LEXOLOGY
Getting the Deal Through

DIGITAL HEALTH 2023

Contributing editors
Eveline Van Keymeulen, Oliver Mobasser, Samantha Peacock, Sara Patel and Brett Shandler

United States
Renee B Appel, Chris DeMeo, Brian L Michaelis, Suzanne L Saxman, John P Tomaszewski, Jamaica Potts Szeliga, Robert S Terzoli, Jr and Breanne E Vaclavik
Seyfarth Shaw LLP

LEXOLOGY
Getting the Deal Through

START READING

Seyfarth

Health Care Group

The health care industry is one of the most highly regulated and constantly changing sectors globally. Organizations operating in these areas are continuously affected by transformation, while trying to maintain an edge in competitive markets.

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.

Seyfarth Health Law Attorneys Featured in AHLA Video Docuseries

Members of Seyfarth's Health Care group were featured in a 2022 video docuseries, produced by the American Health Law Association, titled, "*Health Law Disruption: Cybersecurity & Emerging Data Risks*." Seyfarth's episode, "*Guiding Federal & State Laws,*" focuses on how technology continues to change the face of health care and how this impacts the ability of industry stakeholders to conduct business and care for patients. Speakers also discuss how the firm works closely with clients to help protect their health information and provide guidance for federal and state-specific privacy and security regulations.

Accolades

U.S. News – Best Lawyers® *"Best Law Firms" Rankings*

Recognized again as a National Tier 1 Health Care Law practice by *U.S. News – Best Lawyers®* (2023).

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).

United States

Renee B Appel, Chris DeMeo, Brian L Michaelis, Suzanne L Saxman, John P Tomaszewski, Jamaica Potts Szeliga, Robert S Terzoli, Jr and Breanne E Vaclavik

Seyfarth Shaw LLP

Summary

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?

US digital health funding has remained active in 2022 but has cooled off compared to record highs in 2021. Based on a report by CB Insights titled 'State of Digital Health: Q2 2022', the decrease in funding as well as a decrease in deal volume and median deal size generally has affected almost all sectors across digital health except for healthcare IT, mirroring the broader downtrend in venture funding. Nonetheless, the healthcare market has continued to evolve as the pace of innovation continues to accelerate. The Medical Futurist (TMF) reported that 2022 funding will focus on health-related areas such as biopharma and medtech research and development, screening and diagnostics (genomics and digital diagnostics), wellness and disease prevention (wearable health trackers and home monitoring equipment), care delivery (disease management and digital pharmacies), and financial operations (value-based operations, health management, office automation). Artificial intelligence (AI) continues to be a reference point for innovation in the healthcare market. TMF identifies several AI players to watch in 2022:

- DeepMind (an AI subsidiary of Google touting recent health-related breakthroughs, including predicting age-related macular degeneration, diagnosing acute kidney injury earlier, and detecting breast cancer before symptoms appear);
- Alivecor (a leader in Food and Drug Administration-cleared personal electrocardiogram technology); and
- Skinvision (a skin cancer melanoma detection app).

Investment climate

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

The past few years saw many digital health companies expand and deal values soar for early and growth-stage investments. However, based on a report by RSM US LLP titled 'M&A trends in the healthcare industry: Summer 2022', past levels of healthcare private equity consolidation activity plus acquisitions made by strategic partners, such as healthcare systems, now mean fewer businesses are available for purchase at attractive multiples. At the same time, macroeconomic forces such as increasing interest rates and ongoing labour shortages have resulted in lower deal volume in 2022. Early in 2022, crossover firms such as Tiger Global and D1 Capital announced they were pulling back on late-stage investments. RockHealth reported that several key themes have emerged throughout 2022, including smaller deal sizes across the board, a focus on early-stage funding, reprioritisation of technology investments, and an exit market that is beginning to thaw. Additionally, in the first half of 2022, RockHealth reported that the majority of investors were repeat investors in the digital health space, whereas previous years saw a more balanced distribution between new and repeat investors. According to RockHealth data, with US$2.2 billion raised across 125 deals, the third quarter of 2022 represents the smallest funding quarter in the sector for all of 2022. Further, 2022 year-to-date funding totalled US$12.6 billion across 458 deals,

raising doubts that the 2022 digital health bucket will reach even half of last year's US$29.2 billion. Based on a report by CB Insights titled 'State of Digital Health: Q3 2022', M&A exits are at a five-year low generally.

