

# Mass. Digital Health Developments: What To Know Now

By **Ellen Janos**

Digital health, a term that includes telemedicine, remote patient monitoring, direct to consumer virtual visits, and health apps for smartphones, is now an accepted part of the health care delivery system and has been widely adopted by both health providers and consumers. According to a recent report, the market for digital health was estimated at 2.78 billion in 2016 and is expected to reach 9.35 billion by 2021.[1] The technology is evolving very quickly and counsel for businesses entering this market must keep up with a complex legal and regulatory landscape. Below are some key questions to ask when assessing a digital health service or product.



Ellen Janos

## What is the Digital Health Service or Product Being Offered?

When counseling a business that is entering the digital health market, first ask: What type of services will be provided? Who will provide the services? Will they involve the use of a medical device or health app? The answers to those questions will often dictate the type of corporate entity that must be formed and whether the device or app is subject to regulation by the U.S. Food and Drug Administration or the Federal Trade Commission.

## Entity Formation

If the digital health service includes clinical services furnished by a licensed health care practitioner, those services must be provided through an appropriate legal entity. It is well accepted that Massachusetts prohibits the "corporate practice of medicine"[2]. In 2012, the Massachusetts Board of Registration in Medicine codified a long-standing practice of allowing physicians to practice through licensed entities such as hospitals and clinics or through a nonprofit entity. Therefore, unless these exceptions apply most services provided by licensed health care professionals must be provided through a corporation (or a limited liability company) that meets the ownership and control requirements under the professional corporation laws. A for-profit digital health company that is planning to provide services directly to consumers has various legal strategies to consider that will address the corporate practice of medicine including contracting with a professional corporation or a professional limited liability company to provide the clinical services.

## Professional Standards

If licensed professionals are providing services, attention must be paid to the professional standards for that particular professional. Numerous states have established rules or guidance that dictates many aspects of a telemedicine visit including for example, how and when the physician/patient relationship is established. In contrast, the Massachusetts Board of Registration in Medicine and the Massachusetts Board of Registration in Nursing, among other professional licensing boards, have not set out specific standards for care delivered via telemedicine.

The Board of Registration in Medicine has issued guidance regarding prescriptive practice cautioning that the use of telemedicine to prescribe should be in accordance with current standards of practice and carry the same professional accountability as prescriptions delivered during an encounter in

person.[3]

To the extent that professional services will be carried out by nonphysicians such as nurse practitioners or physician assistants, it is important to ensure that any applicable supervision requirements, such as the written collaboration agreements necessary to oversee a prescriptive practice for nurse practitioners and physician assistants, are met.

## **Regulation of Devices and Apps**

Whether or not the business model contemplates the involvement of a clinician, a key consideration is whether a device or app that is used in connection with the service offering is regulated by the FDA. The law and guidance on whether a health-related device or mobile app is subject to regulation is continuing to evolve.

In general, the FDA regulates medical devices that are intended for use in the diagnosis of disease, or in the cure, mitigation, treatment or prevention of disease.[4] With the growth of mobile apps and health-related software, the FDA, through guidance documents, took a risk-based approach that distinguished applications, hardware and software that might qualify as a medical device subject to regulation from health trackers, disease management apps, and apps providing generalized medical information that would be exempt from regulation or would not fall under FDA jurisdiction at all. Congress recently stepped in through the Cures Act and amended the definition of a medical device to exclude certain digital health technologies such as those that provide administrative support or those that help to maintain or encourage a healthy lifestyle.[5] The FDA will be issuing guidance under this law but, in the meantime, the FDA has signaled its intention to focus only on a small subset of health apps that pose a higher risk to patients if they do not work as intended.

In addition to the potential regulation by the FDA, digital health companies need to be aware of the federal and state truth in advertising laws that will apply to misleading claims about safety or performance. The FTC has been aggressively enforcing the FTC Act which prohibits "unfair or deceptive acts or practices in or affecting commerce".[6] The Massachusetts Office of the Attorney General has long been a leader in the enforcement of unfair and deceptive practices and it can be expected to be just as aggressive in the digital health space using the Massachusetts Consumer Protection Act (Chapter 93A).

## **Protecting Patient and Personal Data**

### **Does HIPAA Apply?**

Data privacy and security is one of the most important legal issues and operational risks for a digital health company. The first question is whether the company is regulated by the Health Insurance Portability and Accountability Act. HIPAA only covers "protected health information" or PHI that is created, collected or maintained by health care providers (covered entities) or companies that provide services to covered entities and as part of those services accesses or uses PHI (business associates). If the business is a covered entity or business associate, the HIPAA privacy rule imposes limits and conditions on the uses and disclosures that may be made of PHI without consumer authorization and gives consumers rights over their health information. Some of the HIPAA requirements such as the "Notice of Privacy Practices" and written authorizations are challenging for digital health companies especially when used on a mobile platform. The HIPAA security rule mandates, such as implementing administrative, physical and technical safeguards, may be less daunting as they can be tailored to the size and scope of the business.

