accountability and the information requirements of art. 13 of the GDPR.

Moreover, in order to meet the obligations of privacy-by-design, it is important to clearly identify the different operators that will take part in the processing and to design the structure of all data processing activities accordingly. The above-mentioned Opinion states that data subjects should be given the option to freely allow the sharing/transfer of personal data to a third party, which is linked to the obligation of privacy-by-default, i.e. that the default features of the applications limit the types of processing to what is strictly necessary for the purposes of the application and/or device.

5.2 How do such considerations change depending on the nature of the entities involved?

Public authorities, unlike individuals, may transfer personal data concerning health without the consent of the data subjects, if it is necessary for the performance of a task carried out in the public interest or in the exercise of public authority and as long as it has a competence conferred by law.

According to the Spanish Data Protection Agency, if a certain processing is not "necessary" for the fulfilment of the mission carried out in the public interest or in the exercise of public powers conferred by law, such processing would lack a sufficient legal basis and would also infringe the principle of minimisation of data, which is also applicable to data processing carried out by public authorities.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Private entities may only share personal data if the data subject has provided their consent or other legal bases of the GDPR allow it. There is also a legal obligation to transfer personal data that is essential for making decisions in public health to

the health authorities. Transfers of data directed to territories outside of the EEA seem very likely in the field of digital health services; the provider may need to obtain an authorisation or alternatively to prove that the country of destination has been subject to a decision of adequacy by the European Commission or establish adequate safeguards conferring legal rights and remedies, such as conducting a Transfer Impact Assessment and enter into Standard Contractual Clauses with the data importer or relying on binding corporate rules, among other options.

In Spain, in the pharmaceutical sector the Spanish Data Protection Agency has approved the "Code of Conduct Regulating the Processing of Personal Data in Clinical Trials and Other Clinical Research and Pharmacovigilance Activities" of the industry association Farmaindustria. Adherence to the code is voluntary, but includes a modern interpretation of the GDPR with fresh legal solutions to sharing this type of data.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

Yes; in Spain, the Spanish Data Protection Agency encourages and promotes public reporting on these projects and it has published a guidance document. Together with the European public cybersecurity agency (ENISA), it has held forums on the subject that have also served to raise the visibility of private and public initiatives in this regard.

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

The "federative model of shared data space" refers to a way of organising those environments in which several entities or organisations collaborate to share data in a decentralised environment. In this model, each entity maintains some control over its own data, but there are agreements and standards in place to facilitate interoperability and information sharing among them. Instead of centralising all data in one location, the federative model allows collaboration and access to distributed data, while respecting the policies and regulations of each participant (as long as they do not contradict the common agreements and standards that allow the existence of the environment itself). The legal entity (for example, an association or a consortium) organises these arrangements.

The data space should have defined governance and information management obligations in a distributed environment. This must be grounded in organisational, legal and IT technical measures. At the legal level, we would recommend, for example, that all relevant stakeholders participating in federative healthcare data sharing adhere to a set of contractual rules that include the possibility of performing prior privacy assurance checks (similar to what must be done with data processors) and audits on the different stakeholders.

6 Intellectual Property

6.1 What is the scope of patent protection for digital health technologies?

The technologies involved in digital health may include medical devices, software and algorithms. AI and machine learning technologies are based on computational models and algorithms.

According to art. 4.4 of Law 24/2015 of 24 July 2015 on patents (Spanish Patent Act), computer programs, mathematical methods, plans, rules and methods for the pursuit of intellectual activities, for games or for economic and commercial activities and ways of presenting information, may not be patentable.

Therefore, the AI and machine learning solutions *per se*, which are essentially software, i.e. a mathematical method, are not patentable. However, AI-related inventions having a technical character would be patentable, since the patent would not relate to a mathematical method as such.

6.2 What is the scope of copyright protection for digital health technologies?

According to the Spanish Copyright Act, protection is granted without requiring the fulfilment of any kind of formality, i.e. it is not necessary to register the work before any office. In Spain, the registration is merely for evidentiary purposes.

Copyright is the most common way to protect software. In this regard, art. 10(1)(i) of the Spanish Intellectual Property Act expressly foresees that computer programs are protected by copyright.

With regard to AI solutions, which allow operators to process, analyse and extract useful information from huge data sets, according to art. 12 of the Spanish Copyright Act, these data sets could be copyright protected as data compilations.

6.3 What is the scope of trade secret protection for digital health technologies?

Law 1/2019, of 20 February 2019 on Trade Secrets defines trade secrets as any information relating to any area of the company, including technological, scientific, industrial, commercial, organisational or financial, which is secret in the sense that it is not generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question, its secrecy has commercial value and it has been subject to reasonable steps to keep it secret.

Trade secrets protection may be the only current existing option for protecting algorithms that are not patentable.

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

The Spanish Organic Law 6/2001 on Universities regards technology transfer as one of the main functions of universities. This law also facilitates the involvement of professors in university spin-offs, for example temporary leaves of absence. In turn, the Spanish Law 14/2011 on Science, Technology and Innovation governs basic aspects of the technology transfer process, for example, the application of private law to transactions between universities and companies.

Results of academic technology are generally transferred or licensed to third parties through invention assignments or licence agreements, respectively, or as a result of the creation of a spin-off company. Universities and public research centres must follow specific state regulations providing protection regarding the ownership of the creations, and are required to follow internal protocols that set out the terms for cooperation between university personnel and private entities. According to Law 14/2011, researchers shall in any case be entitled to share in the profits from the exploitation or assignment of their rights to such inventions obtained by the entities for which they provide their services.

On 6 September 2022, the new Law 17/2022, of 5 September, amending Law 14/2011, of 1 June, on Science, Technology and

Innovation was published. This law regulates further incentives for academics to bring their research to market, or to create start-up companies building on research outcomes. In this sense, Communication 2022/C 414/01 of the European Commission provides guidelines for ensuring adequate compensation for public universities and public research organisations in their contracts with companies, which has a direct impact on the criteria for the preparation of budgets and intellectual and industrial property rights.

6.5 What is the scope of intellectual property protection for software as a medical device?

Although the Spanish Patent Act expressly excludes the patentability of "computer programs", it seems to admit the possibility of patenting computer applications incorporated in patented hardware.

Another alternative to protect software would be through the Spanish Copyright Act, which expressly foresees the protection of computer programs. However, the protection granted by copyright is not as strong as patent protection, since the software will not be protected against the development of other programs meeting similar needs.

Other potential ways of protecting software are using trade secrets, as well as trademarks legislation. However, regarding trade secrets, competitors may try to reverse engineer the software and it is key that reasonable steps are taken to keep it secret (such as signing non-disclosure agreements and prohibiting reverse engineering in licensing agreements).

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

The Spanish Patent Act does not mention the condition that the inventor must be a natural person. However, the Guidelines published and followed by the Spanish Patent and Trademark Office for the examination of Spanish patent applications specifically establish that "only natural persons can be designated as inventors, and never, legal persons". Taking also into account that the understanding of the term inventor as referring to a natural person appears to be an internationally applicable standard, at this moment it is not possible for an AI device to be named as an inventor of a patent since the inventor must be a natural person in Spain.

The same is applicable at European level. Although there is no express provision in the European Patent Convention (EPC) which states that the inventor must be a natural person, it recognises moral rights to the inventor and contains references to the inventor being a natural person. In that regard, in 2018 two patent applications in which the inventor was an AI system, referred to as DABUS, were filed before the European Patent Office (EPO). It rejected the application on the grounds that they do not meet the legal requirement of the EPC that an inventor designated in the application must be a human being, and not a machine. The decision has been confirmed by the Board of Appeal of the EPO.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

Government-funded inventions in Spain fall within the general regime for inventions, which includes the Spanish Patent Act, Royal Decree 316/2017 approving Regulations for the implementation of the Spanish Patent Act, and Orders ETU/296/2017 and ETU/320/2018. In addition, Royal Decree 55/2002 on the exploitation and transfer of inventions made in public research bodies sets, specifically, the ownership regime that must rule the inventions created by research staff working for several Spanish research agencies, such as the Spanish National Research Council and the Carlos III Health Institute.

7 Commercial Agreements

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

The FENIN has a Code of Ethics which includes minimum principles to which its members must adhere when entering into collaboration agreements with healthcare professionals. The main requirements are that a legitimate need for the services must have been identified beforehand, that the agreements must be documented in writing, all conditions should be agreed on market terms and be transparent, which means that the agreement should be notified in advance to the employer and that any publication or presentation of results will need to mention the collaboration.

Collaboration agreements should address confidentiality, ownership of the results, publication rights and adherence to ethical rules.

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

Any agreement with non-healthcare companies needs to include an express commitment by the non-healthcare company to adhere to the ethical rules to which the healthcare company adheres, in addition to the usual provisions regarding ownership of results, confidentiality and publication rights.

In the event that the digital health solution under development will need to be approved as a medical device, the agreement should address regulatory matters in order not to jeopardise approval.

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

As mentioned above, the data space should have defined governance and information management obligations in a distributed environment. This must be grounded in organisational, legal and IT technical measures. At the legal level, we would recommend, for example, that all relevant stakeholders participating in federative healthcare data sharing adhere to a set of contractual rules.

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

The key legal aspects to be included in the contracts are: liability; non-authorised use of AI; requirements for the uses of the authorised use of AI (for example the need for human medical intervention or IT minimum requirements); privacy issues; cybersecurity; sharing information; IP considerations, Service Level Agreements and other classical elements of the IT contracts; and the obligation to share incidents related to the service, etc.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning can be used for the prediction of population health risks, enhancing health information management, quick and accurate diagnosis of conditions that are difficult to uncover or, for example, providing early health information to patients.

8.2 How is training data licensed?

Before licensing training data, it is vital to determine if personal data is involved, in which case the enhanced data protection principles apply.

Before licensing any data, the machine learning providers should obtain sufficient information about the provenance of the data, ascertain whether the data controller has collected the data in compliance with the law, and whether they have sufficient permissions to apply the data in the training.

The agreement should further foresee the scope of permitted use of the licensed data and allocation of developed and derived data.

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

As mentioned above, it is very difficult for an algorithm to be protected by IP rights (if at all as a trade secret), so its improvement (even if it is not produced by machine learning) is also unlikely to generate any IP rights.

The automatic learning algorithms learn from the information provided by their programmers and from there, they generate new works through a series of independent decisions, which may result in learning new methods or the creation of new algorithms and models.

In Europe, the European Court of Justice has stated on several occasions, notably in its landmark Infopaq decision (case C-5/08, *Infopaq International A/S v. Danske Dagblades Forening*), that copyright only applies to original works and that originality must reflect the "author's own intellectual creation". This expression is generally understood to mean that an original work must reflect the author's personality. This can be interpreted to mean that there must be a human author for a copyright work to exist. In this case, the discussion is if it could be the programmer (or the company who hired him/her) who owns the IP rights.

If the machine learning process can be sufficiently described and put into use in a technical context, the subject matter could also fall within the patentable domain.

In this context, it is of vital importance that the parties involved in the machine learning process, generally at least the AI/machine learning provider and the provider of the data set used to teach the algorithm, must foresee beforehand in their contractual terms not only how the data input and resulting data can be used, but also how these data are going to be allocated and who will own the IP rights, such as trade secrets and patents, to the developed, clinical or derived data.

8.4 What commercial considerations apply to licensing data for use in machine learning?

The foremost consideration in the licensing of data for their use in machine learning is the protection of personal data, due to the sensitivity of the data involved. The parties should address the provenance of the data and check that the necessary permissions to use such data are in place.

The correct allocation of IP rights under licensing contracts is also of the utmost importance in order to protect the parties and to secure the commercial viability of the project. Typically, it should be considered and foreseen beforehand who owns the background IP and the IP developed based (in part) on the other party's data, who owns and under what conditions the results and derived data may be used, and if there are any specific allocations, for example, for specific categories of data or assets.

9 Liability

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

The GLPCU imposes strict liability for personal injury or material damage that is caused by a defective product. The manufacturer of a product or an "own brander" (i.e. someone who, by putting their name, trademark or brand on a product, holds themselves out as the manufacturer) are primarily liable for defective products under the GLPCU.