Recent deals

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

On 1 January 2022, the introduction by CMS of new Current Procedural Terminology codes to bill for remote monitoring services fuelled funding for digital health solutions monitoring complex chronic conditions. Notably, Biofourmis, a virtual care and digital medicine-focused company, raised US$300 million in a Series D investment led by global growth equity firm General Atlantic and Omada Health, a digital chronic care management company, scored US$192 million in a Series E funding led by Fidelity Management & Research Company. In addition, Somatus banked US$325 million to target kidney and renal diseases and ConcertAI grabbed US$150 million for its real-world data solutions for cancer research. In stark contrast to 2021, where the vast majority to digital health deals were special purpose acquisition company (SPAC)-related, Fierce Healthcare reported that after digital health exits yielded poor returns in 2021, initial public offerings stalled in the first quarter of 2022 with just one initial public offering (IPO) versus 23 IPOs in the previous quarter and no deals involving SPACs, compared with six SPAC deals in the fourth quarter of 2021.

Due diligence

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

Digital health companies come with heightened due diligence investigations for investors and purchasers. The typical areas of due diligence conducted in a digital health acquisition include:

- intellectual property;
- 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, the scope of practice, patient consent, information privacy, and fraud and abuse;
- licensing or 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. It is important for investors to understand the target's practices in these areas during the due diligence stage. With myriad federal regulations and a growing patchwork of state and local laws targeting digital health ventures, investors should fully vet the target's compliance prior to consummating any investment. In addition, due diligence should include

labour and employment matters, in particular with respect to compliance with wage and hour laws. Some digital health companies have relied heavily 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 the covid-19 pandemic, 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. More specific issues may be triggered depending on the unique characteristics of the digital health company at hand. Given the current healthcare climate, RockHealth reported that potential buyers are inclined to complete more robust due diligence, investigating a potential target's profitability, burn rate and tech stack for cracks and concerns. This level of due diligence will generally be required in any event if the buyer expects to purchase representation and warranty insurance in connection with an acquisition.

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 startups to multi-round investments and IPOs. In a push to comply with the Cures Act data portability requirements before 2022–2023 deadlines, there has been an emergence of startups in the integration services and application programming interface (API) category, such as Flexpa (focusing on health plan payer patient access APIs) and Zus Health (a shared development platform backed by a shared data record). In addition, the Infrastructure Investment and Jobs Act, which was signed into law at the end of 2021, promises to make digital health products and services available to significantly more people across the country, citing broadband internet as necessary for equality in healthcare access. President Joe Biden hailed the new law's investment of 'US$65 billion to help ensure that every American has access to reliable high-speed internet through a historic investment in broadband infrastructure deployment.'

LEGAL AND REGULATORY FRAMEWORK

Legislation

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

The safety and efficacy of digital health products are governed by the Federal Food, Drug, and Cosmetic Act (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 and sets requirements for design, manufacture, packaging and distribution. The FDCA also confers investigative and enforcement authority.

The commercialisation of digital health technology is governed in part by the FDCA but also comes under the Federal Tort Claims Act (FTCA) and regulations at 16 CFR Ch 1. The FTCA targets deceptive trade practices generally, which include the commercialisation of digital health technology, and imposes breach notification rules on entities that are not covered by

the Health Insurance Portability and Accountability Act (HIPAA). The FTCA provides broad enforcement authority to issue penalties and requires companies to cease and desist certain practices.

HIPAA and regulations at 45 CFR Parts 160 and 164, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act govern the privacy and security of electronic protected health information (ePHI), which is information that identifies a person and relates to their healthcare. HIPAA's requirements for ePHI apply to healthcare providers, health plans and their 'business associates', including digital health vendors. In 2021, the Office for Civil Rights (OCR) proposed amendments to HIPAA regulations that would allow healthcare providers more flexibility in sharing patient information for care coordination purposes. Final regulations have been delayed into 2023.

Several states regulate both 'medical information' as well as genetic and biometric data. The California Privacy Rights Act, which becomes fully operative on 1 January 2023, expands the concept of protected data to include 'sensitive' personal information that includes biometric identifiers, genetic information, and health information that is more expansive than HIPAA. See Cal Civ Code section 1798.140(ae). Several other states have also passed similar laws that include the protection of 'health' or 'medical' data. Further, most states have added 'medical data' to the categories of data that 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; and address occurrences of information blocking. On 6 October 2022, the types of records to which the Act applied expanded from eight types of clinical notes to all requested electronic health information. Final enforcement rules are still pending, however.

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 CFR 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.

Read this article on Lexology

The ONC administers the 21st Century Cures Act and regulations at 45 CFR Parts 170 and 171.

