DIGITAL HEALTH 2022

In association with
Seyfarth Shaw LLP

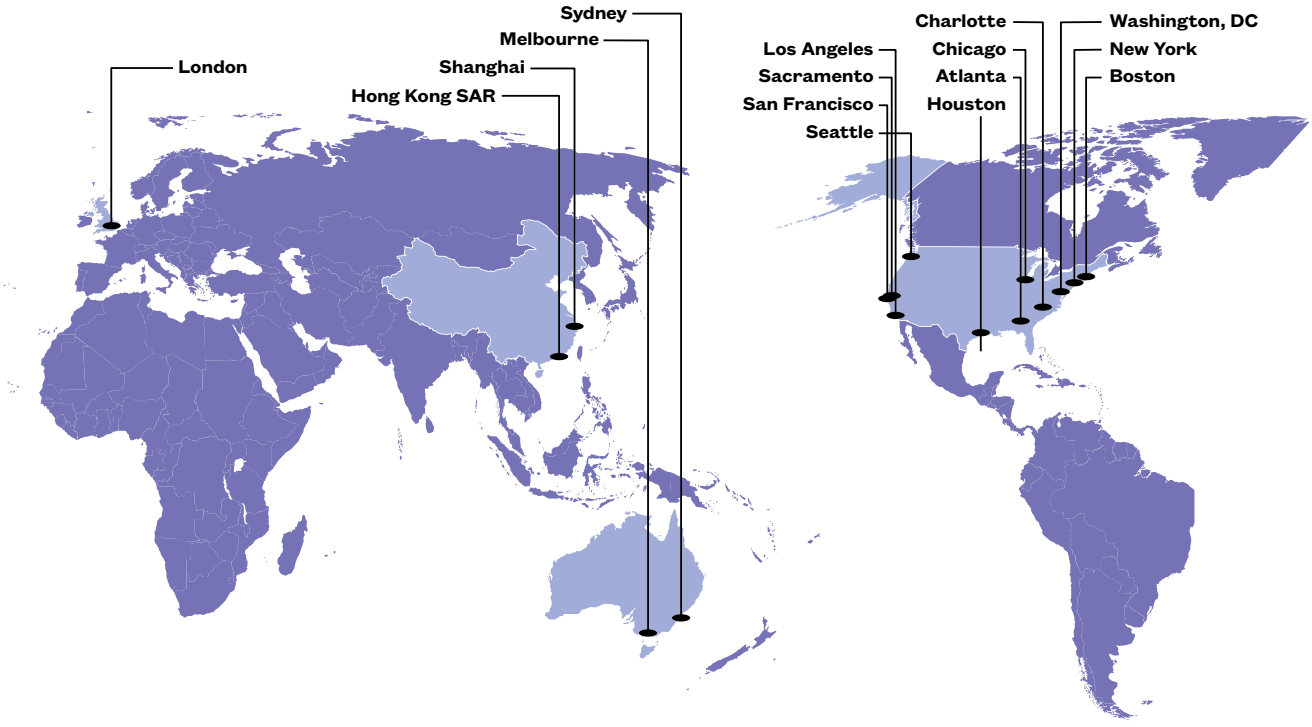
LEXOLOGY
Getting the Deal Through

Seyfarth

Seyfarth

About the Firm

With more than 900 lawyers across 17 offices, Seyfarth provides advisory, litigation, and transactional legal services to clients worldwide. Our high-caliber legal representation and advanced delivery capabilities allow us to take on our clients' unique challenges and opportunities no matter the scale or complexity. Whether navigating complex litigation, negotiating transformational deals, or advising on cross-border projects, our attorneys achieve exceptional legal outcomes. Our drive for excellence leads us to seek out better ways to work with our clients and each other. We have been first-to-market on many legal service delivery innovations and we continue to break new ground with our clients every day. This long history of excellence and innovation has created a culture with a sense of purpose and belonging for all. In turn, our culture drives our commitment to the growth of our clients, the diversity of our people, and the resilience of our workforce.



