International
Comparative
Legal Guides

Digital Health 2021

A practical cross-border insight into digital health law

Second Edition

Featuring contributions from:

Advokatfirma DLA Piper KB
Arthur Cox LLP
Astolfi e Associati, Studio Legale
Baker McKenzie
Bird & Bird LLP
Cliffe Dekker Hofmeyr
Consumer Technology Association (CTA)
D'LIGHT Law Group
Deloitte
Gilat, Bareket & Co., Reinhold Cohn Group
GVA LPC
Hammad and Al-Mehdar Law Firm
Haynes and Boone, LLP
Herbst Kinsky Rechtsanwälte GmbH
Johnson & Johnson
KYRIAKIDES GEORGOPOULOS LAW FIRM
Lee and Li, Attorneys-at-Law
LexOrbis
Llinks Law Offices
Machado Meyer Sendacz e Opice Advogados
McDermott Will & Emery AARPI
McDermott Will & Emery LLP
NeuroPace, Inc.
OLIVARES
Quinz
VISCHER

ICLG.com

ISBN 978-1-83918-097-2
ISSN 2633-7533

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Publisher
James Strode

Editor
Jane Simmons

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Digital Health 2021

Second Edition

Contributing Editor:
Roger Kuan
Haynes and Boone, LLP

Introductory Chapters

Expert Chapters

Q&A Chapters

USA


Roger Kuan


Jason Novak


Phil Kim

Haynes and Boone, LLP

1 Digital Health and Health Care IT

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 technologies in this area?

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.

1.3 What are the core legal issues in health care IT?

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 (Pre-Cert Program), and Laboratory Developed Test (LDT) regulated under the Clinical Laboratory Improvement Amendments (CLIA) 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 (IMLCC), which regulates the licensure of physicians to practice telemedicine in the list of member states.
- 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.

2 Regulatory

2.1 What are the core health care regulatory schemes?

The Federal Food, Drug and Cosmetic Act (FFDCA, FDCA, or FD&C Act) is the principal legislation by which therapeutic products, including medical devices, are regulated in the United States.

The HIPAA, as amended by the Health Information Technology for Economic and Clinic Health Act (HITECH Act) set forth federal privacy and security requirements for how certain entities must safeguard protected health information (PHI), including PHI in electronic form (ePHI), and how to handle security breaches of such PHI. Various individual states may also have their own privacy laws relating to their residents that are even more strict than federal requirements.

2.2 What other regulatory schemes apply to digital health and health care IT?

In addition to the FD&C Act, HIPAA, and the HITECH Act, digital health and healthcare IT are also subject to various health care laws and regulations designed to protect identifiable health information, promote transparency, and prevent fraud, abuse, and waste (respectively). Such laws and regulations include, but are not limited to, the federal Anti-Kickback Statute, the Ethics in Patient Referrals Act (or "Stark Law"); the federal False Claims Act; and the so-called "Sunshine Act" (as well as state-law equivalents of each of the foregoing).

2.3 What regulatory schemes apply to consumer devices in particular?

Consumer devices are regulated under the statutory and regulatory framework that applies to all products that are labelled, promoted, or used in a manner that meets the following definition of a "device" under Section 201(h) of the FD&C Act:

> *"An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:*
>
> - *recognised in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them;*
> - *intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals; or*
> - *intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals; and*
> - *which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolised for the achievement of its primary intended purposes. Notably, certain software functions are excluded from the definition of "device" pursuant to Section 520(o) of the Food, Drug & Cosmetic Act. As is evident from the definition above, the objective "intended use" of a product is critical in determining whether it will be regulated as a medical device."*

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 controls and special controls), and Class III (general controls and premarket approval (PMA)). The level of risk that the device poses to the patient/user is a substantial factor in determining its class assignment.

- **Class I** – Devices that present minimal potential for harm to users, typically simpler in design than Class II or Class III devices. Examples include enema kits, tongue depressors, and elastic bandages. 47% of medical devices fall under this category.
- **Class II** – Most medical devices are considered Class II devices. Examples of Class II devices include blood pressure monitors, powered wheelchairs, and pregnancy test kits. A total of 43% of medical devices fall under this category.
- **Class III** – These devices usually sustain or support life, are invasive or implanted, or present potentially unreasonable risk of illness or injury. Examples of Class III devices include implantable pacemakers and breast implants. 10% of medical devices fall under this category.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The United States Department of Health and Human Services (HHS) regulates the general health and safety of Americans through various programs and divisions, including the United States Food and Drug Administration (FDA), Centers for Medicare and Medicaid Services (CMS), Office of Inspector General (OIG), and Office for Civil Rights (OCR), among many others.