The GLPCU will only apply to an algorithm or a solution if they are considered to be "products". In this regard, there are precedents of the Spanish High Court declaring that a software is considered a product.

This area is under review by the EU regarding AI. The European Commission has adopted a Proposal on adapting non-contractual civil liability rules to AI, published on 28 September 2022. This Proposal highlights the establishment of common rules on the disclosure of evidence on high-risk AI systems so that plaintiffs can substantiate their fault-based liability claims; it also eases the burden of proof for damage caused by an AI system and establishes a presumption of causation for cases where there is a causal link between the AI system and the damage.

9.2 What cross-border considerations are there?

Suppliers (if they were aware of the defect) and importers of the defective product in the EU can also be liable. Liability is joint and several in the event that there are different potential liable parties. In the specific case of medical devices, Spanish Royal Decree 1591/2009 regulating medical devices rules that manufacturers who are not established within the EU shall designate a single authorised representative within the EU, both the manufacturer and the EU representative may be liable.

9.3 What are best practices to minimise liability risks posed by the use of generative AI in the provisioning of digital health solutions?

Regarding legal measures, the uses that are permitted and those that are not permitted should be very clearly stated in the agreement. In addition, what the AI can do and what it cannot

do should also be stated by contractually remarking the need for human supervision (for example, to detect the aforementioned hallucinations, see question 4.8) and the fact that if the AI receives bad information and bad feedback it will also integrate it. Therefore, if these indications of quality of information and feedback are not followed, a bad result shall be generated for which the AI shall not be responsible (for example, biases can be generated, including discriminatory biases). In addition, there are aspects of data protection that, if well regulated, shall avoid being penalised for breaches of the data privacy obligations generated by the other party. Finally, the limitation of liability clauses (with a quantitative approach and concept of liability) are also important, especially if the dispute ends up in litigation procedures.

10 General

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

Hospitals and healthcare professionals are increasingly relying on Cloud-based services to store information related to patients and to make it accessible. Challenges in this area are the protection of personal data, prevention of cyberattacks and IT contract issues.

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

Regulation remains an important issue. Whether the digital health solution will require approval as a medical device has to be assessed from the outset through a risk classification of the product and this will affect the product development cycle. Non-healthcare companies will need to factor in longer product development cycles than for non-healthcare digital offerings.

Reimbursement strategies and developing a sustainable business model are becoming increasingly important. Non-healthcare companies need to understand the clinical problems they want to address and whether payers will see a value in it.

The healthcare provided in Spain is predominantly public. Therefore, the importance in gaining acceptance by public healthcare authorities also needs to be considered, in particular, when the digital health solution satisfies an unmet and clearly identified need.

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 understanding the business model, clarifying the regulatory and market access issues and the positioning of the product, and the specific revenue model, including potential reimbursement.

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

Key barriers preventing widespread clinical adoption of digital health are not so much regulatory as they relate to organisational, budgetary or cultural reasons. The COVID-19 pandemic has been a turning point. The Digital Spain Plan 2025 identifies the following fields of action to increase the efficiency and quality of public healthcare services in Spain: (i) research to measure and improve health outcomes and to design preventive systems; (ii) support to patients in order to automatise and provide them with tools to be better informed in making health decisions; (iii) patient empowerment with telemedicine, self-diagnostic or enhanced accessibility tools; and (iv) streamlining of information systems to enable better data sharing and interoperability.

Leaving aside the prevailing attention to digitalisation of information, digital health solutions such as mHealth are not generally present in the clinical practice because they have not been generally incorporated in the public National Health System and therefore are not financed.

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?

Certification initiatives are mainly coming from the public sector rather than physician associations. We are not aware of any formal requirement of endorsement by physician certification bodies in Spain in order to introduce digital health solutions into clinical practice. Note, however, that some regional health authorities have accreditation and/or certification systems in place for mobile applications (mHealth). They award accreditations and/or include them in repositories of accredited apps for use in the regional public health system (Healthcare Quality Agency of Andalusia with the Distintivo AppSaludable (seal of quality) and Catalonia's TIC Salut Social and iSYS Score). Such accreditations are a driver for clinical adoption.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

There is no specific reimbursement process for digital health solutions within the Spanish health system. Spanish patients, when treated by the National Health System, receive all healthcare products and treatments included in the list of health benefits of the National Health System (Royal Decree 63/1995). Digital health solutions can be incorporated by the National Health System or by regional authorities, so that patients can benefit from them without charge. In this regard, each autonomous community may decide to incorporate digital health solutions that qualify as medical devices to their healthcare services. Regarding telemedicine, within the National Health System, it is provided by the National Health System professionals and, therefore, does not need a reimbursement process.

Any medical consultations outside of the National Health System are not reimbursed, whether in person or via telemedicine, unless they are provided under an agreement between the services provider and the National Health System.

10.7 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 Ministry of Health approved in December 2021 the Digital Health Strategy of the National Health System. This strategy seeks to maintain a good level of citizens' health along with the improvement of the public health system by adapting it to the digital world.

The following objectives may be highlighted: the empowerment and involvement of people in their health care; the generation of valuable processes to improve the public health system; the adoption of data management policies to have interoperable and quality information; and the application of innovation and focus on 5P healthcare policies (People, Prevention, Predictable, Personalised, Participative) to adapt the National Health System to current needs.

Montserrat Llopart Vidal is a Partner in the International Commercial & Trade department and leads the Healthcare and Compliance Law practices in the Baker McKenzie Barcelona office.
She is a regular speaker and contributor to specialist conferences and publications, and she is recognised by the leading legal directories such as *Chambers and Partners*, *The Legal 500* and *Best Lawyers* and in the *InspiraLaw* Top 50 Women's List for Spain and Portugal.
Montserrat is the former head of Baker McKenzie's Barcelona office and the Firm's pharmaceutical law group in the EMEA region.

Practice Focus

Montserrat assists healthcare companies throughout the lifecycle of healthcare products, from R&D to commercialisation and more specifically in the areas of clinical trials (agreements, regulatory procedures, processing of personal data), market access (pricing and reimbursement), products and companies regulations, commercial relations between healthcare industries (distribution, (co)promotion, manufacturing, supply, licensing, partnership agreements), relations with healthcare professionals and/or patients including compliance communication & advertising, e-health (connected devices, telemedicine, hosting of health data) and product liability. Her practice encompasses both advisory and litigation matters.

Baker McKenzie
Av. Diagonal, 652
Edif. D, 8th Floor
Barcelona 08034
Spain

Tel: +34 93 206 0820
Email: montserrat.llopart@bakermckenzie.com
LinkedIn: www.linkedin.com/in/montserratllopart

David Molina Moya is a Senior Associate and Head of the Data Protection and Digital Law Service in the Barcelona office. For 10 years, David has provided legal advice on all types of digital projects for all types of sectors, focusing especially on aspects of personal data protection, technological contracting, copyright, legal protection of software and e-commerce. He also participates in M&A operations in which high-value intangible assets are involved and has also intervened in administrative and judicial procedures and arbitration of conflicts with a strong technological component. Despite working in all types of sectors, he has done so especially in the health, automotive, infrastructure, mass consumption and real estate sectors.
David is a member of the Bar Association of Barcelona (ICAB), the ESADE Business Innovation & Technologies Club and the Spanish Professional Privacy Association (APEP). Before devoting himself to law, he was a full-time university professor at the Pompeu fabra University (UPF) at just 23 years of age.
David is certified by the British Standards Institution (BSI) in ISO 27001 (information security means from a technical point of view) and in ISO 27701 (management, security and legal measures related to compliance with information regulations of privacy).

Baker McKenzie
Av. Diagonal, 652
Edif. D, 8th Floor
Barcelona 08034
Spain

Tel: +34 93 206 0820
Email: david.molina@bakermckenzie.com
LinkedIn: www.linkedin.com/in/david-molina-moya-62647151

Switzerland


Tobias Meili


Carlo Conti


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 technologies in your jurisdiction?

Widespread use of telemedicine: Telemedicine solutions enjoy an extensive presence and are widely recognised in Switzerland. For instance, the largest medical telemedicine centre 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. 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 ensure 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) and the general public. 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 revision to mandate all healthcare providers to use the EPR.

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 be permitted 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 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 are the core legal issues in digital health for your jurisdiction?

If a digital health technology classifies as a medical device, it must satisfy the criteria outlined in the TPA. However, this law establishes the fundamental principles governing the authorisation, monitoring and labelling of such products only in a general manner. Various other laws and ordinances at federal and cantonal level, the application of which rely on the intended area of use of digital health technology, detail these general requirements (see questions 2.1 *et seq.*). The large number of regulations to be observed make the regulatory requirements quite complex.

Furthermore, digital health technologies (such as the EPR) must comply with the provisions of the Swiss Federal Act on Data Protection (FADP). Especially in health matters, it should be noted that data relating to health, genetic and biometric data represent sensitive personal data (Art. 5(c)(2-4) FADP). To process such data, the explicit consent of the data subject is required (Art. 6(7)(a) FADP).

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

The Swiss market for digital health products and services is expanding rapidly. Diverse 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 (see: https://www.mckinsey.com/ch/~/media/mckinsey/locations/europe%20and%20middle%20east/switzerland/our%20insights/digitization%20in%20healthcare/digitalisierung%20im%20gesundheitswesen%20%20die%2082mrdchance%20fr%20die%20schweiz%20de.pdf) assumes that the potential for utilising digital health in Switzerland amounts to around CHF 8.2 bio.

1.5 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 also important players on 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.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The core principles are outlined in the TPA which refers to medicinal products and medical devices as "Therapeutic Products". 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.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

In addition to the TPA, the data protection requirements of the FADP (see question 1.3) and the requirements of the EPRA must be complied with as part of the implementation of the EPR (see question 1.2). Economic considerations, as well as cost control and affordability of digital health technology, are dealt with by the Federal Health Insurance Act (HIA). The cantonal health laws, of which there are 26, might also apply to digital health technology. Furthermore, other regulatory schemes, such as the Federal Product Safety Act, the Federal Foodstuff and Utility Articles Act, the Federal Cartel Act, the Federal Unfair Competition Act (UCA) and IP legislation may apply, depending on the circumstances.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Although a distinct national framework for "consumer healthcare devices" does not exist, several laws and regulations do apply to such items (see questions 2.1–2.2). Both the TPA and the MedDo explicitly state that software may qualify as a medical device if used for medical purposes (Art. 4(1)(b) TPA & Art. 3(1)(c) MedDO).

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

In Switzerland, the FOPH is by default the competent authority for all public health aspects, unless the cantonal 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 & 82 TPA).

2.5 What are the key areas of enforcement when it comes to digital health?

If digital health technologies or products do not comply with the provisions of the 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 (Art. 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).

2.6 What regulations 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, 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 personal data 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.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

See question 2.6 above.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care:** Telemedicine and virtual care 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, Mobile Apps, Virtual Assistants (e.g. Alexa):** Wearables, mobile apps and virtual assistants can collect and process personal health data; therefore, they 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.
- **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 8.1–8.3.
- **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, as well as 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: while this technology raises significant concerns regarding data protection, the purpose of a medical treatment using big data may only be achieved through transparency. Furthermore, there may be situations where legal requirements are in direct opposition to one another.
- **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 manufacturers explicitly designate it for medical use. Moreover, adherence to data protection requirements may be necessary.

3.2 What are the key issues for digital platform providers?

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 authority 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 to consider for use of personal data?

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 penalties.

4.2 How do such considerations change depending on the nature of the entities involved?

The FADP distinguishes between private 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.

4.3 Which key regulatory requirements apply?

The general data processing principles apply (see question 4.1).

As stated, the FADP provides for several obligations of data processors. In particular, the data controller is required to fulfil information obligations when collecting personal data and when using automated individual decision-making processes. Further, the data controller must implement appropriate technical and organisational measures and ensure privacy-friendly settings. Subject to certain exceptions, a data controller is obliged to maintain a record of data processing activities. Also, under certain circumstances, the data controller must conduct data protection impact assessments and report breaches of data security. Additionally, the data controller must ensure the data subjects' rights.

4.4 Do the regulations define the scope of 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 controller must (a) anonymise the 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 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 data only for non-personal purposes, and (c) publish the results in a way that prevents the identification of the data subject.

