September 11, 2015

Digital health is a growing field that promises improved patient education, wellness, engagement, access to care, and outcomes, among other things. However, with these new technologies come unique regulatory concerns that digital health companies must consider. While there are a wide range of digital health companies with different focuses, some common legal issues must be considered when entering the field.

Patient data privacy and security laws

- **The Health Insurance Portability and Accountability Act (HIPAA)**: Digital health companies must consider privacy and security concerns. Any application or device that stores or transmits protected health information (PHI) and generated by or on behalf of a covered entity like a physician, hospital, or health plan, or a business associate of such an entity, will be subject to HIPAA. HIPAA does not cover personal data that is stored or transmitted through an application or device used solely by an individual; however, when information collected by an individual is provided to a covered entity or its business associate, it may become PHI subject to HIPAA.
- **State privacy laws:** In addition to HIPAA, many state laws also protect personally identifiable information which includes a broader category of information than just health information but may also specifically call out health information for protection. These laws outline breach notification obligations that digital health companies must consider when using and transmitting customer information. It is important to be aware of the laws of states where a digital health company's customers are located in addition to where the digital health company is operating.

Diagnosis and treatment and the Food and Drug Administration (FDA)

The FDA regulates devices intended for use in the diagnosis or treatment of a disease or other condition. In addition to traditional medical devices, certain mobile medical applications fall within the authority of the FDA. In early 2015, the FDA released its final guidance on mobile medical applications, stating that it intends to regulate those medical applications that are medical devices as defined under the Food, Drug, and Cosmetic Act and whose functionality could pose a risk to the patient's safety if the mobile application does not function as intended.

Consumer protection laws and the Federal Trade Commission (FTC)

The FTC protects consumers from unfair or deceptive acts or practices as well as false or misleading claims. In the digital health space, companies must be careful about the claims made regarding effectiveness. The FTC also has jurisdiction over data breaches in some instances that may apply to digital health companies beyond HIPAA and state law requirements.

Communications Devices and the Federal Communications Commission (FCC)

The FCC regulates communications devices and may include within its regulatory authority some digital health devices. The FCC and FDA entered into a Memorandum of Understanding agreeing to work together to ensure overlapping regulation does not occur. However, the possibility for some overlap still exists.

Fraud and abuse laws

Digital health companies should also consider business arrangements with providers such as hospitals and physicians. These arrangements must be structured so not to violate federal fraud and abuse laws, including the federal Anti-Kickback Statute and the Stark Law, and comparable state laws. The federal Anti-Kickback Statute prohibits knowingly offering, paying, soliciting, or receiving any remuneration to induce referrals of items or services reimbursable by a federal health care program. The federal Stark Law prohibits physicians from referring Medicare patients for designated health services to an entity with which the physician

has a financial relationship (including ownership and compensation arrangements), and prohibits the submission of a claim for reimbursement for services rendered pursuant to a prohibited referral. Many states have comparable state laws, some of which are broader and apply to services reimbursed by any source, not only services reimbursed by government health care programs. Digital health companies that provide marketing of or generate leads for health care services, for example, may implicate these laws. Care must be taken to structure digital health services to comply with such laws and to take advantage of available exceptions, where possible.

Licensure

Digital health companies that engage in telehealth should be aware of state licensure rules. There is no single standard adopted by each state in connection with telehealth licensure. Most states deem health care professionals, including physicians, to be practicing where the patient resides and require licensure in that state. For digital health companies offering patients access to licensed professionals nationwide, such businesses may implicate licensure requirements in all 50 states. Digital health companies must ensure that the health care professionals with whom they contract are appropriately licensed, have a process for confirming licensure, and are solely responsible for practicing within their licensed jurisdiction(s).

Corporate practice of medicine

The Corporate Practice of Medicine ("CPOM") doctrine may prohibit an unlicensed business corporation from practicing medicine or employing physicians to do so. Certain states have a broad CPOM doctrine that extends to different types of health care professionals, such as dentists and physical therapist, while other states do not recognize the CPOM doctrine at all. Some states have exceptions to this general doctrine. Accordingly, digital health companies that seek to provide access to medical or other health care services must structure their businesses to comport with relevant state CPOM laws.

Fee-splitting prohibitions

Certain states prohibit licensed professionals and/or licensed facilities from sharing their professional fees with unlicensed entities and individuals, also known as "fee-splitting". Payments must be appropriately structured to comply with state fee-splitting prohibitions.

Cooley has digital health regulatory attorneys experienced in structuring business arrangements to comply with these and other relevant legal requirements. Please contact any of the authors of this client alert for assistance.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as “Cooley”). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. This content may be considered **Attorney Advertising** and is subject to our legal notices.

Key Contacts

Phil Mitchell New York	phil.mitchell@cooley.com +1 212 479 6581

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.