The FDA is the principal regulatory body charged with administering and enforcing the provisions of the Food, Drug & Cosmetic Act, including those that relate to medical devices. The FDA's jurisdiction covers all products classified as food, dietary supplements, drugs, devices, or cosmetics, which have been introduced into U.S. interstate commerce.

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

Currently, the key area of enforcement with respect to digital health and healthcare IT relates to products that are being marketed without the necessary FDA clearances or approvals and/or without complying with the applicable device regulations. Accordingly, the FDA's primary role in enforcing the Food, Drug & Cosmetic Act in the digital health/healthcare IT space is identifying those products that meet the definition of a "device" and determining whether such products present a significant enough risk to consumer health/safety to justify an enforcement action. As in many other contexts, FDA takes a risk-based approach to enforcement in connection with digital health and healthcare IT products.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

The FDA refers to software functions that are device functions as "device software functions". Device software functions may include "Software as a Medical Device (SaMD)" and "Software in a Medical Device (SiMD)". According to the FDA, software functions that meet the definition of a device may be deployed on mobile platforms, other general-purpose computing platforms, or in the function or control of a hardware device. If a software function that meets the definition of a device is deployed on a mobile platform, it may be referred to as a "mobile medical app".

Many software functions are not medical devices, meaning such software functions do not meet the definition of a device under section 201(h) of the Food, Drug & Cosmetic Act, and the FDA does not regulate them as devices. Some software functions may meet the definition of a medical device, but because they pose a lower risk to the public, the FDA exercises enforcement discretion over such devices (meaning it will not enforce requirements applicable to devices under the Food, Drug & Cosmetic Act).

Consistent with the FDA's existing oversight approach that considers functionality of the software rather than platform, the FDA has expressed its intention to apply its regulatory oversight to only those software functions that are medical devices and whose functionality could pose a risk to a patient's safety if the device were to not function as intended.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  - State specific practice of medicine licensing laws and requirements.
  - Data privacy laws including HIPAA, CCPA and HITECH Act with respect to health data that is collected from patients during consultation.
  - Data rights to health data collected from patients during consultation.
  - FDA regulatory issues such as SaMD, 510k certification and PMA.
  - Stark Law and Anti-Kickback Statutes.
- **Robotics**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with respect to health data that is collected and used to train software used to operate the robotic device.
  - Tort liability (products liability or negligence theories) for injuries sustained by patients during surgery.
  - FDA regulatory issues such as 510k certification and PMA.
- **Wearables**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regards to health data that is collected by devices.
  - Data rights to health data that is collected from device wearers.
  - FDA regulatory issues such as SaMD, 510k and PMA if the manufacturer seeks to make diagnostic or therapeutic claims for their devices.
- **Virtual Assistants (e.g. Alexa)**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regards 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 manufacturer seeks to make diagnostic or therapeutic claims for the virtual assistant.
- **Mobile Apps**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regards 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 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 (SaMD)**
  - FDA regulatory issues such as SaMD, 510k and PMA if manufacture 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.
- **AI-as-a-Service**
  - 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 manufacturer makes diagnostic or therapeutics claims for the AI/ML-powered software. Unique issues with evaluating safety and efficacy of AI/ML-powered software used to diagnose or treat patients.
  - Data rights issues related to the data sets that are used to train AI/ML software with. Even more complicated if the training data set includes data sets from multiple parties with differing levels of data rights.
- **IoT and Connected Devices**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regards to health data that is collected by the IoT connected devices.
  - Data rights to the health data that is collected by the IoT connected devices.
- **3D Printing/Bioprinting**
  - Data privacy laws including HIPAA, CCPA and HITECH Act with regard to handling of patient imaging data used as 3D printing templates.
  - FDA regulatory issues such as SaMD, 510k, PMA and Biologics License Application (BLA) depending on whether the manufacturer is making and selling rendering software, printing equipment and bioink with cells or other biological compositions.
- **Natural Language Processing**
  - FDA regulatory issues if the natural language processing (NLP) software is used as part of a medical device or SaMD used as a diagnostic or therapeutic purposes.
  - Tort liability (products liability or negligence) for injuries sustained by patients using these apps or devices, that incorporates the NLP software, for diagnostic or therapeutic purposes.

3.2 What are the key issues for digital platform providers?

The key issues for digital platform providers are:

- Compliance with data privacy laws including HIPAA, CCPA and HITECH Act with regards 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 issues to consider for use of personal data?