4.5 What are the key contractual considerations?

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 processor, it is necessary to establish a written data processing agreement (DPA). For joint controllers or independent controllers, a contractual agreement is not mandatorily required, unlike under the EU GDPR. However, it might 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 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Swiss law does not recognise any proprietary rights to personal data. However, the FADP grants data subjects the right to request and obtain information from the data controller on whether personal data relating to them is being processed. Also, the FADP provides for a right to data portability, subject to certain conditions.

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

The principle applies that only accurate data may be processed. Every data subject has the right to have inaccurate 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 an automated decision, the 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 be reviewed by a natural person.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

Currently, there are no specific legal or regulatory issues in Switzerland that pertain exclusively to generative AI companies. However, the Federal Council (i.e., the Swiss government) is examining regulatory approaches to AI, suggesting that there may be potential legal and regulatory challenges ahead.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

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 secrecy), 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 secrecy, 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. Data may only be transferred to countries that offer 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 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 do such considerations change depending on the nature of the entities 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 question 4.4). 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 refuse 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

When it comes to processing (including sharing) of health data, often the consent of the data subject is necessary (see questions 5.1 *et seq.*).

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

A project called "DigiSanté" aims to promote digitisation in the healthcare sector and facilitate the seamless exchange of health data. To achieve the digitisation, strategies are being developed in the period 2023–2024, which will be implemented in stages starting in 2025.

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

The restrictions imposed by applicable Swiss data protection legislation apply.

6 Intellectual Property

6.1 What is 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). Computer-implemented inventions, that solve a technical problem, are patentable.

6.2 What is the scope of copyright protection for digital health technologies?

The Swiss Federal Copyright Act (CopA) protects literary and artistic intellectual creations with individual character, irrespective of their value or purpose. Computer programs are explicitly defined as copyright-protected works. Digital health software can therefore be protected by copyright if the requirements are satisfied. 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 What is the scope of trade secret protection for digital health technologies?

Trade secrets are protected by provisions of the UCA and Criminal Law. 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 What is 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?

In principle, only individuals can be considered inventors. However, there is currently a debate in Switzerland regarding whether it is necessary for an inventor to be a natural person.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

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.

7 Commercial Agreements

7.1 What 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. As a starting point, the involved parties must 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 IP rights be protected. Additionally, publication rights, marketing rights, regulatory responsibility and product liability ought to be contractually agreed upon.

7.2 What 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 questions 2.1 *et seq.*), particular attention should 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 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 machine learning 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 considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

See questions 8.1–8.3 and 9.3.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning is a sub-discipline of AI and describes an automated process (learning process) for the continuous enhancement of an application. Switzerland's digital health sector is significantly and dynamically influenced by machine learning, which is utilised in numerous research projects. Various domains are encompassed by the application of machine learning in digital health in Switzerland, which contributes to the enhancement of healthcare management, personalised medicine, treatment planning and diagnostics.

8.2 How is training data licensed?

In general, training data licensing ought not to be regarded differently from that of other types of information or data: if the training data constitutes an original work of literature or art, it may qualify as protected intellectual property under the CopA. Compilations of pure facts that possess individual characteristics may qualify as collected works (Art. 4 CopA) if they express individual characteristics. Thus, the training data are licensable in the same manner as any other copyright.

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

Intellectual property may only be created by a natural person

(i.e., a human) in accordance with Swiss copyright and patent law (Art. 6 CopA; Art. 3(1) Patent Act). As a result, advancements achieved through machine learning without explicit human intervention do not qualify as inventions protected under Swiss IP 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 an algorithm.

8.4 What commercial considerations apply to licensing data for use in machine learning?

When procuring data for machine learning, it is crucial to consider significant commercial factors. These include, but are not limited to: i) establishing data ownership and IP 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 machine learning in digital health technologies may potentially involve sensitive personal data, which raises several obligations under the FADP (see question 1.3).

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).

Violation of the reporting obligation primarily triggers criminal law consequences (Art. 87(1)(c) TPA). However, civil liability may also be triggered 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 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 might 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 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.

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 1.3). 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 questions 2.3 and 2.6).

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 intended business model and the intended products and/or services. A comprehensive compliance organisation considering the aforementioned factors, among others, should be established prior to the entry of non-healthcare companies into the digital healthcare market. Ultimately, it might be useful to evaluate 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 are the key barriers holding back a wider use of digital health solutions in Switzerland. In addition, Switzerland is a federal state composed of 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 Swiss Medical Association (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 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with 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 (see question 2.2). 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 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 already mentioned, the evolution of Swiss regulatory (digital) health policy is to be seen in conjunction with the one of the EU. 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 impacted by EU regulatory developments.

Tobias Meili is a partner in the Corporate and Commercial Law, Life Sciences and Health Law practice groups and on the IP and IT team. He advises clients in the areas of corporate and commercial law, corporate governance (including responsible business conduct matters), mergers and acquisitions and contract law. In addition, he provides support to our clients in the areas of data protection and IT law.
Due to his extensive experience as a private practitioner, as well as an inhouse counsel in senior roles (Accenture; Syngenta), he combines an authentic, pragmatic and solution-oriented approach to giving advice with solid legal expertise and skills as a negotiator.

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

Carlo Conti is an of counsel in the Life Sciences and Health Law practice group. He advises institutions and organisations on questions of life sciences and health law and on matters of governmental and administrative law. He is a member of a number of boards of directors.
He has many years of professional experience and deep knowledge of all areas of life sciences and health law, as well as governmental and administrative law. He held executive positions in the pharmaceutical industry for more than 15 years. Carlo Conti then served as a member of the State Council for the Basel-Stadt Canton where he was 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 and vice-chairman of the agency council of Swissmedic.

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/specialists/17/conti-carlo

Martina Braun is an of counsel and a member of the IP and IT team. She advises and represents companies, foundations and individuals on all aspects of IP law and IT, with a particular focus on copyright, trademarks and data protection. Her key area of expertise is advising on contract law. She specialises in particular in licensing and sponsorship agreements in the sports and entertainment sector. She also deals with various questions related to personality rights.
Martina Braun completed her doctoral thesis on copyright law and recently completed a CAS in international sports law.

Wenger Plattner
Seestrasse 39
P.O. Box, 8700 Küsnacht-Zürich
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 an associate and mainly deals with commercial law and various regulatory matters. His primary practice areas consist of life sciences and health law, competition law and general contract law. Furthermore, he advises companies and organisations on matters pertaining to Swiss corporate and commercial law and administrative law, as well as EU law. He regularly publishes in his fields of expertise.

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

Taiwan


Hsiu-Ru Chien


Eddie Hsiung


Shih-I Wu

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 Taiwan 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. In this 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. However, the medical device software of AI or ML technology shall be subject to the approval of the central governmental authority in charge of the subject industry.

In general, "digital health" should cover areas such as mobile medicine (mHealth), medical health information (Health IT), wearable devices, telehealth and telemedicine, personalised medicine, and other applications of information and communication technology (ICT) in the medical and health fields.

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

Based on Taiwan's complete semiconductor and ICT industry supply chain, cross-border integration of medical technologies, as well as innovative digital health technologies such as healthcare big data, IoT, AI and 5G technology, biomedical chip technology, sensors, wearable devices, biobanks, telehealth and telemedicine are being invested, created and developed in various fields and industries, and also by government organisations.

1.3 What are the core legal issues in digital health for your jurisdiction?

With respect to digital health in the context of a medical device, it is subject to regulations under the Medical Devices Act, which took effect on May 1, 2021. The term "medical device", as defined in the Medical Devices Act, shall refer 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 Taiwan legal perspective, the manufacturing or importation of medical devices may be conducted only after a medical device permit licence that grants registration and market approval is issued by the government authority.

Personal data protection is also a critical issue where any personal data is to be collected, used or processed in the course of providing any digital health products or services.

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

There are no official statistics concerning the digital health market size in Taiwan. Nonetheless, according to the estimated data of 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 to reach NT$14.2 billion (around US$490 million) in 2025, with a compound annual growth rate of 10.2%; the growth rates for digital health, precision medicine, and regenerative and immunomedicine composites were estimated to be about 11%, 11.5% and 4.8%, respectively. According to the public information on the achievements of the Executive Yuan, digital medical industry revenue has seen growth of over 10% in recent years, reaching NT$50.2 billion (around US$1.7 billion) in 2022.

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

In Taiwan, the digital health market is mostly invested in by major electronic technology companies. The revenue of these companies is calculated on the basis of the overall enterprise, so it is difficult to distinguish their revenue or rank with respect to the digital health field.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

The Medical Devices Act provides for core regulations governing medical devices.

As indicated under question 1.3, the manufacturing or importation of medical devices is only permitted after a medical device permit licence that grants registration and market approval is issued by the Ministry of Health and Welfare (MOHW).

Medical device manufacturing must comply with the guidelines set forth in the Good Manufacturing Practice (GMP) under the Pharmaceutical GMP Regulations.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

Depending on the issues involved, the following laws and their related regulations apply:

- The Personal Data Protection Act (PDPA).
- The Physicians Act.
- The Consumer Protection Act.
- The Civil Code.
- The Telecommunications Act.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

The Consumer Protection Act and the Civil Code are the main laws providing for the relevant consumer rights and product liabilities. The manufacturing and sale of consumer devices should also follow the regulations under the Commodity Labelling Act and the Commodity Inspection Act.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

The MOHW is the competent authority responsible for supervising healthcare-related matters, products and industries. The MOHW has a broad mandate to improve the quality of healthcare.

Under the MOHW, the Food and Drug Administration (TFDA) is responsible for regulating the system for the safety and quality of food, drugs, medical devices and cosmetics. The TFDA grants product registration and clinical trial approvals, monitors manufacturing and importation, and conducts safety surveillance activities on health-related products.

2.5 What are the key areas of enforcement when it comes to digital health?

The Medical Devices Act outlines a three-tier risk-based classification system for medical devices: Class I products with low risk; Class II products with medium risk; and Class III products with high risk.

Additionally, any person who manufactures or imports medical devices without the required prior approval may be subject to imprisonment for not more than three years and may, in addition thereto, be imposed with an administrative fine of not more than NT$10 million.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

In addition to the regulations mentioned in our answer to question 2.1, the Guidance for Medical Software Classification, as announced by the TFDA, also applies to Software as a Medical Device. On December 24, 2020, the TFDA announced the revision of the Guidance for Medical Software Classification, which excludes medical software used to measure heart rate and blood oxygen (including wearables) for daily health management of the general public within the scope of a medical device, if they are not related to the diagnosis or treatment of diseases. Recognition of classification is still subject to the judgment of the competent authorities.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

No specific regulations are enacted specifically for AI/ML powered digital health devices or software solutions. Medical devices are all governed by the Medical Devices Act; Chapter IV of the Medical Devices Act provides for regulations concerning management of medical device clinical trials.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  - Service provider – Pursuant to the Physicians Act, a physician may not treat, issue a prescription or certify a diagnosis to patients that are not diagnosed by the physician himself or herself except for certain special (i.e., remote areas) or urgent circumstances. According to Article 2, Paragraph 2 of the Rules of Medical Diagnosis and Treatment by Telecommunications, "special circumstances" refers to those meeting any of the following criteria: (1) acute inpatients who, according to the discharge service plan, require follow-up treatment within three months after being discharged; (2) residents of institutional residential long-term care organisations who hold valid chronic disease refill prescriptions from the medical care provider, whom they have entered into a medical service agreement with, and who require diagnosis or treatment by the provider's physicians; (3) patients in need of integrated care by family physicians, as specified in the Rules and Decrees by either competent authorities or their subordinate agencies; (4) participants requiring follow-up treatment within three months after diagnosis and treatment from the responsible medical team and who have been previously qualified by related Rules and Decrees for the telecare programmes approved by competent authorities or their subordinate agencies; or (5) foreign patients without citizenship and not covered by the National Health Insurance (NHI) who intend to undergo or have undergone treatment in medical institutions in Taiwan. Taiwan is currently planning to amend the "Rules of Medical Diagnosis and Treatment by Telecommunications" to expand its scope of application, in hopes of accelerating the development of telemedicine.

