CLA
CALIFORNIA LAWYERS ASSOCIATION

Vol 27, No. 1
Winter 2017-18

The Journal of the Antitrust, UCL and Privacy Section of the California Lawyers Association

Articles

DIGITAL HEALTH PRIVACY: OLD LAWS MEET NEW TECHNOLOGIES

By Reece Hirsch and Jenny Harrison[1]

I. INTRODUCTION

When the Health Insurance Portability and Accountability Act ("HIPAA") was enacted in 1996, the smart phone was not even a gleam in Steve Jobs' eye, and mobile health apps and cloud computing did not exist. Even though the primary regulations implementing and amending HIPAA became effective in 2003, 2005, and 2013, regulators and lawmakers continue to play catch-up, striving to apply HIPAA's regulatory framework to an ever-evolving technology landscape.

Recent years have seen the proliferation of devices and applications that permit consumers to create, store and share health information like never before, from activity trackers to personal health records ("PHRs"). This type of information, which exists outside the traditional medical record maintained by healthcare providers, is often referred to as "consumer-generated health information" ("CHI"), and it has caught the attention of the regulators.[2]

The main regulators of the digital health field are the Department of Health and Human Services Office for Civil Rights ("OCR") and the Federal Trade Commission ("FTC"), along with state attorneys general. OCR has jurisdiction under HIPAA to regulate HIPAA-covered entities (*i.e.*, healthcare providers that engage in standard electronic transactions, health plans, or healthcare clearinghouses) and business associates of those entities. The FTC derives its jurisdiction from Section 5 of the Federal Trade Commission Act (the "FTC Act"), which empowers the agency to regulate "unfair or deceptive acts or practices." A business may fall under the FTC's authority if it makes an inaccurate or misleading statement in its website privacy policy (a potentially deceptive practice) or has inadequate security that is inherently unfair or harmful to consumers (a potentially unfair practice).

State attorneys general have the authority to regulate unfair and deceptive practices that are parallel to the FTC's, under the so-called "baby FTC Acts." State AGs also have the authority to enforce HIPAA since enactment in 2009 of the Health Information Technology for Economic and Clinical Health ("HITECH") Act, which amended HIPAA. This article will review (i) how HIPAA privacy and security standards are being applied to new technologies like mobile health apps, activity trackers, personal health records and cloud computing vendors, and (ii) how to determine which agencies have the authority to regulate these new domains, and under what circumstances.

---

1 Reece Hirsch is a partner in the San Francisco office of Morgan Lewis and co-head of the firm's Privacy & Cybersecurity Practice, specializing in healthcare privacy and security matters. Jenny Harrison is Corporate Counsel, Privacy at Salesforce in San Francisco.

2 FTC Commissioner Julie Brill has made it clear that CHI is considered sensitive and requires greater protections than other types of consumer data. *See* Fed. Trade Comm'n, Consumer Generated and Controlled Health Data (May 7, 2014 seminar).

II. OCR'S JURISDICTION AND APPLICATION OF HIPAA

HIPAA's privacy and security requirements apply only to a limited group of covered entities: healthcare providers that engage in standard electronic transactions, health plans, healthcare clearinghouses, and business associates of those entities. A mobile app developer that collects health information may be subject to HIPAA's requirements, but only if it is considered a business associate of a covered entity.

A. Who Qualifies as a Business Associate?

Under HIPAA, a business associate is a person or entity acting on behalf of a covered entity that creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA (*i.e.*, a covered entity function).[3] If an entity is found to be a business associate, then it must comply with certain security and privacy requirements. The key language for many companies is whether it is "acting on behalf of a covered entity." If a company provides a service directly to the consumer, then it is not a business associate because an individual patient or consumer is not a covered entity. However, a company may be a business associate if it provides the same service to individual patients or health plan members on behalf of a covered entity.