What type of personal data is it? If it is personal health information (PHI), it would thereby be subject to HIPAA. Contrast

this with wellness data, for example, which would appear to be health-related but in reality, is separate and distinct and, therefore, not regulated by HIPAA. Of course, personal data in general is subject to various, state, federal, and international data privacy laws.

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 need to be developed, tracing the path of data across various states and nations, thereby identifying the jurisdictions that will define the scope of data compliance requirements for a data user. As stated above, each impacted territory, whether state or country, may have unique data compliance (data privacy) laws that must be accounted for in executing the data strategy. Of note, data mapping is a requirement under several of the potentially applicable healthcare laws and as such, it factors into several parts of the data strategy.

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

Assuming the data under consideration is patient health information (PHI), in dealing with HIPAA, a threshold determination is whether one is an entity subject to HIPAA (referred to as a "Covered Entity"), or a "Business Associate" of said Covered Entity by way of providing certain services for the Covered Entity. Covered Entities, aside from providers of healthcare that bill through claims, include, for example, government healthcare programmes (e.g., Medicare, Medicaid, military health programmes, veteran health programmes), health maintenance organisations (HMOs), employee sponsored health plans, and health insurance companies. Business Associates are parties (person or entity) that are not part of a Covered Entity workforce but, by virtue of acting on behalf of, or providing certain services to, a Covered Entity, receive access to PHI that is in the possession of the Covered Entity and which the Covered Entity has responsibility for.

4.3 Which key regulatory requirements apply?

HIPAA is the primary and fundamental US federal law related to protecting patient health information. In relation to HIPAA, the HITECH, 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 covered entities and their business associates for HIPAA violations. The CCPA, enacted in 2018, is an example of a state statute primarily focused on addressing the enhancement of privacy rights and consumer protection for that state's residents. Similar applicable laws exist in many U.S. states. Especially for data transactions with the EU, the General Data Protection Regulation (GDPR), in force since May 2018, protects natural persons in relation to the processing and movement of personal data.

4.4 Do the regulations define the scope of data use?

Generally, yes, and particularly, the regulations concerning PHI, HIPAA and HITECH define the allowable 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, intellectual property rights arising out of the research, as well as primary and secondary uses of the data, are essential to clearly define. Field restriction language can also become important, as it can minimise the impact of a data transaction agreement to a company's overall business strategy. With PHI involved, if an involved entity has been identified as a business associate, then a Business Associate Agreement may be needed between the business associate and covered entity. With non-PHI involved, data processing agreements may still be needed for handling data, even though it is not subject to HIPAA. Other potentially important terms include terms addressing data breaches, data handling during and after the agreement period, and associated representation/warranty language associated with any breach.

4.6 How important is it to secure 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.

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 personal health information 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 personal health information (PHI), the regulatory requirements only increase, with federal laws such as HIPAA and HITECH 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 might 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 HIPAA and HITECH, entities that qualify as Covered Entities and Business Associates may have to execute Business Associate Agreements to be in proper standing, and may have to ensure that all associated parties involved meet the obligations imposed by federal laws for the handling of PHI.

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

Please see Section 4.

6 Intellectual Property

6.1 What is the scope of patent protection?

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 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 establishes *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?

Trade secret protection can be used to protect formulas, practices, processes, designs, instruments, patterns, or compilations of information that is not generally known to the public and have inherent economic value. Trade secrets have no fixed term but require the owner to appropriately mark the information and to put in appropriate safeguard measures to guard the information from being release to the public. However, unlike patents, trade secrets cannot prevent independent development of the trade secret information.

6.4 What are the typical results on academic technology transfer rules?

Most academic institutions require their professors, researchers and students to assign any IP they develop with the institution's resources or funding to back them. In some instances, the institutions, applicable departments and the professor/researcher enter into separate royalty sharing agreements.

The IP is typically out-licensed to third parties for commercialisation on terms that may include: royalties; upfront payments; milestone payments; and equity in the licensee company.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

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're appropriately marked and appropriate protections are put into place to ensure that they're not released to the public). An 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.

7 Commercial Agreements

7.1 What considerations apply to 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 their digital health solution(s).
- Companies sharing technology or know-how to develop combined digital health solution(s).

Ownership of intellectual property 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 intellectual property 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 intellectual property 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 apply in agreements between health care and non-health care companies?

The most important legal considerations to pay attention to in agreements between healthcare and non-healthcare companies are data privacy compliance and data rights.