- Regulations for medical devices – The regulations mentioned in our answer to question 2.1 should be complied with if the equipment/devices involved are considered as medical devices.
- Personal data protection – Taiwan's personal data protection law should also be followed if any personal data is to be collected, used or processed.
- Product liability – Manufacturers and sellers of products are subject to the duties and liabilities under the Consumer Protection Act and the Civil Code.
- Attribution of responsibility – Provision of the service of telemedicine may involve the user (patient), the healthcare service provider (physician) and the manufacturer/seller of the product. The attribution of responsibility of the relevant parties should be determined generally based on the contracts, as well as the tort law (Civil Code and Consumer Protection Act).

- **Robotics**
  Similar issues as for Telemedicine/Virtual Care regarding regulations for medical devices, personal data protection, product liability and attribution of responsibility.
- **Wearables**
  Similar issues as for Telemedicine/Virtual Care regarding regulations for medical devices, personal data protection and product liability.
- **Virtual Assistants (e.g. Alexa)**
  Similar issues as for Robotics.
- **Mobile Apps**
  Similar issues as for Wearables.
- **Software as a Medical Device**
  Similar issues as for Wearables.
- **Clinical Decision Support Software**
  Similar issues as for Robotics. There would also be issues under the Physicians Act if the AI is intended to replace the role of physicians.
- **Artificial Intelligence/Machine Learning Powered Digital Health Solutions**
  Similar issues as for Robotics. There would also be issues under the Physicians Act if the AI is intended to replace the role of physicians.
- **IoT (Internet of Things) and Connected Devices**
  Similar issues as for Wearables.
- **3D Printing/Bioprinting**
  Similar issues as for Wearables.
- **Digital Therapeutics**
  Similar issues as for Robotics. There would also be issues under the Physicians Act if the AI is intended to replace the role of physicians.
- **Digital Diagnostics**
  Similar issues as for Robotics. There would also be issues under the Physicians Act if the AI is intended to replace the role of physicians.
- **Electronic Medical Record Management Solutions**
  Similar issues as for Wearables.
- **Big Data Analytics**
  Similar issues as for Robotics, if the results of data analysis will be used as the basis for diagnosis or treatment.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Similar issues as for Wearables.
- **Natural Language Processing**
  No special regulations for Natural Language Processing.

3.2 What are the key issues for digital platform providers?

The PDPA is the main law governing the collection, processing and use of personal data so as to prevent harm to personality rights and to facilitate the proper use of personal data. Digital platform providers should follow the requirements under this Act if any personal data is involved in the products or services provided by digital platform providers.

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

Under Taiwan law, the PDPA is the main law governing personal data protection. The key issues to consider for use of personal data under the PDPA include, among others, the following:

- Whether the data is considered "personal data" under the PDPA.
- Whether the "personal data" is considered "sensitive personal data" under the PDPA. Please see our response to question 4.4 for the definition of "sensitive personal data".
- Whether the use of personal data complies with relevant requirements under the PDPA, such as the requirement to obtain the necessary informed consent from the data subject as required by the PDPA, etc. (or whether any exemption from the requirement applies).

4.2 How do such considerations change depending on the nature of the entities involved?

The considerations indicated in our response to question 4.1 above would not change regardless of the nature of the entities involved; however, the available types of exemptions from the requirement to obtain informed consent from the data subject are different between non-government entities and government entities.

4.3 Which key regulatory requirements apply?

Under the PDPA, unless otherwise specified by law, a company is generally required to give notice to (notice requirement) and obtain consent from (consent requirement) an individual before collecting, processing or using any of said individual's personal information (i.e., the "informed consent" requirement), subject to certain exemptions. To satisfy the notice requirement, certain matters must be communicated to the individual, such as the purposes for which his or her data is collected, the type of personal data and the term, area and persons authorised to use the data, etc.

In case the personal data is regarded as "sensitive personal data" (please see our response to question 4.4), the consent must be made in writing, and the following must be complied with: (i) the collection, processing or use must not exceed the necessary scope of the specific purpose(s); (ii) the collection, processing or use based solely on the consent of the data subject is not otherwise prohibited by law; and (iii) such consent is not given by the data subject out of his/her free will.

4.4 Do the regulations define the scope of data use?

Pursuant to the PDPA, "personal data" is defined broadly to include: name; date of birth; I.D. card number; passport number; characteristics; fingerprints; marital status; family information; education; occupation; medical record, medical treatment and health examination information; genetic information; sexual life information; criminal record; contact information; financial conditions; social activities; and other information which may directly or indirectly identify an individual. Additionally, personal

data pertaining to a natural person's medical records, healthcare, genetic information, sexual life information, physical examination and criminal records are known as "sensitive personal data", and thus are generally subject to stricter regulations under the PDPA.

4.5 What are the key contractual considerations?

In case any collection, use or processing of personal data is contemplated under a contract, it is suggested that the above-mentioned "informed consent" requirement be fully complied with, unless any of the available exemptions are satisfied. Additionally, it may be arranged to have the parties (or, at least for the party who will actually collect, use or process personal data) agree to the "compliance clause" to ensure a party's compliance with the PDPA throughout the contract period.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

Compliance with the PDPA, in particular, obtaining required "informed consent" for collection, use and processing of personal data and using and processing the collected personal data within the necessary scope of the specific purpose(s), is the key legal issue; as any violation of the PDPA (e.g., unlawful collection, use or processing of personal data) may be subject to civil, criminal and/or administrative liabilities. For example:

- Civil liability: A company would be liable for the damages caused by any unlawful collection, processing or use of personal data due to its violation of the PDPA (Article 29 of the PDPA).
- Criminal liability: Any unlawful collection, processing or use of personal data in violation of the PDPA with the intention of obtaining unlawful gains and thereby causing damage to others would be subject to imprisonment for no more than five years and may, in addition thereto, be imposed with a criminal fine of not more than NT$1 million (Article 41 of the PDPA).
- Administrative liability: Any unlawful collection, processing or use of personal data in violation of the PDPA may be required to be corrected, and any failure to correct such violation within a specified period of time would be subject to an administrative fine (Articles 47 and 48).

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

With respect to data inaccuracy, pursuant to the PDPA, a data subject has the right to correct or supplement his/her personal data, as well as the right to request the deletion of the data.

As for data bias and discrimination, currently no specific laws or regulations have been promulgated or amended to address the issues regarding data bias or discrimination. In this regard, we believe that more and more discussions will emerge in legal fields such as labour/employment law (with respect to sex, race, religion or belief, political views, etc.), privacy law, antitrust and any other area where "equality" or "fairness" would be an important factor with respect to social life and economic activity, especially from the viewpoint of issues that may be caused by the use of AI algorithms and big data analytics.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

With respect to generative AI, the data-usage legal or regulatory issues indicated in our responses to questions 4.1 through 4.7 above would also apply and must be addressed by generative AI companies. For example, generative AI should also follow the "informed consent" requirement unless any of the available exemption criteria are satisfied.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Please see our response to question 4.1 above, as sharing personal data would be considered to fall within the definition of "processing" and/or "use" of personal data under the PDPA.

5.2 How do such considerations change depending on the nature of the entities involved?

Please see our response to question 4.2 above.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Please see our response to question 4.3 above.

Please also note that, in case the personal data is regarded as "sensitive personal data" (please see our response to question 4.4), an exemption from the "informed consent" requirement for collection, use and processing of personal data (including data sharing) is "where it is necessary for statistics gathering or academic research by a government entity or an academic institution for the purpose of healthcare, public health or crime prevention, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject".

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

In Taiwan, the NHI system has been implemented since 1995, and the National Health Insurance Administration (NHIA), the competent authority for NHI matters, has collected a considerable amount of NHI data, including personal NHI data, over the years. The NHIA entrusted the NHI data to the National Health Research Institute (NHRI) to establish the National Health Insurance Research Database (NHIRD), which was available for external use between 2000 and 2016. In addition, the NHIA has established the National Health Insurance Information Integration Service to provide access to the NHI data, which has been pseudonymised through encryption algorithms, for external use. However, in 2012, seven individuals sent separate letters to the NHIA refusing to allow the NHIA to release their personal NHI data to third parties for purposes other than those related to the NHI matters, while the NHIA rejected such claims. The subsequent petitions and administrative lawsuits filed by those individuals resulted

in unfavourable final judgments against them, and in 2017, they filed a petition for interpretation of the Constitution, requesting that the relevant statute be declared unconstitutional.

Taiwan's Constitutional Court announced a judgment in August 2022 (Ref. no.: Xian-Pan No.13) regarding the PDPA, holding that relevant laws should be promulgated or amended within three years to reflect/address the following: (i) there would be an independent supervision mechanism for personal data protection under the PDPA; (ii) the requirements and controls governing the use of the NHI data by the NHIA for the purpose of establishing databases, as well as the release of the personal data (i.e., establish the rules for material issues such as the subject, purpose, requirements, scope and manner of storage, processing, external transmission of and external access to the database and the organisational and procedural supervision and protection mechanisms); and (iii) the rules relating to the cessation (opt-out) of the use of the NHI data as requested by the data subject.

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

With respect to federated models of healthcare data sharing, the issues indicated in our responses to questions 4.1 through 5.3 would also apply and must be addressed. For example, the "informed consent" requirement should be followed unless any of the available exemption criteria are satisfied.

6 Intellectual Property

6.1 What is the scope of patent protection for digital health technologies?

According to the Patent Act, the subject of a patent right may be an invention, a utility model or a design:

- Invention – the creation of technical ideas, utilising the laws of nature.
- Utility model – the creation of technical ideas relating to the shape or structure of an article or combination of articles, utilising the laws of nature.
- Design – the creation made in respect of the shape, pattern, colour, or any combination thereof, of an article as a whole or in part by visual appeal. For computer-generated icons (Icons) and a graphic user interface (GUI) applied to an article, an application may also be filed for obtaining a design patent.

Under the Patent Act, any invention/utility model/design is patentable provided it complies with the requirements for patentability, such as novelty, inventive step and enablement. However, please note that diagnostic, therapeutic and surgical methods for the treatment of humans shall not be granted a patent under the Patent Act. Thus, if a concerned "digital health" invention or technology involves diagnostic, therapeutic and surgical methods for the treatment of humans, it may be deemed an unpatentable subject matter.

Moreover, a digital health invention or technology may relate to the creation of a software or an algorithm. "The Examination Guidelines for Computer-related Inventions" provide rules for deciding whether such invention can be granted a patent. The Guidelines classify statutory subject matters for software patents: process; product; and computer-readable storage media. "Process" is defined as a series of specific operational steps to be performed on or with the aid of a computer. "Product" encompasses a computer or other programmable apparatus whose actions are directed by a computer program or another form of software. "A computer-readable storage medium" is an article of manufacture that, when used with a computer, directs the computer to perform a particular function. Software patents are patentable if the data format interacts with computer software or hardware to produce technical effects (such as enhancing data processing, storage performance, security, etc.).

6.2 What is the scope of copyright protection for digital health technologies?

A "work" under the Copyright Act means a creation that is within a literary, scientific, artistic or other intellectual domain, which includes oral and literary works, musical works, dramatic and choreographic works, artistic works, photographic works, pictorial and graphical works, audio-visual works, sound recordings, architectural works and computer programs. There are no registration or filing requirements for a copyright; however, there are certain features that qualify for being copyrighted, such as "originality" and "expression".

Software designed for "digital health" can be protected through copyright.

6.3 What is the scope of trade secret protection for digital health technologies?

Trade secrets are protected if they satisfy the following constituent elements: information that may be used in the course of production, sales or operations; has the nature of secrecy; has economic value; and its owner has taken reasonable measures to protect the secrecy. There are no registration or filing requirements for a trade secret to be protected by law. Any digital health technology that meets the requirements can be protected by the Trade Secrets Act.

To keep trade secrets confidential during court proceedings, the court trial may be held in private if the court deems it appropriate or it is otherwise agreed upon by the parties. In an IP-related lawsuit, the parties may apply to the court to issue a "protective order", and the person subject to such protective order should not use the trade secrets for purposes other than those related to the court trial and should not disclose the trade secrets to those who are not subject to the order.

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

In general, academic institutions have specific internal policies to regulate the ownership and management of the technologies created by their scholars, researchers, graduate students and employees. Academic institutions may license or assign their IPs to a third party for commercial purposes.