One practical litmus test for the "acting on behalf of" question is who pays for the service. If the consumer is the customer and pays directly for the service, then the company is most likely not a business associate. However, if a covered entity is the customer, then the company is most likely a business associate and would be subject to HIPAA regulation. There is a gray area when a provider only partially pays for the service, for example if the provider only pays for 75% of a fee or provides a partial rebate. OCR has yet to issue sufficient guidance to resolve some of these questions, so it is up to the developer to assess its connection to covered entities and to determine whether it qualifies as a business associate or not.

B. Consequences of Business Associate Status

If a company is a business associate, it is governed by the HIPAA privacy rules and may only use and disclose PHI as provided in the company's business associate agreements with covered-entity customers. If a company is not a business associate, then its privacy policies are governed by FTC privacy principles and the terms of the company's own posted privacy policy. Thus, business associate status has an enormous impact on the business's information collection and disclosure practices. As a business associate, a developer can, with limited exceptions, only use and disclose PHI to provide the contracted services to the covered entity. If the company is not a business associate, it will have greater latitude to use and disclose collected personal information, so long as there is disclosure and appropriate consent obtained through the privacy policy.

Because different privacy and security standards apply depending on the developer's business associate status, it may be necessary to segregate personal information if the developer has both business associate and direct-to-consumer operations.

---

3 45 C.F.R. § 160.103 (2014).

III. APPLYING EXISTING LAWS TO NEW TECHNOLOGIES

Each year brings the introduction of new devices and applications that collect, use, and disclose CHI and PHI. Existing privacy regulatory regimes typically do not contemplate, and may be a poor fit for, these new technologies. In the face of this onslaught, federal and state regulators have tried different enforcement strategies to keep pace with new technological advances and societal trends.

A. Mobile Apps

There are thousands of health-related mobile apps that collect and track health information, connect patients with their healthcare providers, or provide other health services. Whether a mobile app developer is considered a business associate is a case-by-case factual determination, often turning on whether the developer is "acting on behalf of a covered entity." In February 2016, OCR issued guidance for mobile health app developers.[4] The guidance provided six examples of how HIPAA applies and does not apply to mobile apps that collect, store, manage, organize, or transmit health information.

Under OCR's guidance, a mobile app is not considered a business associate if it simply allows a consumer to input her own health information and there is no relationship between the mobile app and the consumer's healthcare providers or health plan.[5] In such a scenario, the mobile app is acting on behalf of the consumer, not a covered entity, and, therefore, is not a business associate.

A mobile app developer is still acting on behalf of the consumer, and, therefore, is not considered a business associate, if its app allows a consumer to input personal information or access a healthcare provider's test results, or the app transmits the information to the provider at the consumer's direction.[6] If the developer and healthcare provider have an interoperability arrangement, entered into at the consumer's request to facilitate the secure exchange of health information, the developer is still not a business associate because such an agreement is intended to facilitate access to health information initiated by the consumer. A developer would be considered a business associate if it contracts directly with a healthcare provider for patient management services, such as for remote patient health counseling, monitoring patients' food and exercise, or patient messaging.[7]

To assist mobile app developers in assessing their business associate status, OCR, along with the FTC and FDA, have developed a Mobile Health Apps Interactive Tool. This tool can be used to assist developers in determining whether the app is subject to HIPAA, the FTC Act, the FTC's Health Breach Notification Rule, and/or the Federal Food, Drug and Cosmetic Act.[8]

---

4 U.S. Dep't of Health & Human Servs., Office for Civil Rights, Health App Use Scenarios & HIPAA (2016), https://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/OCR-health-app-developer-scenarios-2-2016.pdf.

5 *See id.* at 2 (scenario 1).

6 *See id.* (scenario 2).

7 *See id.* (scenario 3).

8 Fed. Trade Comm'n, Mobile Health Apps Interactive Tool, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool (last visited Sept. 29, 2017).