United States

Chris DeMeo, Sheryl Tatar Dacso, Tonya M Esposito, Brian L Michaelis, Adam H Laughton, John P Tomaszewski, Jamaica Potts Szeliga and Robert S Terzoli, Jr

Seyfarth Shaw LLP

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

1 | Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

The US digital health market is one of the largest consumers of health care dollars in the world. Based on a report by CB Insights titled, 'The State of Healthcare: Q3 2021 Report,' the expectation is that health care tech activity will continue to increase over Q3 2021. Since 2020, the market has evolved as technology has improved. 2020 was a record-setting year for investments, by not only private and corporate investors, but also by the US government. There are new market entrants and others that have either remained stagnant, declined, or merged. The Medical Futurist (TMF) reported that 2021 funding will focus on health-related areas such as research and development (precision medicine), screening and diagnostics (genomics and digital diagnostics), wellness and disease prevention (wearable health trackers), care delivery (disease management, telehealth monitoring, digital pharmacies), and financial operations (value based operations, health management, office automation). We direct you to their infographic that is a composite of the digital health environment by category and market presence. TMF also notes that the increased funding in the market will likely fuel an increase in market introduction, penetration, and disruption, as the different players pursue different strategies with their funding. Covid-19 and anticipated future variants continue to fuel the dramatic growth in mobile health (mhealth), telemedicine, health care analytics, and digital health devices. TMF identifies several AI new players to watch in 2021, including EchoNous (recent FDA approval of its Kosmos and its hand-held platform for AI-led ultrasound of various organs) and PatchAI (cognitive platform focusing on patient engagement for health care engagement using an intelligent virtual assistant). TMF also identifies the technologies to watch into 2021: (1) digital wearables; (2) virtual reality, and (3) 'smart pills.'

Investment climate

2 | How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

During 2021, many digital health companies expanded and deal values soared for early- and growth-stage investments. These developments introduced opportunities for digital health, but they also revealed new challenges, including increased competition, new operational demands, and a need for a more strategic spend on capital. Digital health start-ups raised $6.7 billion more in the first three quarters of 2021 than in all of 2020. The sector raised $6.4 billion in the first quarter, $8.2 billion in the second, and $6.7 billion in the third. Mercom Capital Group, a global communications and research firm, reported that funding activity was up by 138 per cent during the first half of 2021, compared to $6.3 billion raised in the first half of 2020. The market continues to grow in 2021 and, as estimated by IQVA, could reach $66 billion by 2025. Becker's Health IT reports that the most funded digital health companies in 2021 have been those that use software to accelerate research and development, deliver on-demand health care services, and support disease treatments. Mental health has been the top-funded therapeutic focus so far in 2021, with $3.1 billion raised. Telehealth continues to receive substantial funding despite the decrease in utilisation following patients receiving vaccinations and returning to see their doctors in person. RockHealth reported that the first half of 2021 closed with $14.7 billion invested across 372 US digital health deals, with a $39.6 million average deal size. Fifty-nine per cent of that funding came from 48 mega deals ($100 million+), including one of the largest single rounds of investment in digital health history, Noom's $540 million Series F round. The type of investors have changed, with public market investors, companies seeking acquisition targets, and Special Purpose Acquisition Company (SPAC) trusts all looking to get in on the action.

Recent deals

3 | What are the most notable recent deals in the digital health sector in your jurisdiction?

Of the digital health deals done over 2021, RockHealth reports that the vast majority (>80 percent) of this activity is SPAC-related. It is suggested that the use of SPACs has contributed to the recent exit strategy activity involving digital health transactions. A SPAC involves a public entity merging with a private company to take it public. Those public entities – the SPACs – are blank check companies (shell companies without operations) that go through an IPO in order to raise money, with the intent to use these funds to acquire a privately held company. They generally have up to two years to make an acquisition, and they must acquire a target with fair market value of at least 80 per cent of the SPAC's funds. After acquisition, the target company is traded on a public exchange. The US SEC has started looking into these transactions. Visit here for more information regarding the use of SPACs in digital health transactions.

Due diligence

4 | What due diligence issues should investors address before acquiring a stake in digital health ventures?

Digital health companies are acquisition or investment targets that frequently come with heightened due diligence concerns for investors and purchasers. Basic questions relate to: IP; reimbursement generally

and for the particular mode of digital health at issue, as not all are reimbursed equally and many are not reimbursed at all; outsourcing; policies and procedures around privacy, data security, and the collection of personally identifiable information; regulatory compliance at the federal and state level, including licensing, scope of practice, patient consent, information privacy, and fraud and abuse; licensing/registration requirements; and IT compliance with government or industry standards (which can present a serious cybersecurity issue). Digital companies are prime targets for malicious internet activity, including ransomware attacks. Investors must understand the company's practices in these areas before making any financial commitments. With a myriad of federal regulations, and a growing patchwork of state and local laws targeting digital health ventures, investors should vet the target's compliance prior to consummating any investment. Finally, due diligence should include labour and employment concerns, in particular around compliance with wage and hour laws. Some digital health companies have heavily relied on the independent contractor service model, which has come under increasing attack at the state level. In addition, liberal work-at-home policies, adopted in the wake of covid-19, present challenges in employee engagement, capturing all hours worked and ensuring that employees are not working off the clock. Investors should review the target's commitment in these critical areas as well. More specific issues will apply depending on unique characteristics of the digital health company.