Technology companies and other vendors that service health care providers as business associates will need to enter into business associate agreements (BAAs) with covered entity customers. When drafting a BAA for a digital health company, it is important to watch out for onerous indemnification provisions that covered entities often seek to include.

One of the most important obligations for both covered entities and business associates under HIPAA is the reporting of data breaches. Covered entities must undertake a four-factor risk assessment to determine whether or not the PHI has been compromised and has to be reported to the federal Office for Civil Rights as well as to the patient. Business associates must report such breaches to the covered entity.

Keep in mind that many digital health services and products obtain health data directly from the patient or consumer, which may not be data that is protected under HIPAA. Customer contracts and consumer-facing materials should be clear as to whether the data that is maintained by the business is subject to HIPAA.

### **Massachusetts Data Security Law**

Whether the digital health business is covered by HIPAA or not, if the business collects or maintains "personal information" from Massachusetts consumers or its Massachusetts employees it will be subject to the Massachusetts data security law.[7] Personal information is defined as a resident's first name and last name or first initial and last name in combination with financial information such as a Social Security number, a driver's license number, or credit card or other financial account number.[8] Businesses covered under this law are required to develop, implement and maintain a comprehensive written information security program or "WISP" that contains administrative, technical and physical safeguards that are appropriate to the size, scope and type of business.

The data security law requires that data containing personal information be encrypted during wireless transmission and while stored on laptops or other portable devices.[9] Any unauthorized acquisition or unauthorized use of unencrypted data must be reported to the Office of the Attorney General, which has broad enforcement authority, as well as to the consumer.

### **Getting Paid**

Payment and coverage for services delivered via telemedicine are one of the biggest challenges for telemedicine adoption. Patients and health care providers may encounter a patchwork of arbitrary insurance requirements and disparate payment streams that do not allow them to fully take advantage of telemedicine." — American Telemedicine Association, 50 State Telemedicine Gap Analysis: Coverage & Reimbursement

For Massachusetts-based telemedicine providers payment continues to be a challenge. Efforts by the Massachusetts Legislature to pass parity laws have failed thus far. The parity laws passed by state legislatures around the country typically are limited to coverage parity — that is, private payors must cover telehealth services and not impose additional limitations on coverage provided via telehealth. More important for providers is reimbursement parity which requires payers to reimburse telemedicine services at the same rate as in-person services.

Despite the lack of a parity law, many Massachusetts insurers have begun to offer telehealth services to their members and provide reimbursement to their providers. Payment rules are typically found only in the insurers' telehealth payment policy or provider manual. These payment rules vary a great deal, with some insurers requiring a two-way video conference and others dictating the location of the patient (i.e., in the hospital or physician office and not at home).

Reimbursement is much more limited on the government payer side. Medicare will only reimburse for telehealth when the patient is present at a specific location (e.g., in a county outside of a Metropolitan Statistical Area or in a Health Professional Shortage Area). Each year, a number of bipartisan bills are introduced in Congress aimed at expanding Medicare coverage for telehealth services.

Unlike most states, MassHealth does not reimburse for telehealth services under its fee-for-service program. Fortunately, beginning in January 2018, MassHealth is expected to cover almost 1 million members under its accountable care organization program providing new opportunities to include digital health into the care delivery system for Medicaid beneficiaries.

## What's Ahead?

Digital health companies will play an increasingly important role in the health care delivery system as payers continue to look for ways to bring down the costs of health care while improving access, quality and patient outcomes and will rely on counsel to stay on top of the fast-moving legal environment.

---

*Ellen L. Janos is a member at Mintz Levin Cohn Ferris Glovsky and Popeo PC in Boston. She previously served as an assistant attorney general for the Commonwealth of Massachusetts.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

[1] <http://www.marketsandmarkets.com/PressReleases/telehealth.asp>

[2] *McCurdo v. Getter*, 10 N.E.2d 139 (Mass. 1937) (enjoining a corporation from practicing optometry through employment of licensed optometrists).

[3] Board of Medicine Prescribing Practices Policy and Guidelines (Policy 15-05 Adopted Oct. 8, 2015).

[4] 21 U.S.C. § 321H.

[5] Public Law 114-255, § 3060.

[6] Section 5(a) of 15 U.S.C. 45(a); see <https://www.ftc.gov/news-events/press-releases/2016/12/marketers-blood-pressure-app-settle-ftc-charges-regarding> (marketer of blood pressure app settles charges regarding the accuracy of readings).

[7] G. L. c. 93H.

[8] G. L. c. 93H, § 1.

[9] 201 CMR 17.04(3) and (5).