6.5 What is the scope of intellectual property protection for software as a medical device?

Software can be protected by IP rights such as patents, copyrights or trade secrets. For software-implemented inventions such as a medical device, if it coordinates software and hardware to process information, and there is a technical effect in its operation, it might become patentable.

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

In judicial practice, an AI device cannot be named as an inventor of a patent. Judgments from the Taiwan Intellectual Property and Commercial Court hold that a patent invention is the creative output of the human spirit, and cannot be created by an AI device; from the perspective of Taiwan laws, only natural or legal persons can enjoy such rights.

6.7 What are the core rules or laws related to government-funded inventions in your jurisdiction?

For projects in scientific and technological research and development (R&D) to be subsidised, commissioned or funded by the government, or to be conducted under scientific and technological R&D budgets prepared by public research institutions (organisations) pursuant to the law, the "management and utilisation of the R&D results" should comply with the Fundamental Science and Technology Act and the Government Scientific and Technological Research and Development Results Ownership and Utilisation Regulations. Specifically:

- The R&D results and the income from such a project may be conferred, in whole or in part, to the executing R&D units for ownership or licensing for use, and are not subject to the National Property Act.
- The ownership and utilisation of the R&D results and the income therefrom should be determined based on the principles of fairness and effectiveness by assessing the percentage contribution of capital and labour, the nature of the R&D results, potential uses, societal benefits, national security and impact on the market.

7 Commercial Agreements

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

Issues in relation to the rights (especially the IP ownership), obligations and division of responsibilities are critical for collaborative improvements. The applicable laws and agreements between the parties would need to be carefully analysed and arranged for in this regard.

For a collaborative improvement involving a fund provider and an inventor/developer, the IP laws adopt similar rules to govern the ownership of the said improvement. With respect to patent rights and trade secrets, the agreement between the parties shall prevail, or such rights will be vested in the inventor or developer in the absence of such agreement, and the fund provider may use such invention.

With respect to copyright, the person who actually creates the work is the author of the work unless otherwise agreed upon by the parties; the economic rights arising from the work should be agreed upon by the parties, or the author owns such rights in the absence of such agreement. However, the commissioning party (fund provider) may use the work.

For improvements that are jointly made by several parties, attention shall be paid to the issue of co-ownership. The Patent Act clearly provides the following provisions for co-owned patents:

- Where a right to apply for a patent is jointly owned, the patent application related thereto shall be filed by all the joint owners. If a co-owner contravenes the provision for "joint-application" by individually filing an application and obtains a patent as a result thereof, other co-owners may file a cancellation action with respect to such patent and seek revocation of the patent right.
- Where the right to apply for a patent is jointly owned, the right to apply for the patent shall not be assigned or abandoned without the consent of all joint owners. Where the right to apply for a patent is jointly owned by two or more persons, none of the joint owners shall assign his/her own share therein to a third party without the consent of other joint owners. Where one of the owners of the right to apply for a patent abandons his/her own share, this share shall be vested in other joint owner(s).
- Where a patent right is jointly owned, except for exploitation by each of the joint owners, it shall not be assigned, entrusted, licensed, pledged or abandoned without the consent of all the joint owners. Where a patent right is jointly owned, no joint owner may assign, entrust or establish a pledge on his/her own share without the consent of all the other joint owners. Where a joint owner of a patent right has abandoned his/her own share, this share shall be vested in other joint owner(s).

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

As indicated in our answer to question 2.1 above, the manufacturing or importation of medical devices is only permitted after a medical device permit licence granting registration and market approval is issued. Given that, whether the company has or is required to obtain the permit licence would be a critical issue.

7.3 What 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 considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

Generally speaking, if two or more contractual parties are involved in the use of generative AI, considerations should include, among others, internal allocation of risk associated with contractual liabilities, tort liabilities, criminal liabilities, agreement on ownership of IP rights (if any), data sharing/transfer, etc.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

According to our understanding of the practice, the current applications of ML include, among others: (i) clinical decision support – for example, analysing medical images with ML to improve the accuracy of diagnosis results; and (ii) big data forecasting – by analysing large amounts of data, tracking or forecasting the relationships between different medicines and side effects.

Please note, however, that although an AI might be able to make decisions by itself, under current Taiwan law, only a licensed physician may practice as a physician. Thus, AI and ML are merely "technologies" or "tools" to assist physicians.

8.2 How is training data licensed?

If any personal data would be collected, used or processed with respect to training data/data licensing, the PDPA regulatory regime (e.g., our response to sections 4 and 5) would apply – for example, it should be arranged to have the data collector obtain the necessary "informed consent" unless any exemption applies. If any intellectual property is involved in the licensing, it is suggested that the customary licensing practice (e.g., IP licensing agreement to be entered into by the licensor and licensee) be followed.

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

Determining the owner of the intellectual property of an AI-created work is expected to be a legal issue that will be widely discussed as AI use develops and becomes more widespread. According to the views of many experts and scholars, AI development can be generally divided into the following three phases, and we are currently in phase 2:

(i) Phase 1: all intrinsic knowledge/information of AI is given by humans, and AI simply functions as a tool to respond to human query inputs. AI does not have the ability to learn or think.

(ii) Phase 2: AI learns through computer software designed by humans, which is called "deep learning". In addition to responding to human query inputs, AI is able to use its limited intrinsic perception and logic to help its users make decisions.

(iii) Phase 3: AI has evolved to have the ability to think for itself and act sufficiently like a human (i.e., it may have perceptions and emotions). That is, AI has a self-training ability, and the ability to evaluate, determine and solve problems.

With respect to phase 1, as the AI merely functions as a tool utilised by humans to create a work or invention, the human (user of the AI) should be the owner of the intellectual property (copyright or patent).

In phase 2, AI already has the ability of deep learning, and it is not merely a tool for humans. However, there would be issues as to whether AI has the ability to create an "original expression" under copyright law or to be an "inventor" under patent law, and if not, whether the human using the AI can be considered as the one who actually creates the "expression" or the invention. Such issues would be more important and cannot be ignored in phase 3, when AI has evolved to have the ability of independent thinking and can create an "expression" and make an invention like a human.

We believe that the above view is also generally supported by a letter of interpretation issued by Taiwan's Intellectual Property Office (IPO) dated April 20, 2018 (Ref. No.: 1070420), which provides that as AI is not a "person" from a legal perspective, any AI-created work cannot be protected by copyright.

In general, our preliminary view is that such issues might not be solved under the current IP regime in Taiwan; it is a real challenge faced by, and needs to be addressed by, the government, legislators, representatives of the court system and other legal practitioners in the future, along with the development of AI.

8.4 What commercial considerations apply to licensing data for use in machine learning?

As indicated in our response to question 8.2, if any "personal data" would be collected, used or processed with respect to training data/data licensing, the PDPA regulatory regime (e.g., our responses to sections 4 and 5) would apply. Specifically, in case of any "sensitive personal data", more restrictions would apply – such as the requirement that the "informed consent" be in writing (see question 4.3). We believe PDPA compliance as indicated should be carefully considered with respect to data licensing.

9 Liability

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

The theories of liability applying to adverse outcomes are mainly as follows:

- Civil liability – breach of contract, torts and product liability: the Civil Code; and the Consumer Protection Act would apply.
- Criminal liability – injury (intentional act or negligence) or carrying out activities of manufacturing or importation without the required permit or approval: the Criminal Code; the Physicians Act; the Pharmaceutical Affairs Act; and the Medical Devices Act would apply.
- Administrative liability – carrying out activities of manufacturing or importation without the required permit or approval; the Medical Devices Act would apply.

9.2 What cross-border considerations are there?

In case any digital health-related services are provided to Taiwan persons from offshore, there may be an issue as to whether such offshore entity would be required to comply with the Taiwan regulatory requirements regarding licensing (e.g., prior approval/permit/licence required for running a medical device company or carrying out healthcare-related activities) as healthcare is a regulated industry in Taiwan. Please also see our response to question 10.2 for such regulatory requirements.

From a contract perspective, even if the governing law of the contract for the digital health-related service is foreign law (i.e., non-Taiwan law) and a foreign court is agreed in the contract for dispute resolution, we still cannot completely rule out the possibility that in case of any dispute where the Taiwan persons file the suit in a Taiwan court, the Taiwan court would still review the matter and rule that the Taiwan laws (such as the Taiwan Consumer Protection Act) would apply in order to protect said Taiwan persons.

9.3 What are best practices to minimise liability risks posed by the use of generative AI in the provisioning of digital health solutions?

To mitigate relevant liability risks posed by the use of generative AI, the providers of the products/solutions may wish to ensure that such products/solutions have met and complied with the applicable technical and professional standards with reasonably expected safety requirements before such products/solutions are brought to the market, as required under Taiwan's Consumer Protection Act.

10 General

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

With respect to cloud-based services for digital health, the PDPA will be applicable, as an organisation using the cloud-based service may carry out the activities of collecting data from the data subjects, which would then be passed to a service provider for processing and use. Therefore, from a Taiwan legal viewpoint, the key issue in cloud-based services for digital health is PDPA compliance. Please see our responses to sections 4 and 5, specifically, where personal data is considered "sensitive personal data", the requirement for the informed consent be in writing (see question 4.3), and an exemption from the "informed consent" requirement for use by non-government entities or academic institutions under certain circumstances (see question 5.3).

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

Please note that healthcare is a regulated industry in Taiwan. For example, running a medical device company, as well as manufacturing and selling medical devices, would require prior approval/permits under current regulations. Additionally, pursuant to the Physicians Act, a person may not practice medicine as a physician without a required licence, and, in the context of telemedicine, a physician may not treat, issue a prescription, or certify a diagnosis to patients that are not diagnosed by the physician himself or herself except for certain special (i.e., remote areas) or urgent circumstances (please also see question 3.1 above).

Given the above, it is advisable for non-healthcare companies to consider the above licensing/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 perspective, it is suggested that venture capital and private equity firms analyse in depth whether the target digital healthcare venture's business model is in line with Taiwan's regulatory regime at the due diligence stage – most importantly, the compliance with licensing/regulatory requirements as indicated under question 10.2 above as well as the PDPA compliance, especially if the personal data collected by the target company would involve "sensitive personal data".

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

According to our observation, the current legal obstacles in Taiwan that would hinder the developments of digital health solutions may include, for example: (i) as indicated in question 3.1, a physician may not treat, issue a prescription or certify a diagnosis to patients that are not diagnosed by the physician himself or herself except for certain special (i.e., remote areas) or urgent circumstances. Therefore, providing telemedicine services by physicians is generally not permitted under current laws in Taiwan; or (ii) there are generally more restrictions on collection, use and processing of "sensitive personal data", which should be normally involved as to 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 (e.g., Taiwan Surgical Association) do not play an important role in the clinical adoption of digital health solutions. Compliance with existing regulatory requirements is of the most importance. Please see our response to question 10.2 above for the licensing/regulatory requirements that need to be followed from a Taiwan regulatory perspective.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

To our knowledge, there are no private insurers that specifically exclude patients who utilise digital health solutions from filing insurance claims when an insured matter occurs and no additional documentation is required, unless it is specified in the insurance policy. Regarding reimbursement by the government, we notice that there is a pilot plan announced by the NHIA in 2020 aiming to include virtual care for remote areas in the coverage of our NHI. Under the said pilot plan, patients who are seen through medical institutions that are approved to conduct virtual care may only need to pay for registration fees, subject to certain exceptions specified in relevant regulations.

10.7 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 announced a judgment in August 2022 regarding the PDPA, holding that relevant laws should be promulgated or amended within three years to reflect/address certain issues regarding the PDPA as well as the NHI data/NHIRD. The PDPA was therefore amended in May 2023, and the preparatory office of the independent "Personal Data Protection Commission" (PDPC) was established in December 2023. It would be prudent to closely follow the developments of the establishment of the PDPC as well as any further amendments to related laws and regulations in the near future.

Hsiu-Ru Chien has an educational background in science, management and law, and is a certified attorney-at-law and patent attorney in Taiwan. She passed the Chinese Patent Bar in 2013. Her practice focuses on patent prosecution, enforcement, licensing and transactions, as well as other IP-related matters. She is serving as the Deputy Secretary of General of the Taiwan Patent Attorney Association. As a partner at Lee and Li, she periodically publishes IP-related articles in international journals such as the *World Intellectual Property Report* and *International Law Office Newsletter*. She has been honoured as Patent Lawyer of the Year 2021 in Taiwan by 2021 *Corporate Intl Magazine Global Award*, Best Patent Prosecution Attorney (Taiwan) by *APAC Insider Legal Awards*, and Top 100 Women in Litigation 2020 by *Benchmark Litigation Asia-Pacific*.

