Bloomberg BNA

Health IT Law & Industry Report™

VOL. 8, NO. 19 MAY 9, 2016

BLOOMBERG BNA INSIGHTS

Digital Health 101: There's No Regulator-Free Path to the Digital Health Market

BY JAMES DEGRAW AND IRA PARGHI

The aggressive growth of digital health has brought with it a spate of regulatory activity, with the U.S. Department of Health and Human Services Office for Civil Rights ("OCR"), Food & Drug Administration ("FDA"), and Federal Trade Commission ("FTC") all engaging in enforcement activity and attempting to provide guidance on a range of issues.

James DeGraw is a partner in Ropes & Gray's corporate technology group in San Francisco. He can be reached at james.degraw@ropesgray.com.

Ira Parghi is of counsel in Ropes & Gray's health-care law group in San Francisco and a member of the firm's privacy & data security group. She can be reached at ira.parghi@ropesgray.com.

What are the rules in this brave new world? And who enforces them?

But new and established players in the digital health sphere often look at all this activity and come away befuddled. They often ask: What are the rules in this brave new world? And who enforces them?

The answer often depends on non-obvious relationships between individual consumers, devices, and data handlers. This article clarifies at a high level the scope of authority of the OCR, FDA, and FTC with respect to digital health-related matters. It also touches on other laws on personal information and particularly sensitive health information that may be relevant in the digital health space.

 ISSN 2151-2876

''Digital health'' is itself a broad and sometimes unclear term. It encompasses a wide range of technologies and products, from electronic health records and personal health records to health-related software applications (including mobile life style or medical apps), medical devices, and ''wearable'' technologies.

Office for Civil Rights

Perhaps the most widely known health information privacy statute is the Health Insurance Portability and Accountability Act (''HIPAA''), which is enforced by the OCR. HIPAA applies to ''covered entities'' (health care providers, payers, and clearinghouses) and ''business associates'' (entities that obtain Protected Health Information (''PHI''), or identifiable medical information, from covered entities in order to perform certain functions or activities on behalf of the covered entities).

It is a fairly prescriptive statute and places a broad range of privacy and information security-related obligations on both covered entities and business associates.

HIPAA only applies to those entities acting in those contexts. This leaves outside of HIPAA's scope a wide range of actors and, by extension, applications and tools.

But HIPAA only applies to those entities acting in those contexts. This leaves outside of HIPAA's scope a wide range of actors and, by extension, applications and tools.

As the OCR expressly stated in a recent guidance document, HIPAA does not apply to ''direct to consumer'' software, applications, or other digital health products. This is because any health information collected or processed by such products is directly from, and for, the consumer.

What is counter-intuitive about this is that a covered entity itself provided a consumer an app that collects, stores, and/or transmits what HIPAA deems to be PHI—even if similar to a consumer-focused app—then the product would be subject to HIPAA.

Likewise, a software developer that contracts with a covered entity to collect, maintain, or transmit PHI through a software program is deemed to be a business associate under HIPAA, and accordingly will be subject to HIPAA requirements.

The OCR guidance poses a number of questions intended to help application developers and other players in the digital health space evaluate whether their products are governed by HIPAA. These questions include:

(1) whether the application creates, receives, maintains or transmits identifiable information;

(2) who the clients for the application are, and whether those clients include covered entities or business associates;

(3) whether the application is independently selected by the consumer;

(4) whether all decisions to transmit health data to third parties are controlled by the consumer; and

(5) whether the developer has any contractual or other relationships with third party entities, other than interoperability agreements.

If an application developer or other company is found to be a business associate under HIPAA, it becomes subject to a number of requirements, both legal and operational.

It is required to have business associate agreements with its covered entity customers, and to use PHI only in ways expressly permitted by those agreements. It must comply with those HIPAA provisions that apply to business associates, including those on risk analysis, policies, training, and audits. It must also satisfy particular HIPAA requirements if it wishes to buy or sell PHI, de-identify PHI, or aggregate data from more than one customer.

Even if an application developer avoids direct HIPAA regulation, as explained below, the FTC may still regulate the application in complementary ways to those of the OCR. And the application may also still be subject to FDA oversight.

Food & Drug Administration

The FDA has, like the OCR, issued guidance on the applicability of the Food, Drug & Cosmetic Act (''FDCA'') to health- or life-style-related apps. That guidance emphasizes that such an application may be subject to the FDCA only when it meets the FDCA's definition of ''medical device,'' and is intended to either be used as an accessory to a regulated medical device, or to transform a mobile platform into a regulated medical device.

If the application is intended to be used to diagnose, cure, mitigate, treat, or prevent a disease or condition, or to affect the structure or any function of the body, it is a device.

The application's intended use is evaluated with reference to its labeling claims, advertising materials, and statements made by its manufacturers. Thus, for instance, an app that simply is intended to be used by a physician as an educational tool will not constitute a medical device and will not be subject to the FDCA's requirements.

If a digital health product does meet the definition of ''device,'' then, if it could endanger patient safety were it not to function as intended, it will be subject to FDA regulation.