Financing and government support

5 What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

Private funding options for digital health companies range from early stage start-ups to multi-round investments and IPOs. In its 2021 report on the Venture Capital Ecosystem, MossAdams attributes much of the explosion in 2021 digital health ventures as being driven by covid-19, noting that, 'The pandemic shone a bright light on the need for increased collaboration across public and private spheres to better monitor the spread of diseases, manage stores and availability of supplies and therapeutics, and prioritize in times of crisis.'

On 15 November 2021, President Joe Biden signed the Infrastructure Investment and Jobs Act (Public Law No: 117-58) into law. Citing broadband internet as necessary for equality in health care access, the President hailed the new law's investment of '$65 billion to help ensure that every American has access to reliable high-speed internet through a historic investment in broadband infrastructure deployment.' This financial commitment promises to make digital health products and services available to significantly more people across the country.

LEGAL AND REGULATORY FRAMEWORK

Legislation

6 What principal legislation governs the digital health sector in your jurisdiction?

The digital health sector is governed by several legislative regimes. The safety and efficacy of digital health products are governed by the FDCA and regulations at 21 CFR Ch 1. The FDCA sets out the processes for review and approval of new devices for public use, circumscribes the technology's approved use or uses, and sets requirements for design, manufacture, packaging, and distribution. The FDCA also confers investigative and enforcement authority.

Commercialisation of digital health technology is governed in part by the FDCA, but also comes under the FTCA and regulations at 16 CFR Ch 1. The FTCA targets deceptive trade practices generally, which includes commercialisation of digital health technology, and imposes breach notification rules on entities that are not covered by HIPAA. The FTCA provides broad enforcement authority to issue penalties and require companies to cease and desist certain practices.

HIPAA and regulations at 45 CFR Parts 160 and 164, as amended by the HITECH Act, governs 'protected health information' (PHI), which is information that identifies a person and relates to the person's health, treatment, or payment therefore. HIPAA also governs the consequences of a breach of PHI. HIPAA applies to 'covered entities' (eg, health care providers that electronically submit claims for reimbursement). Such covered entities and their 'business associates' must comply with HIPAA when using digital health technology. In 2021, OCR proposed amendments to HIPAA regulations that would allow health care providers more flexibility in sharing patient information for care coordination purposes. Final regulations are pending.

States have started to evolve their privacy laws to include both 'medical information' as well as genetic and biometric data. The California Privacy Rights Act (the successor to the California Consumer Privacy Act) has expanded the concept of protected data to include 'sensitive' data. This is so that individuals now have an affirmative right to limit the collection and use of 'sensitive personal information.' (See Cal Civ Code §1798 121). This sensitive personal information includes information about biometric identifiers, genetic information, and health. See Cal Civ Code §1798 140(ae). Note that the word used is not 'medical' but 'health.' This is a much broader characterisation of 'sensitive' than merely information that comes from a Covered Entity under HIPAA. Several other states have also passed similar laws which include the protection of 'health' or 'medical' data. Further, most states have added 'medical data' to the categories of data which require notice if there is a security breach of systems processing such data.

The 21st Century Cures Act was passed in 2016 to advance interoperability; support the access, exchange, and use of electronic health information (EHI); and address occurrences of information blocking. In 2021, the Act's final rule, making a patient's EHI more electronically accessible at no cost, went into effect.

Practitioners in this space must identify applicable legal regimes and how such provisions impact the use of the digital health technology at issue.

Regulatory and enforcement bodies

7 Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

The FDA administers the FDCA and has jurisdiction over the safety and efficacy of digital health technology. The FDA reviews new digital health technology and sets forth approved uses, receives adverse event reports and complaints regarding medical devices, and investigates and issues penalties against digital health technology manufacturers for violations of the FDCA.

The FTC administers the FTCA. The FTC sets guidelines for the promotion of digital health technology and investigates and issues penalties to companies for deceptive practices and health information data breaches.

The OCR administers HIPAA and regulations at 45 C.F.R. Parts 160 and 164, as amended by the HITECH act. The OCR investigates compliance by 'covered entities' and 'business associates' with HIPAA's security, privacy and breach response provisions and issues penalties for non-compliance.