Lee and Li, Attorneys-at-Law
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei 11072
Taiwan

Tel: +886 2 2763 8000 ext. 2806
Email: hrchien@leeandli.com
LinkedIn: www.linkedin.com/in/hsiu-ru-chien-66b3b639

Eddie Hsiung is licensed to practise law in Taiwan and New York. His practice focuses on M&A, securities, financial services, general corporate and commercial, start-ups, etc. He has participated in many corporate transactions (M&A, IPO, JV, cross-border investments) spanning a broad range of industries and areas, including TMT, bio-tech, big data, digital financial services, etc. In addition to the above-mentioned traditional practice areas, he is familiar with legal issues regarding digital economy, digital transformation and the application of new technologies such as fintech, blockchain, virtual assets, AI and data protection, and is often invited to participate in public hearings, seminars and panel discussions to provide advice to the government, regulators, legislators and university/research institutions in these areas on regulatory policies.

Lee and Li, Attorneys-at-Law
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei 11072
Taiwan

Tel: +886 2 2763 8000 ext. 2162
Email: eddiehsiung@leeandli.com
LinkedIn: www.linkedin.com/in/eddie-hsiung-a3050a14

Shih-I Wu has a dual background in biological engineering and law and specialises in handling intellectual property and civil disputes. Shih-I has a wealth of experience in litigation and administrative remedy procedures for patent applications, patent infringement and patent cancellation, as well as in civil and criminal litigation regarding trade secrets, copyrights, and trademark rights. She has undertaken significant trade secret cases and a landmark case concerning protection of computer software. She is also familiar with reviewing IP contracts and consulting on related disputes, and has experience in IP transaction negotiations, royalty audits and tax exemption applications, as well as civil disputes, product liability and consumer protection, fair trade disputes, environmental law disputes and labour disputes. Shih-I's writings on the practice of IP rights have been published in both domestic and foreign journals.

Lee and Li, Attorneys-at-Law
8F, No. 555, Sec. 4, Zhongxiao E. Rd.
Taipei 11072
Taiwan

Tel: +886 2 2763 8000 ext. 2515
Email: shihiwu@leeandli.com
URL: www.leeandli.com/EN/Professions/600/294.htm

Lee and Li, founded more than half a century ago, is the largest law firm in Taiwan providing legal services in the Greater China area by collaborating with law firms and IP agencies in Mainland China. Besides our headquarters in Taipei, we have offices in Hsinchu, Taichung and Kaohsiung, as well as strategic alliances in Beijing and Shanghai. Our services are performed by a total of around 860 employees, including nearly 200 Taiwan-qualified lawyers, 50 foreign lawyers, over 100 Taiwan patent agents/patent attorneys, more than 100 technology experts, and specialists in other fields such as Taiwan- and U.S.-certified public accountants, as well as the PRC patent attorneys and PRC-qualified lawyers of our strategic alliances.

www.leeandli.com

理律法律事務所
LEE AND LI
SINCE 1965 ATTORNEYS-AT-LAW
關懷・服務・卓越
we care・we serve・we excel

United Kingdom


Sally Shorthose


Toby Bond


Emma Drake


Pieter Erasmus

Bird & Bird LLP

1 Digital Health

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

Apps, programmes and software used in the health and care system – either standalone or combined with other products such as medical devices or diagnostic tests.

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

The key emerging digital health technologies in the United Kingdom (**UK**) are as follows:

- 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 distance support to patients either through healthcare practitioners or AI; the integration of telemedicine services with digitised health systems.
- Health data analytics – the digital collation, analysis and distribution (including on a commercial basis).
- Personalised medicine – using genomics to get a faster diagnosis of a condition and being given personalised treatments based on that diagnosis.

1.3 What are the core legal issues in digital health for your jurisdiction?

The two core legal issues are:

- compliance, in the digital collation and handling of patient data, with the requirements of the UK's General Data Protection Regulation (**UK GDPR**) and the UK Data Protection Act 2018 (**DPA**); and
- compliance, in delivering digital health services, with the relevant UK healthcare regulatory regime. For example, in the case of telemedicine services, the regulatory regime is not yet fully updated to deal with the issues arising from the delivery of telemedicine services.

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

Certain sources estimate that the UK healthcare IT and digital market is currently valued at around £5 billion, although this is likely to grow significantly.

1.5 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 in the UK include:

- Babylon Health;
- Teladoc;
- Cera;
- Huma;
- DnaNudge; and
- Lumeon.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

England, Scotland, Wales and Northern Ireland each have their own regulatory regime and competent authority. In England (approximately 85% of the UK population), the relevant legislation is the UK Health and Social Care Act 2008. Broadly equivalent legislation and regulators are in place in the other UK nations. All national regimes require all providers of regulated healthcare services (including e.g. telemedicine) to meet the requirements of the applicable legislation and to register with the relevant national regulatory body in order to be able to legally undertake those services.

Medicines and healthcare products (including software as a medical device (**SaMD**)) are governed across the UK by the UK Human Medicines Regulations 2012 and the UK Medical Device Regulations 2002 (**MDR 2002**), as amended.

General legislation such as the Electronic Commerce Regulations 2002, the Consumer Rights Act 2015 and the Consumer Protection from Unfair Trading Regulations 2008 may also be relevant to digital health.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health 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 (England, Northern Ireland, Scotland and Wales).

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Consumer health devices are, to the extent they are "medical devices", covered by the MDR 2002, as amended. All medical devices need to meet the applicable UK Conformity Assessed (**UKCA**) marking requirements in these regulations and must be registered. However, as part of the guidance regarding transitional arrangements published by the Medicines and Healthcare products Regulatory Agency (**MHRA**) in October 2022, manufacturers will be able to continue to place CE marked medical devices on the Great Britain market until the end of June 2024. There will be separate requirements for certain medical devices placed on the Northern Ireland market, which is currently aligned with the EU regime.

All consumer devices that are not regulated as medical devices under the MDR 2002 are regulated by the UK General Product Safety Regulations 2005 and those other CE/UKCA marking regulations which apply to the specific product, e.g. UK Electrical Equipment (Safety) Regulations 2016, etc. Evidence of compliance with applicable CE/UKCA marking laws and regulations must be compiled and maintained by a nominated responsible person in the UK where the manufacturer is based outside the UK. Based on recent guidance, manufacturers of the aforesaid consumer devices that are not regulated as medical devices may continue to use the CE marking on the Great Britain market until 31 December 2024.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

For the healthcare regulatory regimes in the four nations, the relevant regulatory authorities are:

- England – Care Quality Commission.
- Scotland – Healthcare Improvement Scotland.
- Wales – Care Inspectorate Wales.
- Northern Ireland – The Regulation and Quality Improvement Authority.

The MHRA is the competent regulatory authority for medical devices and maintains the register of such devices. Various regulatory bodies have responsibility for particular UKCA marking regulations.

2.5 What are the key areas of enforcement when it comes to digital health?

Primary areas of concern:

- Telemedicine service providers: Loss of registration (and thus loss of ability to legally provide healthcare services) for failing to comply with the relevant standards. Serious criminal conduct may result in prosecution and significant fines.
- Medical devices (including software): Failure to comply with the relevant regulations can result in the product being recalled and withdrawn from market by the MHRA, and, if there is serious failure to comply with the regulations, an unlimited fine and/or six months imprisonment on conviction.
- In general: Privacy and data security.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

SaMD is governed by the MDR 2002, as amended. In 2022, the MHRA published a "roadmap" for its *Software and AI as a Medical Device Change Programme* published the previous year. Though, the roadmap provides that the changes will primarily come in the form of guidance, some secondary legislation is expected. For example, the MHRA intends to develop secondary legislation to account for cybersecurity and IT risks relating to the large amount of personal data generated in the field of SaMD. The MHRA have further indicated that their aim is to bring new regulations into force by July 2024. The exact outcome of the programme and roadmap on the regulatory landscape in the UK is not yet clear but should become so in the coming years. It will also be interesting to see if any aspects of the EU Medical Devices Regulation are reflected in the new UK legislation.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

See question 2.6 above.

3 Digital Health Technologies

3.1 What are the core legal or 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, healthcare provider (**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**
    - No particular issues.

3.2 What are the key issues for digital platform providers?

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, 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.

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

- 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.
- 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 (e.g. step counts, sporting performance, etc.).
- Identifying the appropriate legal basis for processing data and obtaining any necessary consent.
- Carrying out a Data Protection Impact Assessment (**DPIA**), if required (as is likely) 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.
- Ensuring that any overlapping requirements related to rules on patient confidentiality are met.

4.2 How do such considerations change depending on the nature of the entities 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.

4.3 Which key regulatory requirements apply?

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 (**PECR**) 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 misuse of private information (**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 2024.

4.4 Do the regulations define the scope of 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 question 4.3 above, there are overlapping restrictions under contract, soft law and confidentiality/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 What are the key contractual considerations?

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 preapproved 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).

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

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).

4.7 How are issues with 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 UK's data protection regulator, 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.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

There are no data protection issues that are strictly unique to generative AI companies. The key issues with generative AI in the health sector are:

- ensuring that the use of generative AI to prepare any documentation for use with a patient does not lead to inaccurate processing – there must not be use that could lead to inaccuracies that would lead to any risk to a patient; and
- there must not be any breach of patient confidentiality in using generative AI – this means that a generative AI provider must not be given the ability to access personal data of third parties.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

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 do such considerations change depending on the nature of the entities 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The preceding answers, in particular for questions 4.1, 4.3, 4.5, 5.1 and 5.2, have covered the key regulatory requirements applicable to the sharing of personal data in a digital health context.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

There are numerous NHS initiatives for the sharing of healthcare data. For example:

- NHS Digital, which currently has the 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. This is a role being subsumed by NHS England in early 2024.
- The Health Research Authority's Confidentiality Advisory Group (**CAG**) 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 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.

6 Intellectual Property

6.1 What is the scope of patent protection for digital health technologies?

Monopoly patent protection is available for novel, non-obvious products or processes which have industrial application. Fees are payable on application and renewal. Protection lasts 20 years from the date of application once the patent is granted (see UK Patents Act 1977).

6.2 What is the scope of copyright protection for digital health technologies?

The right to prevent copying, dealing in copies, issuance of copies to the public, performance, broadcast or adaptation for (relevant works only):

- Literary, musical, artistic works (including software) – life of author plus 70 years.
- Published sound recordings – 70 years from date of publishing.
- Broadcasts – 50 years from date of broadcast.

Copyright (generally) arises on creation and fixation of the work, with no requirement for registration. (See UK Copyright, Designs and Patents Act 1988 (**CDPA**).)

6.3 What is the scope of trade secret protection for digital health technologies?

Common law of confidence protects trade secrets. It 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. However, the common law of confidence provides stronger and more comprehensive protection.

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. The institution will typically seek to license the technology either to existing businesses or via the creation of a spin-out company to commercialise the technology.

There are no specific laws governing academic technology transfer.

6.5 What is the scope of intellectual property protection for software as a medical device?

Software is only patentable in the UK to the extent that it meets the requirements in the UK Patents Act 1977. These requirements are stringent and difficult to meet for software. Generally, however, software will be protected as a literary work under the CDPA (see 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?

Following the decision *in Stephen L Thaler v The Comptroller-General of Patents, Designs And Trade Marks* [2021] EWCA 1374, an AI device cannot be named as an inventor of a patent in the UK. In October 2021, the UKIPO issued a public consultation on whether the Patents Act 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 which 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 are the core rules or laws related to government-funded inventions in your jurisdiction?

Government funding for innovation is available in the UK. This funding is classed as a subsidy and therefore must be consistent with WTO rules, the EU–UK Trade and Cooperation agreement and other bilateral UK Free Trade Agreements.

7 Commercial Agreements

7.1 What 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, so the joint owner might find themself in an invidious situation if complete clarity is set out regarding the permitted uses a joint owner may have over the IP.