With respect to data privacy compliance, the parties need to pay attention to their respective roles and responsibilities in the agreement as it relates to compliance with HIPAA and patient informed consent requirements. Failure to properly develop and/or execute processes that are compliant with HIPAA or informed consent requirements can result in patient data that is tainted, which will encumber its use by the parties.

Data rights is another important consideration in this type of agreement where data (e.g., patient medical records, questionnaires, etc.) is typically owned by the healthcare company which then shares it with the non-healthcare company. It is important for the non-healthcare company to secure the data rights it needs from the healthcare company so that they can use the data for what they need it for and to have the healthcare company warrant or represent that they have properly secured the rights to the data from their patients.

8 AI 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 less side effects for larger groups of patients.

8.2 How is training data licensed?

The rights to training datasets 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 intellectual property 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 dataset for any purpose and joint ownership of any intellectual property 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 intellectual property 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 (MPEP) 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:

- **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, deidentified, anonymised, etc.) that is being shared.
  - The file format of the data being shared.
- **Data Use Case**
  - Data used to train ML algorithm of digital health solution.
  - Geographic location(s) for data use.
  - Fields (e.g., oncology, ophthalmology, etc.) that the data can be used in.
- **Data Rights**
  - Ownership of the data and subsequent data generated from the data.
  - Amount of time that the data can be used for.
  - Sub-licensing rights.

9 Liability

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

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 patient health information 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.

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), bring several potential legal issues related to, for example, data use, data rights, data security/cybersecurity (e.g., hacking, loss, breaches), data loss, and personal health information. 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-health care companies should consider before entering today's digital health care 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, FDA, HIPAA/HITECH, 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 health care 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 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?

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 How critical is it for a digital health solution to obtain formal endorsement from physician certification bodies (e.g., American College of Radiology, etc.) as a driver of clinical adoption?

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.

Roger Kuan is a Partner at Haynes and Boone and chair 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.

Haynes and Boone, LLP
201 Spear Street, Suite 1750
San Francisco, CA 94105
USA

Tel: +1 650 687 8836
Email: roger.kuan@haynesboone.com
URL: www.haynesboone.com

Jason Novak is a Partner in Haynes and Boone's Precision Medicine and Digital Health Practice Group, where he focuses on advising entities, both large and small, on the various legal issues that can arise with emerging technologies in the healthcare and life sciences industries. Tech and biotech are traditionally disparate technologies that, when blended together to form many of our most exciting new technologies, bring forth a combination of unique and interrelated legal issues. Jason has extensive experience in IP strategy and 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. Prior to starting this practice, Jason was an IP Director for Thermo Fisher Scientific, where he managed worldwide IP needs in genetic sciences instrumentation and software.

Haynes and Boone, LLP
201 Spear Street, Suite 1750
San Francisco, CA 94105
USA

Tel: +1 650 687 8800
Email: jason.novak@haynesboone.com
URL: www.haynesboone.com

Phil Kim is a Partner in Haynes and Boone's Healthcare Transactions and Regulatory Practice Group. He has extensive experience in healthcare law and represents various types of providers, ranging from healthcare systems, hospitals, ambulatory surgery centres, physician groups (including non-profit health organisations, or NPHOs), home health providers, and other healthcare companies on the buy- and sell-side of mergers and acquisitions, joint ventures, and operational matters, which include regulatory, licensure, contractual, and administrative issues. Phil regularly advises clients on healthcare compliance issues involving liability exposure, including the Stark law, Anti-Kickback Statute, and HIPAA/HITECH privacy issues.
Phil also assists a number of multinational technology companies entering the digital health space with various service and collaboration agreements for their wearable technology. His clients also include public medical device, biotechnology, and pharmaceutical companies, as well as the investment banks that serve as underwriters involved in the public securities offerings for such healthcare companies.

Haynes and Boone, LLP
2323 Victory Avenue, Suite 700
Dallas, TX 75219
USA

Tel: +1 214 651 5959
Email: phil.kim@haynesboone.com
URL: www.haynesboone.com

Haynes and Boone, LLP is an international corporate law firm with offices in California, Charlotte, Chicago, Denver, London, Mexico City, New York, Shanghai, Texas, and Washington, D.C., providing a full spectrum of legal services in energy, technology, financial services and private equity. With more than 575 lawyers, Haynes and Boone is ranked among the largest U.S.-based firms by *The National Law Journal*, *The American Lawyer* and *The Lawyer*. It also was recognised across the board for excellence in the BTI Consulting Group's 2020 "A-Team" report, which identifies the law firms that in-house counsel commend for providing superior client service.

www.haynesboone.com

haynesboone

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group