October 2021

Practice Group(s):

Policy and Regulatory

Health Care and FDA

Digital Health

US Regulatory Considerations Applicable to Digital Health Providers and Suppliers – Part I: HIPAA

Primary Regulatory Regimes Relevant to mHealth

By Michael H. Hinckle, Gina L. Bertolini, and Aiko Yamada

Digital health technologies are revolutionizing the global health environment by advancing healthcare services, Big Data analytics and medical device development and innovation, expanding the reach, accessibility and effectiveness of healthcare beyond traditional models.

The World Health Organization (WHO) has recognized that digital health solutions, through increased use and scale, can revolutionize how people worldwide achieve higher standards of health by providing greater access to services in a more convenient, efficient and cost-effective manner.[1] In particular, the Covid-19 pandemic highlighted the ability of digital health technologies to bridge the gap between patients and traditional healthcare settings, catalyzing a wide-scale adoption of innovative digital platforms and remote care models.

Smartphones, wearable devices, telemedicine platforms, artificial intelligence software, internet applications and other digital health technologies are transforming disease monitoring and diagnosis, access to consumer health information, clinical research and development and health benefits administration. Companies and institutions in the private and public sectors are investing in and integrating digital health technologies to enhance quality and reduce the costs of healthcare, maximize access to data and other information and enhance efficiencies.

While digital health technologies have been developed and used in the United States for many years, their use in the last year, largely in response to the pandemic, has exploded as both patients' and providers' embrace innovative alternatives to in-person care. In recognition of the exigencies created by the pandemic – in particular, the need for social distancing to reduce the risk of community spread and to preserve in-person health resources for the most acute patients – many restrictive Federal and State telehealth regulations have been temporarily lifted, creating new care models and pathways for reimbursement that previously did not exist. In addition, the US government's recognition of the need for health information interoperability and adoption of health information technology (IT) standards to maximize the access, use and exchange of electronic health information have created new opportunities for the development and deployment of enhanced digital health software, devices and other health IT tools.

This proliferation of digital health technologies and new opportunities for reimbursement have attracted non-US companies to enter the United States healthcare market, in some cases establishing digital health businesses in the United States. The development and use of digital health technologies raises complex and evolving regulatory challenges, which can be a hurdle for non-US clients seeking to enter or develop their presence in this market.

This series of articles provides an overview of the predominant regulatory considerations non-US companies should know as they develop or expand their digital health presence in the United States. Although not intended to be a comprehensive guide, these articles will highlight important considerations non-US-based companies should contemplate before entering the US healthcare market.

Part I will provide an overview of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), while **Part II** examines how HIPAA is applied to mHealth (mobile health) application developers, as well as other privacy considerations.

Part III will provide a high-level overview of the Federal Food, Drug and Cosmetic Act (FDCA) and its application to mHealth software developers, including issues unique to non-US companies, while **Part IV** will discuss other potential applicable laws, such as the Federal Trade Commission Act (FTCA) (including the FTCA's Breach Notification Rule), relevant telemedicine laws and Federal and State fraud and abuse laws.

HIPAA OVERVIEW

Digital health has a broad scope, and includes telehealth and telemedicine, remote patient monitoring (RPM), mobile health (mHealth),[2] personalized medicine, artificial intelligence (AI) and various forms of hardware and software health IT.[3] Many IT companies with no previous experience in the healthcare sector, such as mobile application developers, are entering the market for the first time through development of health IT applications. While this series of articles will focus primarily on the regulatory considerations related to mHealth, much of what is written is also applicable to other digital health solutions.

The development and use of mHealth applications require a consideration of multiple regulatory regimes. The first regime considered is HIPAA.

What is HIPAA?

HIPAA is a federal law that protects the privacy and security of patients' health information and requires certain entities to provide notification of health information breaches.

HIPAA is primarily comprised of the following Rules[4]:

- The Privacy Rule[5], which sets national standards for the protection of Protected Health Information (PHI), as that term is defined by the Rule
- The Security Rule[6], which sets national standards for protecting the confidentiality, integrity and availability of PHI that a Covered Entity (as defined by HIPAA's Privacy Rule) creates, receives, maintains or transmits in electronic form (ePHI)
- The Breach Notification Rule[7], which establishes obligations related to the breach of unsecured PHI, including required notifications to affected individuals, government investigators and the media
- The Enforcement Rule[8], which contains provisions relating to compliance, investigations and the imposition of civil money penalties (CMPs) for violations of HIPAA's Privacy, Security and Breach Notification Rules

The Office for Civil Rights (OCR) within the US Department of Health & Human Services (HHS) enforces HIPAA.

Who must comply with HIPAA?

HIPAA applies to Covered Entities[9], which are group health plans, healthcare providers, and healthcare clearinghouses.

- Group health plans, for purposes of HIPAA, are individual and group plans that provide or pay the cost of medical care, including without limitation, Medicare, Medicaid and employee welfare benefit plans or other arrangements that provide employee health benefits.
- Healthcare providers are providers of medical and other services, as further defined by HIPAA, regardless of size, that furnish, bill or are paid for healthcare and that electronically transmit health information in connection with such transactions.
- Healthcare clearinghouses are entities that process or facilitate the processing of health information received from another entity into a standard format, including without limitation, billing services and repricing companies.[10]

A Covered Entity's "Business Associates"[11], which are persons or entities that perform certain functions or activities for or on behalf of a Covered Entity that involve the use or disclosure of such Covered Entity's PHI, are subject to HIPAA.[12] A Business Associate's subcontractors that will access or use the Covered Entity's PHI to provide services to the Business Associate, such as cloud providers, also must comply with HIPAA.[13] Examples of Business Associate activities include claims processing, data storage and maintenance, data analysis, development of health IT such as electronic health records, utilization review and billing or revenue cycle management services.