There may be better ways of approaching this – have ownership following the ownership of background on which the improvement is made or assign it in accordance with predetermined fields of use. Royalty payments and licences to background technology should also be provided for.

7.2 What 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 the norm.

7.3 What 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 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 may be an issue, along with rules and regulations governing generative AI itself, which are rapidly evolving and very region-dependent.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

The statistical and pattern recognition capabilities of machine learning have a wide range of possible applications in the digital health context. These encompass activities which are trivial for any human to complete, but challenging for traditional computer systems (e.g. converting handwritten medical records into text) and those which require many years of human expertise (e.g. detecting breast cancer in mammograms). Their use also covers the full range of potential medical purposes from diagnosis, prevention, monitoring, prediction and prognosis of disease to its treatment and alleviation. Applications currently receiving particular attention are the use of pattern recognition techniques to detect abnormalities in medical imaging data. Olfactory AI is also emerging as a new potential diagnostic technique for certain diseases.

However, any digital health problem which involves the identification of signals in a noisy environment is potentially susceptible to the use of machine learning.

Machine learning can also be applied to the manner in which digital health services are delivered. Natural language processing can, for example, be used to facilitate human interaction with systems which are themselves based on machine learning techniques. Potential applications include "chat bots" combined with expert diagnostic systems to replicate a doctor's consultation. Current systems are limited to diagnosing specific conditions in tightly controlled situations. Future systems will generalise this approach to broader diagnostic platforms with general application. Recent advances in language models and generative AI will open new possibilities for synthesising and communicating information in a healthcare setting.

8.2 How is training data licensed?

Under English law there is no single property right which applies to data *per se* and there is a general reluctance to treat information as a form of property. There may, however, be legal rights which may, depending on the nature/source of the data, be used to control access to, use and disclosure of training data. These include rights in confidential information along with IP rights in the data elements (e.g. copyright, where applicable) or in an aggregation of data (e.g. copyright in original databases or EU database rights).

Where these rights exist, they can form the subject matter for a contractual licence to training data, e.g. an IP licence and/or knowhow licence. The English courts have also recognised that it is possible to impose contractual restrictions on access to, use and disclosure of data even where that data is not protected by other rights. Training data can therefore also be licensed on a purely contractual basis under English law. The possibility of granting a purely contractual licence does not, however, give rise to some general right of "ownership" in the data being licensed.

Unless they refer to intellectual property rights in the data, reference to "ownership" of data in licences may give rise to confusion as this term has no clear legal meaning under English law.

Well-drafted data licences will commonly focus on the rights and restrictions regarding access, use and disclosure of the data and will only refer to ownership in the context of intellectual property rights in the data. They will also address (often complex) issues relating to access, use and disclosure of derived data which is created by the licensee using the licensed data. Data provisions in AI service agreements should also consider the status of meta-data which may be generated through customer interactions with the system.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning 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 which 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 machine learning 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 machine learning 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 machine learning 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.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Many machine learning projects often involve collaboration between a party with expertise in deploying machine learning and another party with access to the data required to train a machine learning system to solve a particular problem. Common commercial issues which 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 which 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 which 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 intellectual property 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 which is used to provide the service, or potentially to develop new AI models for use in a different context.

Customers may resist contractual terms which 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.

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 GDPR might create joint and several liability between partnering organisations if GDPR noncompliance 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, Scottish 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 post-Brexit, at least in the short term.

9.3 What are best practices to minimise liability risks posed by the use of 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 expert clinicians who can overrule them if they propose a potentially harmful path, thereby shifting all responsibility to the clinician or their place of work.

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 machine learning practice for medical device development.

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 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, and these regulations can vary from jurisdiction to jurisdiction – no broad-brush approach will be applicable. It is also a fast-moving market and keeping up with the changes in regulation is 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, MDR and WEEE.
- Consider competition – are they first, second or third to market?
- Consider patent protection – has this been secured where applicable and have they taken steps to protect and exploit unregistrable IP, such as trade secrets?
- Do they own all necessary IP?
- Do they have good supply and service contracts in place, and secure sources of hardware?

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 aforementioned reform plans in the field of medical device regulation indicate that the regulatory environment is undergoing significant change to "catch up".

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* (**ABHI**) plays a key role in representing the industry to stakeholders, such as the Government, NHS and regulators.

Lobbying in the UK is less formalised, although ensuring that the particular digital health solutions meet certain criteria such as the NICE Evidence standards framework for digital health technologies would improve the likelihood of widespread adoption.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

This would depend on the product in question. From an England perspective, while there may not yet be specific publicly funded provision of general health apps *per se* direct to patients, the provision of, e.g. telemedicine may, under certain circumstances, be funded via the NHS. This would be an area to keep a close watch on since the recent launch of the NICE Office for Digital Health, which intends to, amongst other things, work with strategic partners to improve digital health approval pathways and reimbursement policy.

10.7 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 trend to watch in 2024 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.

Acknowledgment

The authors would like to thank Max Gross for his invaluable assistance in the updating of this chapter. Max is a trainee solicitor at Bird & Bird LLP, based in London.

Sally Shorthose is a Partner in the Life Sciences and Intellectual Property Group at Bird & Bird LLP, based in London and Dublin, and is the joint head of the International Life Sciences Regulatory Group. Before her return to private practice in 2001, she had spent 11 years working in-house in senior roles in the Life Sciences industry, including several years as Legal Director of the Novartis Group in the UK. She now specialises in transactional IP work and life sciences regulatory and commercial work and regularly undertakes due diligence and freedom-to-operate projects. She is the editor of the Kluwer Law publication, the *EU and UK Guide to Pharmaceutical Regulatory Law*, the latest edition of which was released at the beginning of 2023, and is a regular speaker internationally on all types of IP and regulatory issues. She has spent much of the last three years leading the Brexit advisory team at Bird & Bird.
Solicitor – England & Wales, 1988.
Solicitor – Ireland, 2017.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7982 6540
Email: sally.shorthose@twobirds.com
LinkedIn: www.linkedin.com/in/sally-shorthose-271833

Toby Bond is a Partner in Bird & Bird's Intellectual Property Group, based in London. Much of his work focuses on helping clients navigate issues relating to the protection and commercialisation of data as they take advantage of the power of big data analytics and AI. He has a particular interest in the wider intellectual property issues arising from the development and deployment of AI systems. Toby also advises clients on medical devices legislation and his broader experience covers CE marking, EU batteries legislation, REACH/CLP, RoHS, WEEE and Electromagnetic Compatibility, with a particular focus on emerging technologies including IoT and AI.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7415 6718
Email: toby.bond@twobirds.com
LinkedIn: www.linkedin.com/in/toby-bond-49a2112b

Emma Drake is a Legal Director in Bird & Bird's Privacy and Data Protection Group. She works with a variety of healthcare and life science clients, from traditional pharmaceutical companies to health informatics providers to new entrants handling personal data in the context of wellness apps or new technology. She has helped clients on diverse topics spanning application of research exemptions, anonymisation, assessing the compliance of new medical technologies, patient support programmes and the processing of data for pharmaceutical regulations such as pharmacovigilance or restrictions under the ABPI code.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7415 6728
Email: emma.drake@twobirds.com
LinkedIn: www.linkedin.com/in/emma-drake-43a3573b

Pieter Erasmus is a Senior Associate in the Intellectual Property 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 advice in relation to a broad range of matters in these fields, including pharmaceuticals, medical devices, general healthcare, clinical trials, marketing and advertising of health products, etc. Pieter's experience further includes corporate and commercial work, including transactional work and the drafting of a wide range of general and bespoke commercial agreements in the life sciences and healthcare sectors. He is a co-author of the Kluwer Law publication, the *EU and UK Guide to Pharmaceutical Regulatory Law*, the latest edition of which was released at the beginning of 2023. Before joining Bird & Bird in 2019, he spent over six years working at the Johannesburg offices of Africa's largest law firm.

Bird & Bird LLP
12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7905 6217
Email: pieter.erasmus@twobirds.com
LinkedIn: www.linkedin.com/in/pieter-miguel-erasmus

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 technologies in your jurisdiction?

The key technology areas in digital health 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 (IoMT), 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).

1.3 What are the core legal issues in digital health for your jurisdiction?

Some core legal issues to digital health are:

- Patentability of digital health technologies, especially with respect to innovations in software and diagnostics.
- Data privacy and compliance with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), the California Consumer Privacy Act (CCPA), and the federal Health Information Technology for Economic and Clinical Health Act (HITECH Act).
- The Federal Food, Drug and Cosmetic Act (FFDCA, FDCA, or FD&C Act), which regulates food, drugs, and medical devices. The FFDCA is enforced by the US Food and Drug Administration (FDA) which is a federal agency under the US Department of Health and Human Services (DHHS). Relevant FDA regulations and programs related to digital health include 510(k) certification, Premarket Approval (PMA), Software as a Medical Device (SaMD), Digital Health Software Pre-certification Program, and the Laboratory Developed Test regulated under the Clinical Laboratory Improvement Amendments program.
- Practice of Medicine Laws that relate to licensure of physicians who work for telemedicine and virtual health companies. These can be state-specific or part of the Interstate Medical Licensure Compact Commission, which regulates the licensure of physicians to practice telemedicine in the list of member states.
- The Ethics in Patient Referrals Act (or "Stark Law") and Anti-Kickback Statutes that apply to telemedicine and virtual health providers who enter into business arrangements with third parties that incentivise care coordination and patient engagement.

1.4 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 2020 range from a low of $39.4 billion to a high of $181.8 billion.

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

- Optum.
- Cerner Corporation.
- Cognizant Technology Solutions.
- Change Healthcare.
- Epic.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

In the US, the FDCA and subsequent amending statutes is the principal legislation by which digital health products that meet the definition of medical devices are regulated.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health in your jurisdiction?

The HIPAA, as amended by the HITECH Act, is a core healthcare regulation related to digital health. The HIPAA sets forth the federal privacy and security requirements for how certain entities must safeguard protected health information (PHI) (inclusive of electronic PHI or ePHI) and how to handle security breaches of PHI or ePHI. In the US, individual states may also have state-specific healthcare privacy laws that pertain to their state residents that might apply to digital health offerings in a particular state and that may also be more strict than the 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, Stark Law, the federal False Claims Act, laws pertaining to improper patient inducements, federal Civil Monetary Penalties Law and state-law equivalents of each of the foregoing.

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Consumer devices are regulated under the statutory and regulatory framework of the FDCA as applies to all products that are labelled, promoted or used in a manner that meets the definition of a "device" under the FDCA. Additionally, the regulations that apply to a given device differ depending on the regulatory class to which the device is assigned and is based on the level of control necessary to ensure safety and effectiveness – Class I (general controls), Class II (general contracts and special controls), and Class III (general controls and PMA). The level of risk that the device poses to the patient/user is a substantial factor in determining its class assignment.

From a consumer standpoint, digital health devices and offerings are also subject to laws and regulations that protect consumers from unfair and deceptive trade practices as enforced on a federal level by the Federal Trade Commission (FTC).

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

In the US, the DHHS regulates the general health and safety of Americans through various programmes and divisions, including the FDA, Centers for Medicare and Medicaid Services, Office of Inspector General and Office for Civil Rights, among many others.

The FDA is the principle regulatory body charged with administering and enforcing the provisions of the FDCA, including those that relate to medical devices and SaMD. The FDA's jurisdiction covers all products classified as food, dietary supplements, drugs, devices or cosmetics that have been introduced into interstate commerce in the US.

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, providing the FDA with 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.

2.5 What are the key 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.

2.6 What regulations 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 the 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 functionality 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 that 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*.

2.7 What regulations apply to artificial intelligence/machine learning 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 of 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 optimize 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:

i. 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.
ii. Strengthen the FDA's encouragement of the harmonised development of Good Machine Learning Practice (GMLP) through additional FDA participation in collaborative communities and consensus standards-development efforts.
iii. 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 (PEAC) 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.
iv. 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.
v. Advance real-world performance pilots in coordination with stakeholders and other FDA programs, to provide additional clarity on what a real-world evidence generation program 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.