If a digital health product does meet the definition of ''device,'' then, if it could endanger patient safety were it not to function as intended, it will be subject to FDA regulation.

The FDA has identified categories of apps that would meet this requirement. They include:

   ISSN 2151-2876

(1) apps that function as extensions of medical devices by connecting to the devices to control them or for use in patient monitoring or the analysis of device data (such as an app that controls the inflation of a blood pressure cuff);

(2) apps that use attachments, display screens, or device-like functionalities to transform mobile platforms into regulated medical devices; and

(3) apps that perform patient-specific analysis and provide patient-specific diagnosis or treatment recommendations.

Otherwise, however, the FDA will exercise ''enforcement discretion'' with respect to the product, that is, not enforce the requirements of the FDCA, even if it meets the definition of ''device.''

Of note, the FDA has carved out ''general wellness'' apps that pose a low risk to user safety, such as apps that encourage health activities without referring to specific diseases or conditions, or which help patients document their potential medical conditions. Thus, like the OCR, it has explicitly exempted from its regulatory reach direct-to-consumer, lifestyle-oriented digital health products.

The FDA has enumerated different categories of mobile medical apps that will typically be subject to enforcement discretion. They include apps that:

(1) coach or prompt patients to manage their daily health;

(2) provide patients with tools to organize and track their health information;

(3) provide access to information about patients' health conditions or treatment;

(4) help patients document potential medical conditions or communicate them to their health care providers;

(5) perform simple calculations routinely used in clinical practice;

(6) let patients interact with their personal health records or electronic health record systems; and

(7) meet the definition of a medical device system.

Federal Trade Commission

The FTC sees itself as a regulatory gap-filler in situations in which consumer interests are at play. It has long regulated privacy and security practices pursuant to its authority to regulate unfair and deceptive acts and practices under the Federal Trade Commissions Act (''FTCA'').

This includes health information, with respect to which the FTC has asserted a growing role and articulated the view that it does so because existing regulations do not adequately protect health data.

It has, for example, engaged in enforcement activity against a medical testing laboratory whose patient information was found to have been accessible through a file sharing network. That laboratory, of note, was also a covered entity subject to HIPAA.

Similarly, the FTC has taken enforcement action against a provider of dental office management software that was alleged to have deceptively claimed that its products bore industry-standard encryption that would help clients satisfy their obligations under HIPAA. That software company was a business associate under HIPAA.

These cases raise the prospect of overlapping jurisdiction and multiple sets of legal and regulatory obligations for those in the digital health space, and indeed the health care industry generally.

These cases raise the prospect of overlapping jurisdiction and multiple sets of legal and regulatory obligations for those in the digital health space, and indeed the health care industry generally.

The FTC has also been active against health care apps engaged in alleged deception—again, an example of the FTC weighing in on issues that traditionally would have rested in the domain of the FDA. For example, the FTC charged two mobile medical apps developers for claiming that their apps could detect symptoms of melanoma, even in the early stages, alleging that the companies had no evidence to show that their apps could detect melanoma.

It also charged the developers of an app that claimed to be ''scientifically shown to improve vision,'' alleging that the developers did not have scientific evidence to support that claim.

Other aspects of the FTC's enforcement activities are more readily identifiable as falling outside of the purview of the OCR and FDA.

In particular, and in a case with important implications for all players in the digital health space, the FTC has on at least one occasion targeted a consumer-facing company that engaged in alleged deceptive practices that resulted in information mishandling.

In that case, it charged a health billing company with using deceptive registration processes to trick consumers who used its online billing portal into also consenting to the collection of their medical information from pharmacies, medical laboratories, and insurance companies.

Other Regulators

State attorneys general and other state-based and federal regulators also play a potential role in the regulation of digital health products. For example, if an entity is receiving, using, or storing health information but does not do so as a covered entity or business associate, it will not be subject to HIPAA.

However, it may still be subject to state or federal laws that govern particularly sensitive types of information. Such information may relate to HIV/AIDS testing or status, alcohol or drug abuse-related care, or behavioral health care.

If an entity works with information that is sensitive but not PHI, it will not be bound by HIPAA, but it may still be subject to state laws protecting ''personally identifiable information'' (''PII''), which typically includes

sensitive information that is not health-related, such as Social Security numbers or driver's license numbers.

Some states, such as California, have robust legal regimes governing the handling of medical information, and digital health players would be advised to familiarize themselves with their privacy obligations under those laws, as well as those under HIPAA and the FTCA.

Significantly, some states, such as California, have robust legal regimes governing the handling of medical information as well, and digital health players would be advised to familiarize themselves with their privacy obligations under those laws, as well as those under HIPAA and the FTCA.

All of this has yielded a potentially confusing regulatory landscape for digital health industry players. As recent press reports show, companies that attempt to participate in the digital health space would be well advised to keep this landscape well in mind during all phases of product development—and not simply think that if one particular regulatory schema does not directly apply to an application, that none do now or will in the future.

  HITR ISSN 2151-2876