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 (21 CFR Parts 807, 814) include:

- registration;
- listing; and
- Premarket Notification 510(k) (PMN), unless exempt, or Premarket Approval (PMA).

Most:

- Class I devices are exempt from PMN;
- Class II devices require PMN; and
- 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 healthcare providers has triggered various regulatory entities to release guidance on how to secure IT systems in the healthcare space. Most of these guidelines either directly reflect the National Institute of Standards and Technology (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 and consumer protection claims. Contractual liability can be restricted by the limitation of liability provisions that cap 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 healthcare 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 healthcare 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. 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 US$22,000 per claim. Digital health companies, such as electronic health record (EHR) vendors, face the greatest exposure in areas where the technology is related to the submission of claims to the federal government for healthcare services and for subsidies under the Meaningful Use programme. Recent enforcement actions include improper payments to physicians and EHR design features that improperly steer physicians to preferred laboratories. Telemedicine companies are also facing increased scrutiny.

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 that relate to the physical status of an individual protected under state privacy tort laws. 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 (namely, they do not 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 is not anonymised.

De-identified data is not anonymised data. 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 United States. 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 United States 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 versus 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.

In addition to medical data-specific laws, five states have passed omnibus privacy laws that now include medical information as part of the larger scope of protected data. California now considers medical-related data 'sensitive' and imposes additional restrictions and controls on such data beyond what the usual mini-HIPAA law requires. We are seeing this trend increasing with Utah, Virginia, Colorado and Connecticut also passing California-style laws.

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 but 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.

The OCR has investigated and resolved over 29,630 cases by requiring changes in privacy practices and corrective actions by, or providing technical assistance to, covered entities and their business associates. To date, the OCR settled or imposed a civil money penalty in 110 cases resulting in a total dollar amount of US$131,563,132.00.

There are a number of regulations and guidelines that 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 that are not traditionally considered 'covered entities' under 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 (NIST). The NIST standards are also useful where relevant law only requires 'reasonable security' for health data (eg, Cal Civ Code section 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, the FISMA imposes the NIST standards directly onto any direct contractor or subcontractor to the US government. Additionally, by an administrative act, several granting agencies in the US government are imposing FISMA or 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).

Cyber insurance is but one of several risk management strategies for a health organisation to address the 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 healthcare 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;
- security;
- business interruption;
- media liability; and
- errors and omissions.

Some policies cover the cost of defence and remediation while others will pay out an amount for the demonstrable loss up to a limit. Not covered are:

- lost profits;
- lost value based on theft of IP or proprietary technology; or
- 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 that makes it at least re-identifiable (if the data is not already directly identifiable). As such, raw data should be treated with a level of protection that is consistent with the various laws that address health and personal data, namely:

- vendors are often the source of a security breach. Develop and implement a vendor management process that has information security as a central component. This includes regular testing or vetting of vendors. This should be done not just for vendors that touch health information, but also for any vendor that accesses systems that 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 is also 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, breaches);
- information security is a 'state' – it is continually changing. As such, the information security programme 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 healthcare purposes;
- build in risk rating assessments for any new technology that is being deployed and for any M&A targets being considered. While increased cybersecurity risk may not kill a deal, it should have an impact on pricing, earnouts and escrow; and
- 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 continues to be subject matter eligibility under 35 USC section 101. The Supreme Court has held that 'abstract ideas' are not patentable, but 'inventive concepts' are. Subject matter eligibility under section 101 remains in flux with the United States Patent and Trademark Office (USPTO) and federal courts seemingly contradicting one another or themselves at times. Some article units within the USPTO (eg, 3626), continue to take a hard line that computer-implemented digital health-related inventions are 'abstract' and merely 'methods of organising human activity'.

Digital health inventions may fall within the definition of '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 has 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 or applications

of an otherwise abstract idea. The Federal Circuit held that 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 applications and incorporate or recite hardware configured as a 'technological improvement' in a meaningful way to avoid merely claiming an abstract idea.

Congress has more recently jumped into the fray with a Senate Bill addressing subject matter eligibility and section 101, which appears to add more confusion than it resolves (and legislative support at this point is at best questionable).

On the inventorship front, the USPTO has made clear in denying a petition to list artificial intelligence (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 intellectual property 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 ornamental appearance.

For utility patent protection, an invention must be 'useful', 'novel' and 'non-obvious' (35 USC sections 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 (35 USC section 112).

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

The USPTO has created a COVID-19 Prioritized Examination Pilot Program to prioritise the examination of patent applications for inventions related to the coronavirus. The USPTO has created a similar programme for prioritising the initial examination of trademark applications. Applicants 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 2022 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 all important in protecting digital health offerings.