Licensing and authorisation

8 What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

Digital health devices are governed by the FDA. The FDA classifies medical devices, including digital health products, into Class I, II, and III, with the extent of regulation increasing from Class I to Class III. Key elements of the FDA approval process include: (1) registration, (2) listing and (3) Premarket Notification 510(k) (PMN), unless exempt, or Premarket Approval (PMA). 21 CFR Parts 807, 814. Most Class I devices are exempt from PMN; most Class II devices require PMN; and most Class III devices require PMA. The primary difference between PMN and PMA is the need to provide supporting clinical data for PMA. In 2021, the FDA passed then, following the change in presidential administrations and review of stakeholder comments, withdrew a proposed exemption of 83 Class II devices from PMN, stating the proposed exemption was flawed and could have put the lives of Americans using that technology in danger. Once approved, the digital health product is subject to quality system regulation, 21 CFR Part 820, labelling requirements, 21 CFR Part 801, and medical device reporting, 21 CFR Part 803.

Telemedicine is subject to state licensure laws. Generally, a telemedicine practitioner must be licensed in the state where the patient receives the services. A growing number of states have recognised a limited telemedicine licence that allows out-of-state physicians to provide telemedicine services to in-state patients. Several states require a face-to-face visit before telemedicine services can begin.

Soft law and guidance

9 Is there any notable 'soft' law or guidance governing digital health?

The resultant effect of a number of ransomware attacks on health care providers has triggered various regulatory entities to release guidance on how to secure IT systems in the health care space. Most of these guidelines either directly reflect the NIST cybersecurity framework (NIST Framework), or follow the baseline principles of the NIST Framework. This includes State Attorneys General, as well as a reminder of the FTC's guidelines on protecting personal health records ('health' data that may not be considered covered under HIPAA).

Liability regimes

10 What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

Liability regimes for digital health products and services vary by state and include contractual, tort (strict liability and negligence), and consumer protection claims. Contractual liability, including indemnity and warranty, can be restricted by limitation of liability provisions, which cap the injured party's recovery at the cost of a product or service.

Strict product liability covers physical injuries, but is generally not applicable to purely economic losses such as monetary damages for breach or wrongful disclosure of personal information. Individuals suffering a compromise of their personal information often allege negligence in the design or use of a product's cybersecurity features. Although there is no private right of action under HIPAA, its regulations are often used to establish the standard of care and violations thereof. Some states allow common law claims based on violations of privacy and defamation. In 2021, a federal appellate court explained that to recover on such a claim, the plaintiff must establish that the data compromised is sensitive and has been misused, or there is reason to believe it will be misused.

Consumer protection provisions under the FTCA do not create a private right of action. State law imposes liability for deceptive trade practices under statutory and common law, however.

The Telephone Consumer Protection Act (TCPA) prohibits certain 'spam' telephone solicitations, including for health care services. In 2021, the United States Supreme Court unanimously held that to be covered by the TCPA, a device must have the capacity either to store, or to produce, a telephone number using a random or sequential number generator. As such, the decision significantly limited the scope of automated calls and messages that violate the TCPA, giving health care providers more leeway to send automated text messages to patients without obtaining prior patient consent.

Practitioners should know the applicable state law. When dealing with cross-border transactions, the parties can set which state law governs in the contract, subject to certain conflict of laws principles.

The False Claims Act (FCA), imposes liability for false claims to the federal government for payment, including payment for digital health services under federal health care programmes. The FCA allows private citizens acting on behalf of the government to bring suit and receive a portion of the recovery and their attorney's fees if successful. Liability under the FCA includes three times the amount of payment plus penalties of up to $22,000 per claim.

DATA PROTECTION AND MANAGEMENT

Definition of `health data'

11 What constitutes 'health data'? Is there a definition of 'anonymised' health data?

'Health data' includes both regulated data under state and federal medical privacy laws and data which relate to the physical status of an individual protected under state privacy tort laws. In order to be regulated, data must be related to an identified person. However, this is changing with the passage of California, Virginia, and Colorado privacy laws that trigger protections when the individual is identifiable (ie, they don't have to actually be identified). Anonymised data is data that cannot be related to either an identified or identifiable person. If it is possible to take anonymised data and 'reverse engineer' the characteristics of a unique person, then the data isn't anonymised.

De-identified data is not anonymised data. In order for data to be anonymised, it must be practically impossible to associate the data with a specific person – identifiable or not.