1. Recent Actions Involving Mobile Apps

In March 2017, New York Attorney General Eric Schneiderman settled with three health app developers for "misleading claims and irresponsible privacy practices" that violated New York's consumer protection laws. The three health measurement apps purported to measure vital signs without the assistance of any external device. For example, the "My Baby's Beat" app claimed users could monitor a fetus' heartbeat by holding a smartphone running the app to a pregnant woman's stomach. The apps made marketing claims comparing them to traditional medical devices, but they were never submitted to the FDA. The Attorney General found the app privacy policies to be inadequate on a number of grounds, including (i) collecting geolocation data without disclosing that fact, (ii) stating that GPS could be turned off without providing that option, and (iii) presuming consent to the policy through use of the app. The developers also should not have compared their apps to FDA-regulated devices when the app had not been submitted to the FDA. The settlements required the three developers to amend their marketing claims, modify their privacy policies, consent to monitoring, and pay fines ranging from $5,000 to $20,000.[9]

In April 2017, Massachusetts Attorney General Maura Healey entered into a no-fault settlement agreement with a digital advertising company, Copley Advertising, for its geofencing activity. "Geofencing" technology enables a user to create virtual fences and then to "tag" smartphones and other mobile devices as they enter or leave that area. Targeted third-party ads can then be displayed once the phone user opens a mobile app or web browser. The Attorney General alleged that Copley had set virtual fences around reproductive health clinics and methadone clinics in several states, targeting an advertisement about alternatives to abortion to be delivered when GPS data showed that an individual was near a reproductive health clinic. The settlement provides that Copley will not use geofencing technology at or near Massachusetts healthcare facilities to infer the health status, medical condition, or treatment of any individual.[10] If properly disclosed in a privacy policy in accordance with FTC privacy principles, it is possible that geofencing may be permissible, but this is a relatively new practice and the law is still unsettled in this area.

B. Internet of Things

The Internet of Things ("IoT") refers to physical devices or items connected to each other or to the internet, such as smart televisions or home security appliances. In November 2015, Gartner, Inc. estimated that the number of devices connected to the

---

9 N.Y. State Attorney Gen., A.G. Schneiderman Announces Settlements with Three Mobile Health Application Developers for Misleading Marketing and Privacy Practices, https://ag.ny.gov/press-release/ag-schneiderman-announces-settlements-three-mobile-health-application-developers (last visited Sept. 29, 2017).

10 Mass. Attorney Gen., AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities, http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-04-04-copley-advertising-geofencing.html (last visited Sept. 29, 2017).

Internet would exceed 20 billion by 2020. Many of these devices, such as activity trackers and smart medical devices, collect CHI. There is no privacy law that generally regulates IoT data collection and security, but in May 2015, former FTC Commissioner Julie Brill declared that the FTC's enforcement powers extended to privacy and security risks posed by the IoT based on its Section 5 jurisdiction over unfair and deceptive trade practices.[11] Thus, IoT developers must be mindful of what they tell their consumers regarding their data collection and use practices, and what the consumers understand about those practices.

Privacy regulation is based on traditional notions of notice and consent, but these concepts are often difficult to apply to IoT devices. Former FTC Commissioner Brill urged companies to "get creative" about providing privacy transparency and control for consumers to manage their data.[12] For example, a household "command center" could run multiple household devices and describe in simple, consolidated terms how those devices collect and use information. In January 2015, the FTC issued a reported titled "*Internet of Things: Privacy & Security in a Connected World*," which was based on input from technologists, academics, industry representatives, and consumer advocates, at a November 2013 FTC workshop in D.C.[13] The report provided recommended practices and potentially provides insight into future FTC enforcement actions, but it does not have the force of law.

C. Activity Trackers

Activity and fitness trackers are particularly prolific IoT devices that collect and record CHI, such as number of steps per day and heart rate. These devices raise many of the same privacy regulatory issues as health mobile apps. When activity trackers are sold directly to the consumer, the company is not a HIPAA business associate because it is acting on behalf of the consumer, not on behalf of a covered entity. However, a business associate relationship may be triggered if a health plan becomes involved, such as an arrangement in which a health plan purchases activity trackers for its members. In that scenario, business associate status will depend on the specific facts and circumstances of the relationship, such as (1) the degree of control the plan member has over the choice of the device and the sharing of information, and (2) whether the health plan purchases the device or merely recommends it to the member.