3 Digital Health Technologies

3.1 What are the core legal or 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 the 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, and PMA.
  - Stark Law and Anti-Kickback Statutes.
- **Robotics**
  - Data privacy laws including the 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, and PMA.
- **Wearables**
  - Data privacy laws including the 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 the HIPAA, CCPA, and HITECH Act with regard to voice and WIFI signal data that is collected by the virtual assistant.
  - Data rights to the voice and WIFI 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 the 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 the 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 the 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 the 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 the HIPAA, CCPA, and HITECH Act with regard to the handling of patient imaging data used as 3D printing templates.
  - FDA regulatory issues such as SaMD, 510k, PMA ,and Biologics License 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 the 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 the 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 the 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 the 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 the 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, 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 for 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 issues for digital platform providers?

The key issues for digital platform providers are:
- Compliance with data privacy laws, including the 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 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 to consider for use of personal data?

What type of personal data is it? If it is PHI, it would thereby be subject to the 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 the HIPAA. Of course, personal data in general is subject to various, state, federal, and international data privacy laws.

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.

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.

Where is the data coming from and where is it going? To answer this, detailed data maps must 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 do such considerations change depending on the nature of the entities involved?

Assuming the data under consideration is PHI, in dealing with the HIPAA, a threshold determination is whether one is an entity subject to the HIPAA (referred to as a "Covered Entity", (CE)), or a "Business Associate" of said CE by way of providing certain services for the CE. CEs, 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 CE workforce but, by virtue of acting on behalf of, or providing certain services to, a CE, receive access to PHI that is in the possession of the CE and which the CE has responsibility for.

4.3 Which key regulatory requirements apply?

The HIPAA is the primary and fundamental US federal law related to protecting PHI. In relation to the HIPAA, the HITECH Act, signed into law in 2009, further increased patient rights by financially incentivising the adoption of electronic health records and increased privacy and security protection, and also increasing penalties to CEs 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 US states. Especially for data transactions with the EU, the General Data Protection Regulation, in force since May 2018, protects natural persons in relation to the processing and movement of personal data.

4.4 Do the regulations define the scope of data use?

Generally, yes, and particularly, the regulations concerning PHI, the HIPAA, and HITECH Act define the permissible scope of data use.

4.5 What are the key contractual considerations?

Key contractual considerations depend on what is being contracted. For example, for a data transaction involving entities as part of collaborative research, it is essential that IP rights arising out of the research, as well as primary and secondary uses of the data, are clearly defined. 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 CE. With non-PHI involved, data processing agreements may still be needed for handling data, even though it is not subject to the 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.

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

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.

4.7 How are issues with 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 a 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.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

Generative AI companies often rely on publicly available data, such as data scraped from the Internet, to develop and train generative AI tools. The problem with such publicly available data is that they may include private, personal, or otherwise sensitive information. For example, although social media may be publicly available, personal photographs of an individual on a social media page may be considered private information that the individual may not consent to being used for other purposes.

Furthermore, products created by generative AI tools may resemble any one or more of the private information collected and relied on for the generative AI models, thus inadvertently exposing aspects of the private information.

There are already ongoing cases against generative AI companies on the grounds of violation of data privacy rights. For example, in *P.M. v. OpenAI LP*, the plaintiffs allege OpenAI of stealing private information from millions of users without their consent by scraping the Internet to train OpenAI's AI models; therefore conducting theft, misappropriation, and a violation of privacy and property rights.

Although it remains to be seen whether the use of publicly available but private information for the training of generative AI models constitutes a violation of data privacy and other data rights, there is case precedent for the legality of "scraping" publicly available data. For example, in *hiQ Labs, Inc. v. LinkedIn Corp.*, the Federal Circuit held that the practice of "scraping" publicly available data did not constitute an invasion of privacy or an access without authorisation under the Computer Fraud and Abuse Act, as the data had not been marked as "private". It is possible that generative AI companies may use this case as precedent to defend against the use of such data.

Another issue unique to generative AI companies is the use of data that may be subject to IP protection in the development and training of generative AI models. For example, in another ongoing case, *J.L. v. Alphabet Inc.*, the plaintiffs accuse Google of misusing vast amounts of personal information and copyrighted material on the Internet to train its generative AI models. Although the case is yet to be decided, one may argue that the use of the allegedly copyrighted data only for training purposes in generative AI models does not involve "copying" or "reproduction" for commercial purposes, and therefore does not constitute a copyright violation. One can also argue that the use of such data for the training of generative AI models constitutes using the allegedly copyrighted data in a transformative way, falling under the "fair use" exception.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Key issues include data privacy and security generally, regardless of whether the information is PHI or not. For personal data in general, as discussed herein, entities dealing in data must consider the regulatory requirements across different jurisdictions. For US data sharing, federal and state laws must be considered. For international data sharing, ex-US 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 the HIPAA and HITECH Act to consider.

From a personal standpoint, each individual must recognise their own personal right to their own 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 may desire.

5.2 How do such considerations change depending on the nature of the entities involved?

As discussed herein and previously, when data is PHI and subject to federal regulations such as the HIPAA and HITECH Act, entities that qualify as CEs 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The specific federal, state, and local regulatory requirements depend on the types of data, the entity being protected, as well as the organisation sharing the data. HIPAA and the Federal Trade Commission Act (FTCA) are two federal regulations that are of particular relevance to the field of digital health.

HIPAA prevents PHI from being disclosed by covered entities, such as healthcare providers, health plans, and health clearinghouses, without the patient's consent or knowledge, except for certain purposes. The covered entities may be extended to include business associates through a business associate agreement that is required by HIPAA to underline appropriate safeguard for PHI. Business associates may use PHI to perform or provide functions for other covered entities. Such functions may rely on digital health technology, which makes HIPAA particularly relevant for digital health.

A covered entity may use and disclose PHI, without an individual's consent, for certain exceptions. The exceptions that are particularly relevant for data sharing in the field of digital health include: patient treatment; research; public health; and healthcare operations. HIPAA's security rule requires covered entities to safeguard electronic PHI. The rule extends to protection against anticipated impermissible uses or disclosures, which is relevant when covered entities share data to other parties.

Furthermore, the FTCA grants the FTC with permission to regulate against unfair and deceptive trade practices, which include violations based on company privacy policies concerning data sharing. For example, companies that mislead or omit crucial information to consumers regarding data sharing policies may be found to commit a deceptive trade practice. Furthermore, the FTC considers as unfair trade practice the sharing of consumer data for which the benefit does not outweigh the likelihood of substantial injury or harm to the consumer.

Both HIPAA and FTCA also have requirements and protocols in the event a data breach occurs following the sharing of data. For example, the FTC's Health Breach Notification rule requires vendors of personal health records and related entities that are not covered by HIPAA to notify individuals, the FTC, and, in some cases, the media of any breach in unsecured personally identifiable health data.

It is also important to check state and local privacy laws, as they may provide further requirements in the area of data sharing, to the extent such requirements are not pre-empted by federal laws. In particular, states such as California, Colorado, Connecticut, Utah and Virginia have enacted comprehensive privacy regulations (e.g., the California Consumer Privacy Act, Colorado Privacy Act, Connecticut Personal Data Privacy And Online Monitoring Act, Utah Consumer Privacy Act, and Virginia Consumer Data Protection Act, respectively) that govern aspects of data sharing relevant to digital health.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

As discussed herein, the HIPAA provides standards for creating, maintaining, and sharing healthcare data. For example, the HIPAA Permitted Uses and Disclosures define the circumstances in which a CE 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 the HIPAA states that "a covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request". Furthermore, the 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 Health Level Seven [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 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 to 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 What is the scope of patent protection for digital health technologies?

As relevant to digital health, current US 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 US 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.

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 What is 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 US 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 US 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 What is 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 are 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 intellectual property 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 intellectual property 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 What is 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 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). SaMD can also be protectable by patents if it meets US 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 US, both the courts (in *Stephen Thaler v. Andrew Hirshfeld*, E.D.Va., 2021) and the US Patent and Trademark Office have ruled that an AI machine cannot be an "inventor" for purposes of the US 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 must 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 are the core rules or laws related to government-funded inventions in your jurisdiction?

In the US, 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 US industry that is found in all technology transfer programs 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. "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 US industry preference provision before licensing.

7 Commercial Agreements

7.1 What 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 US 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 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 the HIPAA and patient informed-consent requirements. Failure to properly develop and/or execute processes that are compliant with the HIPAA or informed-consent requirements can result in patient data that is tainted, which will encumber its use by the parties.

Data rights are 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 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 be considered.

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 data sets 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 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, the HIPAA requires CEs 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 CE's use of PHI does not fall within a permitted purpose, the CE 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 data sets typically used in generative AI models, parties may consider de-identifying 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 the 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 from the user. The input may itself be considered PHI under the HIPAA or other data worthy of privacy protection under more stringent state laws.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

AI, particularly ML, is used in a variety of ways to enable a myriad of digital health solutions. It has transformed the way healthcare data is processed and analysed to arrive at predictive insights that are used in applications as diverse as new drug discovery, drug repurposing, drug dosing and toxicology, clinical decision support, clinical cohort selection, diagnostics, therapeutics, lifestyle modifications, etc.

Precision medicine models that are powered by Big Data analytics and AI/ML can ensure that an individual's uniqueness (e.g., genome, microbiome, exposome, lifestyle, etc.) factors into the prevention and treatment (e.g., therapeutics, surgical procedures, etc.) of disease condition(s) that the individual is suffering from. An example of this would be companion diagnostic tests that are used to predict an individual's response to therapeutics based on whether they exhibit one or more biomarkers.

AI/ML algorithms trained to predict biological target response and toxicity can also 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 promises 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 and will likely lead to drugs that have greater efficacy and fewer side effects for larger groups of patients.

8.2 How is training data licensed?

The rights to training data sets are typically specified in the agreements between the parties sharing the data. Data rights can be licensed in the same manner as other types of IP rights. That is, it can be treated as a property right (either under copyrights, trade secrets, or as proprietary information) that can be limited by use, field, jurisdiction, consideration (monetary or in kind), etc. As a result, training data licence agreements can be structured with terms that can apportion ownership and rights (e.g., intellectual property, use, etc.) to the trained ML algorithm and any insights that it generates.

Some representative examples are:

- A healthcare system gives a ML drug discovery company access to its data set (i.e., patient medical records) and requires a non-exclusive licence to use the ML algorithm that was trained with its data set for any purpose and joint ownership of any IP rights on clinical insights generated by the ML algorithm.
- A pharmaceutical company gives its data set (i.e., clinical trial data) to a ML data analytics company as part of a collaboration and limits the use of the data for the field of hypertension and asks for an option to exclusively license any IP rights arising from insights generated by the ML algorithm trained with its data set.
- Two pharmaceutical companies agree to combine their data sets (i.e., Car-T research data) with one another and carve out specific fields (e.g., leukemia, lymphoma, breast cancer, etc.) that each of them can use the combined data set for.

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

Current US 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); *Univ. of Utah v. Max-Planck-Gesellschaft 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 US 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 considerations apply to licensing data for use in machine learning?

A variety of different commercial considerations must be addressed when licensing data for use in ML for digital health solutions.

They are as follows:

- Data Set Definition.
- The contents of the data (e.g., genomic, proteomic, electronic health records, etc.) being shared.
- The type of data (e.g., PHI, de-identified, 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.

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 US federal, US state, and ex-US 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 US 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 analogs in ex-US 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 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 de-identify such data to the extent possible, or otherwise ensure that the use of such data in generative AI model training complies under various privacy laws (e.g., the HIPAA, state privacy laws, etc.). For example, the 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 re-identification.

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 data set 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.

10 General

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

As discussed herein and previously, digital health (regardless of whether it is cloud-based), brings 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 US, in several US 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 previously, digital health is a convergence of typically disparate industries: tech; and healthcare. Each industry encounters issues unique to their industry. 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, the 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, intellectual property, FDA/regulatory, data use/privacy/security (including the 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 two 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 US, one that may continue for a substantial period of time, 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 US include the: American College of Radiology; American Board of Medical Specialties; American Medical Association; and the American Board of Professional Psychology.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

From a US 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 if 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 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.

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.

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
555 California Street, Suite 3300
San Francisco, California 94104-1609
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
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

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 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 Houston, New York, London, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg, covering the United States, Europe, Canada, Latin America, Asia, Australia, Africa and the Middle East.

nortonrosefulbright.com

49528_US – 02/24