Data protection law

12 What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

There is no singular data protection legislation in the US. The FTC may bring enforcement actions to protect consumers against unfair or deceptive practices and to enforce federal privacy and data protection regulations. Health data is generally protected at a higher level than non-health data. This is because of the higher likelihood of adverse effects on the individual through the misuse of such data. These protections come from a variety of different sources. The US tends to use 'sectorial' or 'context-specific' data protection regulation. For example, health data that is processed by a doctor is protected under HIPAA. As such, the source of data protection is generally associated with the nature of the processor, and not the nature of the data.

Various states have passed medical information privacy laws, some of which are more rigorous that the federal HIPAA laws. Generally, these differ from HIPAA in how they define 'covered entities' and conduct that requires disclosure and authorisation, but not how they define health

data v protected health information. Similarly, many states have updated their security breach notice laws to include an affirmative obligation to provide reasonable security for any data collected about the individual. This would also include health data.

Anonymised health data

13 | Is anonymised health data subject to specific regulations or guidelines?

Generally, anonymised data is not subject to data protection regulations. However, it is difficult to have useful data that is anonymous. Usually, de-identified data is considered 'pseudonymous,' which is personal information that has been formatted to limit the risks to the individual. Pseudonymous data is still considered protected data, but the risks that can be attributed to the data are lower and thus the protections are fewer.

Enforcement

14 | How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

At the federal level, health data protection laws are enforced by the OCR. The OCR has enforcement authority over 'covered entities' and business associates of those entities. For digital health technologies, if they are considered 'medical devices,' then the FDA has enforcement authority. For state medical privacy laws, the usual enforcement authority is the state Attorney General. Finally, where tort law can be implicated (under either a privacy tort or negligence per se theory), there is a private right of action for the individual. Additionally, some state law may provide for a private right of action for security breaches. The fact that the data is health data would be a factor in assessing damages.

OCR has investigated and resolved over 27,109 cases by requiring changes in privacy practices and corrective actions. As of July 2019, OCR has settled or imposed a civil money penalty in 65 cases resulting in a total amount of $102,681,582.

There are a number of regulations and guidelines which have been developed in the 'medical device' space. The federal government has developed several guidance documents around the privacy and security requirements for 'connected medical devices' and 'software as a medical device.'

Additionally, there are some gaps in the coverage of the federal law, based on definitions in the federal law as to who is a 'covered entity.' States have addressed these gaps by attaching protections to the data instead of regulating the data processor. For example, Texas and California impose protections on health-related data for entities which are not traditionally considered 'covered entities' under the federal health privacy laws.

Cybersecurity

15 | What cybersecurity laws and best practices are relevant for digital health offerings?

Where HIPAA applies, the HIPAA Security Rule imposes specific information security obligations via a set of 'required' or 'addressable' implementation specifications. These are all based on the information security standards promulgated by the National Institute of Standards and Technology. The NIST standards are also useful where relevant law only requires 'reasonable security' for health data (eg, Cal Civ Code §1798.150 – permitting recovery for a failure to implement reasonable security). Similarly, the FDA's guidance on cybersecurity for medical devices and 'software as a medical device' follow the NIST set of standards.

In addition to HIPAA, FISMA imposes the NIST standards directly onto any direct contractor or subcontractor to the US government. Additionally, by administrative act, several granting agencies in the US government are imposing FISMA/NIST requirements on recipients of federal grant money (eg, National Institutes of Health).

Generally speaking, US laws are 'outcomes-based', are technology-agnostic, and do not mandate a particular control set. However, they all require a risk assessment under which security controls are chosen and implemented. As such, it is important to ensure administrating and procedural controls are provided just as much priority as technological controls (eg, encryption).

Ransomware has been an explosive threat in the health care landscape in the last 12 months. From 1 January 2021 to 31 July 2021, there were 2,084 ransomware complaints, a 62 per cent increase over the same time period a year earlier, and more than $16.8 million in losses, a 20 per cent increase from the previous year. Consequently, security in the digital health ecosystem needs to be as focused on systems availability and integrity as it is on confidentiality. It must be remembered that all security breach notice obligations are triggered when there is a compromise of the integrity of data as well as a compromise of the confidentiality of data. Further, having EMR systems down for extended periods of time can have the effect of increasing mortality rates and decreasing quality of care in some of the health care operations that deal with acute patient encounters.

Cyber insurance is but one of several risk management strategies for a health organisation to address risk of loss through data classification, data retention, employee training, strong indemnification by third party vendors and regularly tested incident response plans. There is no 'one size fits all' policy, as each health care organisation is unique. With the recent and dramatic increase in malware attacks, it is likely there will be more rigorous underwriting. Most cyber insurance policies (through one or more policies) cover network (1) security, (2) business interruption, (3) media liability and (4) errors and omissions. Some policies cover cost of defence and remediation while others will pay out an amount for demonstrable loss up to a limit. Not covered are (1) lost profits, (2) lost value based on theft of IP/proprietary technology or (3) cost of improvements to security systems.