The analysis changes when an employer provides activity trackers to its workforce. Such an arrangement probably does not trigger a business associate relationship because the employer is acting in its capacity as an employer, and not a HIPAA-covered entity. However, a business associate relationship may exist if the activity trackers are provided to the employer's group health plan, which is separate and legally distinct from the

---

11 Fed. Trade Comm'n, Data Protection & the Internet of Things (2015), https://www.ftc.gov/system/files/documents/public_statements/640741/2015-05-04_euroforum_iot_brill_final.pdf (Federal Trade Commissioner Judy Brill's keynote address at the EuroForum European Data Protection Days).

12 *Id.*

13 Fed. Trade Comm'n, Internet Of Things: Privacy & Security In A Connected World (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

employer and plan sponsor. Employer group health plans are almost always health plan covered entities under HIPAA.

Activity trackers face the same issues as IoT devices, generally, regarding traditional notice and consent requirements. Wearable fitness trackers typically do not have a user interface to present consumers with choices about data collection. As with IoT devices, activity trackers must be more inventive in developing approaches to privacy notice and consent.

D. Cloud Computing

Another relatively recent and ubiquitous technology, cloud computing, also raises unique privacy and security issues in the healthcare industry. OCR issued guidance in 2016 on cloud computing and HIPAA, recognizing the proliferation of cloud-based electronic medical records and cloud services offering access to networks, servers, storage, and applications. Prior to the HIPAA Final Rule's 2013 compliance date, cloud service providers ("CSPs") were not business associates if they did not access, use, or disclose PHI. In 2013, the business associate definition was modified to include "maintaining" PHI as a basis for a business associate relationship, which thus encompasses CSPs.[14]

In commentary to the HIPAA regulations, OCR created an exception to the business associate rules known as the "conduit" exception.[15] Under this exception, a transmission-only service for PHI is not a business associate, so long as the transmission service is the only service that the company is providing to the covered entity. This applies to paper transmission providers, such as couriers and the post office, and electronic transmission providers, such as certain telecommunications providers and messaging services. Any access to the PHI by a conduit must be "random and infrequent" and "transient in nature." CSPs would not qualify for this conduit exception.[16]

A CSP is still considered a business associate and must abide by the HIPAA security regulations (the "Security Rule") when the CSP only receives encrypted data and does not have an encryption key for the data. OCR refers to such data and services as "no-view" services. "No-view" data is still considered PHI and encryption of data does not exempt a CSP from Security Rule standards. Thus, the CSP must still be aware of and protect against potential risks, such as corruption of data by malware, physical security risks, or data recovery in emergency or disaster situations.

OCR has acknowledged that, when a CSP provides no-view services, it may be appropriate for the covered entity and the business associate to share Security Rule responsibilities.[17] For example, if the covered entity controls who can view PHI, then it may take responsibility for access controls, like authentication or unique user

---

14 45 C.F.R. § 160.103 (2014).

15 *See* 78 Fed. Reg. 5,566, 5,572 (Jan. 25, 2013); *see also* U.S. Dep't of Health and Human Servs., Office for Civil Rights, https://www.hhs.gov/hipaa/for-professionals/faq/245/are-entities-business-associates (last visited Sept. 28, 2017).

16 *See* U.S. Dep't of Health and Human Servs., Office for Civil Rights, https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html (last visited Sept. 28, 2017).

17 *Id.*

identification, while encryption may be a more appropriate function for the CSP. The parties can divvy up security responsibilities based upon their respective security risk management plans. However, even when the covered-entity customer controls authenticating access to ePHI, the CSP may be responsible for internal controls governing authorized access to the administrative tools that manage the resources, such as storage memory, network interfaces and central processing units. Contracts for cloud services can allocate responsibility for compliance with various Security Rule standards. OCR has indicated that it will take that sort of allocation of duties into account when assessing responsibility in an enforcement action.[18]

A covered entity or business associate may use a CSP that stores ePHI on servers outside the U.S. if applicable HIPAA requirements are satisfied. However, if ePHI is being maintained in a country where there are documented increased attempts at hacking or other malware attacks, those risks should be taken into account in the entity's risk analysis and risk management processes.