Copyrights are federal rights that protect original works of authorship fixed in a tangible medium (17 USC section 102). Registration is handled at the United States Copyright Office. 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' (eg, written to paper or entered into a computer. However, copyright registration is necessary to sue under copyright law). Examples of copyrightable subject matter include source code and interface designs.

Trademarks identify the 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 the 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 the secrecy of valuable information. Trade secret information must be:

- information having value by not being generally known;
- valuable to others who cannot legitimately obtain the information; and
- 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?

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

Digital health is an innovative area. Licenses need to account for modifications or improvements 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.

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 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. An OSS licence may affect

the proprietary nature of the software such as requiring disclosure, specific licensing terms to others or free use of the same software. In evaluating licenses to digital health technologies that have software components, a review for code covered by OSS licenses should be considered. Deals may be structured to limit the effects of OSS licenses once the issue is identified and thus protect confidentiality and trade secret rights.

Termination (eg, 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 the plaintiff's trade secret information regarding healthcare software, the court granted compensatory (US$140 million) and punitive monetary damages (not to exceed US$140 million), and also granted injunctive relief, including future monitoring of the 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 Health Insurance Portability and Accountability Act (HIPAA) extends to advertising and marketing, including, for example, customer testimonials. The HIPAA Privacy Rule defines marketing as 'a communication about a product or service that encourages recipients of the communication to purchase or use the product or service'.

In addition, the advertising and marketing of digital health products, like all consumer products and services, is governed by the FTC Act and regulations thereunder, which are overseen by the FTC. Section 5 of the FTC Act prohibits 'unfair or deceptive acts or practices in or affecting commerce'.

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 also governed by the Federal Food, Drug, and Cosmetic Act, which is enforced by the FDA.

Finally, each state maintains separate laws and regulations that cover the marketing and advertising of consumer products, which are enforced by state agencies and the Attorney General's office. Those that mirror the FTC Act are referred to as 'Little FTC Acts' or 'Baby FTC Acts'.

e-Commerce

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

Unique to health-related vendors and services, the Health Breach Notification Rule requires vendors of personal health records and related entities to notify consumers following a breach involving unsecured information. Other pertinent e-commerce laws include the Restore Online Shoppers' Confidence Act (ROSCA), which regulates disclosures and informed consent requirements with online transactions, and the Telephone Consumer Protection Act, which regulates telemarketing, including text messages. Stemming from ROSCA, the Prenotification Negative Option Rule makes it unlawful for any person to charge or attempt to charge any consumer for any goods or services sold online through a negative option feature absent requisite disclosures.

Other applicable laws include the FTC's Consumer Review Fairness Act, which prohibits businesses from obstructing customers from leaving reviews, even if negative and the Mail, Internet, or Telephone Order Merchandise Rule, which requires e-commerce merchants to ship all orders within the advertised time frame, or, by default within 30 days if there is no specified shipping time.

Also, there are evolving state and federal laws surrounding consumer privacy, fees and other components of e-commerce. For example, the CCPA provides, among other requirements, that businesses give consumers certain notices explaining their privacy practices. The FTC continues to monitor developments in online and mobile interfaces to introduce new regulations to uphold its mission of protecting consumers. To that end, in October 2022, the FTC announced proposed rulemaking concerning junk fees. Relatedly, electronic payment processing is subject to a myriad of other consumer protection laws, including but limited to the EFTA and Regulation E.

Because e-commerce crosses many legal territories, the foregoing is not an exhaustive list and rather highlights the key applicable laws and issue areas.

PAYMENT AND REIMBURSEMENT

Coverage

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

Yes. Both the federal Medicare programme and state Medicaid programmes feature coverage and reimbursement for telehealth services, depending on speciality, technology and site of service. The expansion of telemedicine coverage inspired by the covid-19 pandemic remains in place through at least the end of June 2023.

Private insurers are required to provide parity for telemedicine coverage and (or) payment in 43 states. A significant amount of healthcare reimbursement is also self-funded by employers under employee benefit plans that favour telemedicine for its convenience and lower cost.

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 2022, the federal and states' governments continued to support the development and use of digital health, while taking new steps to address transparency, cybersecurity and fraud. Technological advancements, including personal healthcare applications, wearables and artificial intelligence continue to proliferate across multiple specialities and modalities including cardiology and pharmaceutical development.