Best practices and practical tips

16 | What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

Handing anonymised data does not require any management under the various data protection laws, as anonymised data is not 'personal' and thus is not protected. 'Raw' data almost always has meta-data attached to it, which makes it at least re-identifiable (if the data is not already directly identifiable). As such, raw data should be treated with the level of protections that are consistent with the various laws that address health and personal data.

- Vendors are often the source of a security breach. Develop and implement a vendor management process which has as information security as a central component. This includes regularly testing or vetting of vendors. This should be done not just for vendors that touch health information, but also any vendor that accesses systems which could touch health information.
- Develop and test quick and resilient disaster recovery processes. Ransomware is an increasing threat that has been directly linked to at least one death in a hospital. This also is important for vendors to undertake.

- Regularly perform and document risk assessments that cover all data uses, locations, processing activities, vendors, and technologies. Risk assessments must be done periodically and around significant events (eg, new technology deployments, new vendor acquisition, and breaches).
- Information Security is a 'state' that is continually changing. As such, the information security program needs to be flexible and extensible to evolve with the risks.
- Consent cures most ills, but consent must be informed and revocable.
- Secondary use will be problematic unless it is for administrative, operational, or health care purposes.
- Anonymised data is usually not really anonymised, so do not think you can use it for anything.

INTELLECTUAL PROPERTY

Patentability and inventorship

17 | What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

A key patentability consideration of digital health inventions is subject matter eligibility under 35 USC § 101. The Supreme Court has held 'abstract ideas' are not patentable, but 'inventive concepts' are. Subject matter eligibility under section 101 remains in flux with the USPTO and federal courts seemingly contradicting one another or themselves at times.

Digital health inventions may fall within the definition of an 'abstract idea.' Natural phenomena and mathematical equations (algorithms) are considered abstract ideas, not patent eligible. Implementing abstract ideas on a computer does not make them patent eligible. For example, the Court of Appeals for the Federal Circuit recently held that a patent claiming a platform to allow for physicians to connect with patients in real time and transfer patient health information was deemed to be an unpatentable abstract idea - well-known business practices implemented on a generic computer network.

Application of abstract ideas may be patentable if an 'inventive concept' is included. Patent applications should focus on technological improvements or practical usage/applications of an otherwise abstract idea. The Federal Circuit held a patent related to wearable trackers may have included an inventive concept based on the 'plausibly inventive way of arranging devices and using protocols rather than the general idea of capturing, transferring, and publishing data.'

Inventors should craft patent applications and claims narrowly to focus on practical application or applications, and incorporate hardware in a meaningful way to avoid merely claiming an abstract idea.

The USPTO has made clear in denying a petition to list AI as an inventor that only a 'natural person' can be an inventor. Applicants should ensure sufficient human involvement in the development process to list a human as an inventor. The USPTO recently issued a report on AI. Applicants using AI should familiarise themselves with USPTO positions.

Navigating section 101 and inventorship can be difficult. Anyone thinking of applying for a patent should consult an IP attorney.

Patent prosecution

18 | What is the patent application and registration procedure for digital health technologies in your jurisdiction?

Patents are obtained by filing an application with the USPTO. The digital health technology patent process is the same as for any patent application. Two types of patents may protect digital health assets – utility and design patents. Generally, utility patents protect how an invention is used or works while design patents protect an article's appearance.

For utility patent protection, an invention must be 'useful,' 'novel,' and 'non-obvious.' 35 USC §§ 101, 102, and 103. A patent application must include a written description enabling persons skilled in the art to make and use the invention, and show the inventor possessed the invention.

Design patents cover 'new, original and ornamental design for an article of manufacture.' 35 USC § 171. They do not protect functional aspects. Design patents merely require drawings meeting USPTO requirements. They are useful in protecting, for example, ornamental design of a wearable device.

The USPTO has created a covid-19 Prioritised Pilot Programme to prioritise examination of patent applications for inventions related to covid-19. The USPTO has created a similar programme for prioritising initial examination of trademark applications. An applicant should familiarise themselves with the USPTO's requirements to participate in this programme and be sure that they submit the necessary request in time, currently 31 December 2021 for patent applications.

Other IP rights

19 | Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

Copyrights, trademarks, and trade secrets are important in protecting digital health offerings.