HIPAA's Privacy Rule applies generally to Covered Entities, though certain provisions apply directly to Business Associates, as well. Most Covered Entities contract with a variety of Business Associates to carry out their healthcare activities and operations. The Privacy Rule allows Covered Entities to disclose PHI to these Business Associates, provided they enter into what are known as "Business Associate Agreements".[14] One purpose of the Business Associate Agreement is to provide assurances in writing that the Business Associate and its subcontractors will use the Covered Entity's PHI only for the purposes for which the Covered Entity engaged with the Business Associate, will safeguard the information from misuse, and will help the Covered Entity comply with certain duties under the Privacy Rule.

HIPAA's Security Rule and Breach Notification Rule also apply to Business Associates. Many digital health companies, including those who develop or deploy mHealth applications, are considered Business Associates. However, simply accessing PHI does not necessarily mean a digital health company is a Business Associate, since patients can authorize disclosure of their PHI to outside entities, such as third-party application developers. PHI disclosed to a third-party based on a patient's authorization often is no longer protected by HIPAA, depending on the third party and the purpose for such disclosure.[15] Digital health companies will need to engage experienced data privacy and security counsel to navigate these intricacies and to analyze other Federal laws that may be applicable to sensitive health information (such as certain substance use disorder records), as well as relevant state privacy laws.

What is PHI?

PHI means "individually identifiable health information" held by a Covered Entity or its Business Associate in any form or media that: 1) relates to a) the individual's past, present or future physical or mental health or condition, b) the provision of healthcare to the individual, or c) past, present or future payment for the provision of healthcare to the individual[16]; and 2) identifies the individual, or for which there is a reasonable basis to believe can be used to identify the individual. PHI includes 18 common identifiers (e.g., name, address, birth date, Social Security number).[17]

The following is not PHI: 1) "de-identified" health information (as that term is defined in HIPAA's Privacy Rule); 2) individually identifiable health information or other data disclosed by a consumer to a direct-to-consumer application, if the application is not developed or sponsored by a Covered Entity; and 3) individually identifiable health information or other data disclosed pursuant to a valid, HIPAA-compliant patient authorization to an entity not governed by HIPAA.[18] PHI disclosed in relation to research generally is not PHI, though a more detailed analysis is required on a case-by-case basis, and other protections would apply to such information.

De-identified health information neither identifies nor provides a reasonable basis to identify an individual.

There are two methods to de-identify information under the Privacy Rule: the "Expert Determination Method" and the "Safe Harbour Method".[19]

The Expert Determination Method requires a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable to determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, to identify an individual who is a subject of the information.[20]

The Safe Harbour method requires the removal of 18 individual identifiers of the individual (or of relatives, employers or household members of the individual), including names, all geographic subdivisions smaller than a State (except for, in some specific cases, the initial three digits of the zip code), all elements of dates, telephone numbers, account numbers, Social Security numbers, biometric identifiers, etc., where the Covered Entity does not have actual knowledge that the information could be used alone or in combination with other information used to identify the individual.[21]

Part II continues to examine HIPAA and how it is applied to mHealth application developers, as well as discusses other privacy issues and considerations.

Footnotes

1. https://www.who.int/health-topics/digital-health#tab=tab_1.

2. "mHealth" refers to a specific subset of telehealth that is powered by mobile and wireless technologies, such as mobile phones, tablets and wearable devices, that allow consumers to capture their own data to improve health outcomes, health research and to aid or assist in the provision of health care services.

3. https://www.fda.gov/medical-devices/digital-health.

4. 45 C.F.R., Subtitle A, Subchapter C, Parts 160 and 164.

5. 45 CFR, Subtitle A, Subchapter C, Part 164, Subpart E, Privacy of Individually Identifiable Health Information.

6. 45 CFR, Subtitle A, Subchapter C, Part 164, Subpart C, Security Standards for the Protection of Electronic Protected Health Information.

7. 45 C.F.R., Subtitle A, Subchapter C, Part 164, Subpart D, Notification in the Case of Breach of Unsecured Protected Health Information.

8. 45 C.F.R., Subtitle A, Subchapter C, Part 160, Subparts C, D, and E.

9. 45 C.F.R. § 160.103.

10. Id.

11. Id.

12. 45 C.F.R. § 164.104.

13. 45 C.F.R. § 164.308(b)(2).

14. 45 C.F.R. § 164.308(b)(1).

15. See generally 45 C.F.R. § 164.508.

16. 45 C.F.R. § 160.103.

17. 45 C.F.R. § 164.514.

18. 45 C.F.R. §§ 164.508, 164.514.

19. "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule"; see also 45 C.F.R. § 164.514(b).

20. 45 C.F.R. § 164.514(b)(1).

21. 45 C.F.R. § 164.514(b)(2).

* This article was first published by *In-House Community*.

Authors:

Michael H. Hinckle
Partner
Research Triangle Park
michael.hinckle@klgates.com
+1 919 466 1115

Gina L. Bertolini
Partner
Research Triangle Park
gina.bertolini@klgates.com
+1 919 466 1108

Aiko Yamada
Counsel
Tokyo
Aiko.Yamada@klgates.com
+81 3 6205 3630