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.

Introductory Chapter

Expert Analysis Chapters

Q&A Chapters

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

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