Copyrights are federal rights that protect original works of authorship fixed in a tangible medium. 17 USC § 102. Registration is handled at the United States Copyright Office and is necessary to sue under copyright law. Unlike patents, copyrights do not need to be registered for copyright protection. Protection attaches once the work of authorship is 'fixed in a tangible medium,' for example, written to paper or entered into a computer.

Trademarks identify source of goods or services in commerce. A trademark can be registered at the USPTO, the state, or arise based on use in commerce. Obtaining a federal or state trademark registration requires filing of an application. 'Common law rights' attach once the mark is used in commerce. All trademark rights are premised on use in commerce with goods or services. If properly maintained, trademark protection can last in perpetuity.

Trade secret protection comes from reasonable efforts to maintain secrecy of valuable information. Trade secret information must be (1) information having value by not being generally known, (2) valuable to others who cannot legitimately obtain the information and (3) be subject to reasonable efforts to keep it secret. Trade secrets are not registered, and may last in perpetuity.

Licensing

20 | What practical considerations are relevant when licensing IP rights in digital health technologies?

Key considerations to IP licensing rights include modifications or improvements, confidentiality, and termination.

First, digital health is an innovative area. Licences need to account for modifications or improvement of the licensed IP. Will improvements be owned by one party or jointly owned? Addressing these issues in a licence will help to clarify rights and reduce conflict as the technology develops.

Second, confidentiality of IP may be essential in a licence, particularly for trade secrets. A licence should have confidentiality requirements, eg, limiting disclosure to third parties, or employees on a need to know basis. Additionally, if the digital health technology utilises software, both the licensee and the licensor should consider whether

the software contains code that is subject to any open source software (OSS) licence. Some OSS licences require software that incorporates code covered by the OSS licence must be licensed in ways that may affect proprietary rights otherwise existing in the software. Some OSS licences, for example, require that the source code must be disclosed for such software or that any software licences be provided at no charge. In evaluating licences to digital health technologies have software components, a review for code covered by OSS licences should be considered. Deals may be structured to limit the effects of OSS licences once the issue is identified and thus protect confidentiality and trade secret rights.

Finally, termination, for example, for breach or bankruptcy, is a major consideration. A licensor will need to ensure a third party is not granted a right to the licence through bankruptcy proceedings. Such a transfer of licence rights may eviscerate any trade secrets.

Enforcement

21 What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

IP rights for digital health technologies are enforced in the same manner as other property rights, in civil litigation in state and federal court.

A recent decision by a Wisconsin federal court shows the breadth of coverage and remedies for trade secret protection. Where a defendant improperly accessed plaintiff's trade secret information regarding health care software, the court granted compensatory ($140 million) and punitive monetary damages (not to exceed $140 million), and also granted injunctive relief, including future monitoring of defendant.

A recent decision by the Federal Circuit held that, although a patent claim was directed to an abstract idea, the specific configuration of hardware and software provides a 'plausibly inventive' step to overcome a motion to dismiss. This does not mean that claim is in fact patentable, only that the district court could not make such a determination as a matter of law, allowing the case to progress further.

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

22 What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

The advertising and marketing of digital health products and services are governed by several federal and state agencies. At the federal level, to the extent the digital health products in question advertise or market food (including dietary supplements), drugs, biologics, medical devices, certain electronic products (including laser products, x-ray equipment or ultrasonic therapy equipment) or cosmetics, they are governed by the FDA under the FDCA.

The scope of the FDA's regulatory authority is very broad and overlaps with several other government agencies. For example, the FTC regulates many types of advertising and is charged with protecting consumers by stopping unfair, deceptive or fraudulent practices in the marketplace pursuant to the FTC Act. As such, to the extent the digital health products and services in question are marketed to consumers, they will also be subject to regulation by the FTC.

At the state level, the attorney general's office and any related consumer protection agencies also regulate the advertising and marketing of digital health products and services, generally under what are often referred to as state or 'baby' FTC Acts.

e-Commerce

23 What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

Regulations governing e-commerce, including those set forth in the FTC Act, and any state equivalents, are applicable to digital health offerings to the extent they are selling products or services to consumers or collecting personal identifiable information from consumers, or both. In general, the FTC and state regulators enforce federal and state laws applicable to consumer sales and data privacy and collection. Electronic payment processing is also subject to a myriad of other consumer protection legislation, including but limited to the COPPA, the Gramm-Leach-Billey Act and the FCRA.