E. Personal Health Records

There is no universal definition for a personal health record ("PHR"), but it is generally considered to be an electronic record of an individual's health information by which the individual controls access to the information and may have the ability to manage, track, and participate in his or her own care. PHRs are distinct from an electronic medical record ("EMR"), which must be maintained and largely controlled by a healthcare provider. Depending on the amount and type of CHI collected, a mobile health app or IoT device can take on characteristics of a PHR.

Whether a PHR is subject to HIPAA depends, once again, on whether it is used on behalf of a covered entity or the consumer. For example, a health plan may offer a PHR for its plan members to assist in the management of their health. Such a PHR must abide by the Security Rule safeguards and the limitations on uses and disclosures of PHI imposed by the HIPAA privacy regulations (the "Privacy Rule"). On the other hand, a PHR offered directly to consumers where a plan member can input a copy of his PHI obtained from a healthcare provider or health plan would operate outside HIPAA regulations. Instead of being governed by the HIPAA Privacy Rule, the privacy obligations of such a direct-to-consumer PHR would be primarily defined by the PHR's posted privacy policy and FTC privacy principles.

OCR has issued guidance on "Personal Health Records and the HIPAA Privacy Rule,"[19] which states that consumer-directed PHRs that are not offered by HIPAA-covered entities are not subject to HIPAA. The maintenance of medical records in a PHR by a consumer does not create a business associate relationship, even though the records may have been produced by a physician or other covered entity. Rather, to be covered by HIPAA, a PHR vendor must be acting on behalf of a HIPAA-covered entity.

---

18 *Id.*

19 U.S. Dep't of Health and Human Servs., Office for Civil Rights, Pers. Health Records & the HIPAA Privacy Rule, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf.

IV. HEALTH BREACH NOTIFICATION RULE

Recognizing the limits of HIPAA's statutory reach, the FTC issued a Health Breach Notification Rule in 2009, which mirrors HIPAA's Breach Notification Rule and is more prescriptive than state breach notification laws. Entities subject to this rule must notify their customers and others if there is a breach of unsecured, individually identifiable health information. This rule applies to a vendor of PHRs, a PHR-related entity, or to a third-party service provider for a vendor of PHRs or a PHR-related entity. A business is a vendor of personal health records if it "offers or maintains a personal health record."[20] A PHR is defined as an electronic record of "identifiable health information on an individual that can be drawn from multiple sources and is managed, shared, and controlled by or primarily for the individual."[21]

A wide range of mobile health apps, IoT devices, and other digital health services could potentially fall within the definitions of PHR, PHR-related vendor, and third-party service provider. A PHR-related entity is an entity that interacts with a PHR vendor by either offering products or services through the vendor's website or by accessing information in a PHR or sending information to a PHR.

Under the Health Breach Notification Rule, if a breach involves the information of more than 500 people, an entity must notify the FTC as soon as possible, but at least within ten business days after discovering the breach. If the breach involves information of fewer than 500 people, the entity can send the notice on an annual basis within 60 days of the end of the calendar year. If the breach involves more than 500 residents of a particular state, the entity must notify prominent media outlets serving the relevant locale.

V. Conclusion

OCR, FTC, state attorneys general, and other regulators are all trying to protect consumers by applying and adapting existing laws to the new world of digital health privacy. Agency-issued guidance and enforcement actions are excellent sources for navigating this new landscape. Because digital health companies often straddle multiple privacy and security regulatory regimes, it is important to understand which regulatory requirements apply, and to make informed choices when venturing into an area in which applicable law remains unclear.

---

20 16 C.F.R. § 318.2(j) (2009).

21 *Id.* at (d).