Payers continue to authorise additional modalities for reimbursement and states have increasingly promoted digital health adoption. Medicaid reimbursement for video telehealth is available in all 50 states, while 37 states have adopted interstate telehealth licensure compacts for physicians and nurses. At the federal level, the Advancing Telehealth Beyond Covid-19 Act of 2021 passed the US House of Representatives in 2022 and is currently with the US Senate, and the Consolidated Appropriations Act of 2022 has ensured a 151-day extension period for telemedicine expansion following the termination of the covid-19 public health emergency.

On 6 October 2022, the 21st Century Cures Act Final Rule, making a patient's electronic health information more electronically accessible at no cost, went into effect for all electronic health information. In addition, the Office for Civil Rights issued proposed revisions to the Health Insurance Portability and Accountability Act Privacy Rule, which would allow healthcare providers more flexibility in sharing patient information for care coordination purposes. Final regulations have not yet been issued.

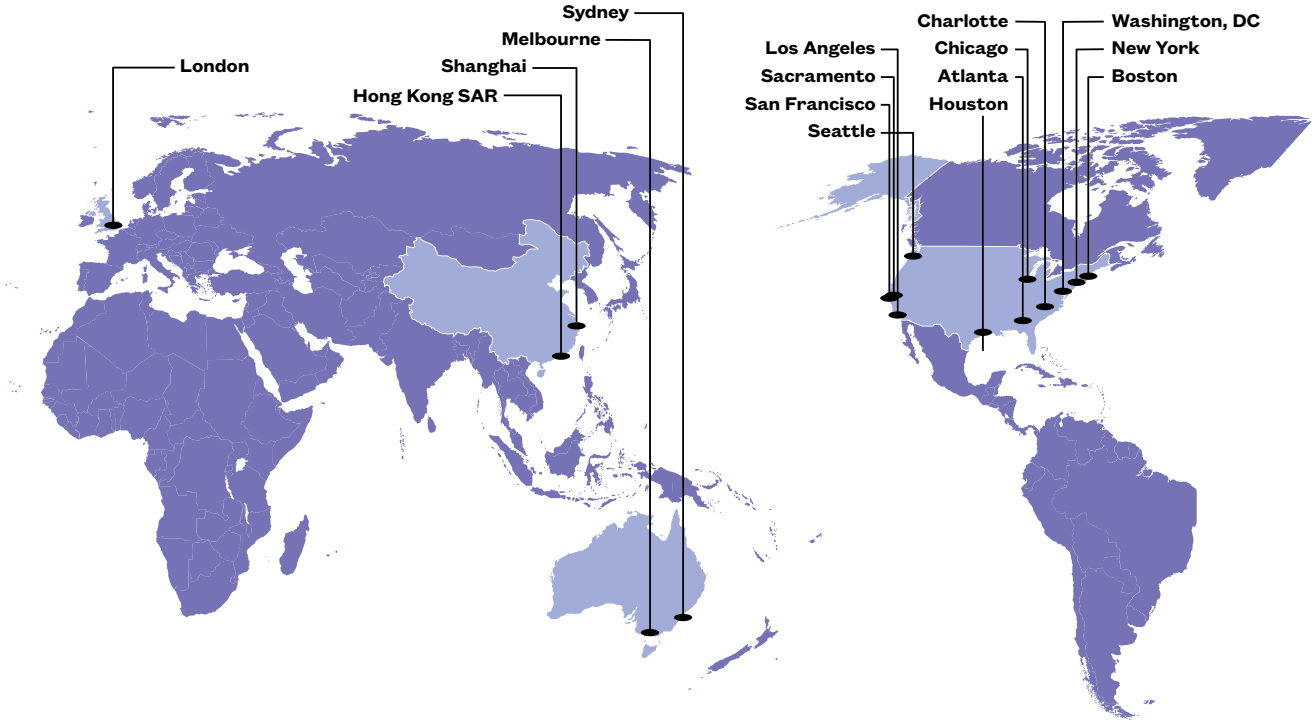
Renee B Appel	rappel@seyfarth.com
Chris DeMeo	cdemeo@seyfarth.com
Brian L Michaelis	bmichaelis@seyfarth.com
Suzanne L Saxman	ssaxman@seyfarth.com
John P Tomaszewski	jptomaszewski@seyfarth.com
Jamaica Potts Szeliga	jszeliga@Seyfarth.com
Robert S Terzoli, Jr	rterzoli@seyfarth.com
Breanne E Vaclavik	bvaclavik@seyfarth.com

975 F Street, NW, Washington, DC 20004, United States
Tel: +1 202 463 2400
www.seyfarth.com

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.



MORE TOPICS AVAILABLE ONLINE AT LEXOLOGY.COM/GTDT

Including

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