PAYMENT AND REIMBURSEMENT

Coverage

24 Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

The US health care system is a complex and significantly privatised model of reimbursement for health care services, where funding and delivery are not integrated. Most health coverage is provided or administered by third-party payers with employers, federal and state governments, and individuals paying for (insurance coverage) or funding (self-funded) policies of coverage. Reimbursement for telemedicine services has seen dramatic changes over the past 10 years, with the past two years being the most significant because of covid-19. The federal Medicare programme, which primarily covers aged and disabled persons, featured limited coverage and reimbursement for telehealth services, depending on the patient's location, the type of services provided and the technology utilised. Most state Medicaid programmes (which mostly cover low income individuals and children) cover telemedicine services with coverage and reimbursement expansions (covid-19-related) for remote communications technology codes such as virtual check-ins and e-visits. The most common specialties that had covered services expansions under Medicaid included behavioural health and substance use disorder services, teledentistry, school-based health services, and speech therapy. Rural health clinics and federally qualified health centres can now be reimbursed as a distant site. The covid-19 pandemic saw CMS and state governments adopt certain emergency waivers and other executive orders that expanded the use of telehealth services, including the types of services eligible for reimbursement, the types of professionals that could provide them and the locations where patients could receive covered services. Telemedicine providers, along with some federal legislators, have taken up the issue of making the coverage and reimbursement expanded during covid-19 a permanent feature of these programmes.

Forty-three states and DC have laws that govern private payer telemedicine reimbursement policies. These policies vary from state to state with respect to how telemedicine is defined, provider eligibility and qualifications, methods of delivery and coverage. Some laws require reimbursement parity between in-person and telemedicine, while most only require parity in coverage. Although most states adopted temporary telemedicine covid-19 emergency policies, it is unclear if all will continue those policies after the pandemic is under control.

UPDATES AND TRENDS

Recent developments

25 What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

In 2021, there were several developments in the digital health sector related to payer acceptance and health information access, as federal and state governments assessed the future of digital health in light of lessons learned from the covid-19 pandemic. In addition, technological advancements continued, resulting in multiple medical devices, implantables, personal health care applications and wearables, which are increasingly integrated into clinical operations.

Payers continue to authorise additional modalities for reimbursement and states have increasingly promoted digital health adoption. According to the Commonwealth Fund, 22 states have changed laws or policies to promote access to telemedicine since 2020. The Commonwealth Fund also reported that in 2021, at least 30 states introduced legislation to revise telemedicine coverage standards. At the federal level, the 'Advancing Telehealth Beyond Covid-19 Act of 2021' was introduced in the US House of Representatives and is currently in committee. However, the Government Accountability Office (GAO) has cautioned against extending covid-19 telehealth waivers beyond the pandemic until further information regarding spending, program integrity, health and safety, and equity is available.

In 2021, the 21st Century Cures Act final rule, making a patient's electronic health information more electronically accessible at no cost, went into effect. In addition, the Office for Civil Rights issued proposed revisions to the HIPAA Privacy Rule, which would allow health care providers more flexibility in sharing patient information for care coordination purposes. Final regulations are pending.

Seyfarth

Health Care Group

The health care industry is one of the most highly regulated and constantly changing sectors globally. Before the unprecedented changes resulting from COVID-19, organizations operating in this space were continuously affected by transformation. Now, the pandemic has caused health care organizations to evaluate and evolve in a variety of ways. Many of these transformations in health care are driven by changing regulations, economic survival, and quality standards, and will continue even after the pandemic comes to an end.

At Seyfarth, we are uniquely positioned to partner with health care organizations to develop successful strategies for navigating and responding to these industry-specific pressures. We foster a collaborative approach, offering our clients comprehensive, thoughtful, and real-world solutions that positively impact their strategies and operations.

We represent clients across the health care space, including telemedicine and digital health companies, and our attorneys are recognized thoughts leaders at the forefront of industry and legal change.

Featured Content: Future of Health Care in the US

Our team has published the second edition of its *Future of Health Care in the US* treatise. This piece provides updates and new insights into what the post-pandemic world may look like for the health care industry. Authors highlight lessons learned from providers and others who have been at the epicenter of the COVID-19 response, and how stakeholders, regulators, and the public at large will use this crisis to address the disparities in how health care is accessed, funded, and delivered.

Accolades

U.S. News & Best Lawyers "Best Law Firms" Rankings

Recognized again as a Tier 1 national Health Law practice by *U.S. News & World Report* (2022).

The *Legal 500* Rankings

Recognized as a leading, nationwide Health Law practice by *The Legal 500* (2012-2014, 2016-2020).

Modern Healthcare

Ranked among the top 50 largest Health Care law firms by *Modern Healthcare.* (2016-2021).

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Digital Business
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt