US REGULATORY CONSIDERATIONS APPLICABLE TO DIGITAL HEALTH PROVIDERS AND SUPPLIERS – PART II: HIPAA (CONTINUED) & ADDITIONAL IMPORTANT PRIVACY CONSIDERATIONS

PRIMARY REGULATORY REGIMES RELEVANT TO MHEALTH

Date: 18 October 2021

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

In Part I, we provided a high-level overview of Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its provisions. In Part II, we discuss how HIPAA is applied to mobile health (mHealth) application developers, as well as examine additional privacy issues and considerations that non-US companies should keep in mind.

HIPAA (CONTINUED): APPLICATION OF HIPAA TO MHEALTH APPLICATION DEVELOPERS

General

If a Covered Entity is the developer of a mobile application ("app") and the app uses Protected Health Information (PHI), HIPAA will apply and will govern the creation, receipt, maintenance and transmission of PHI by the app (unless the PHI was acquired pursuant to a HIPAA-compliant patient authorization specifically releasing the data to the app developer).

If the app developer is not a Covered Entity, a key consideration is if the developer is acting as a Business Associate of a Covered Entity or is a subcontractor of a Business Associate. In other words, does the app developer create, receive, maintain or transmit PHI on behalf of a Covered Entity or Business Associate?

Key Questions

- Does the mHealth app create, receive, maintain or transmit PHI?
- What types of entities or individuals are the ultimate users of the app?
- Who are the app developer's clients? How is the app funded?
    - Are the app developer's clients Covered Entities, such as hospitals, physician practices, clinics, urgent care facilities, pharmacies, clinical or diagnostic laboratories or other health care providers?
    - Are the app developer's clients' health plans, health insurance carriers or health or wellness programs related to an employer-sponsored health plan?
    - Was the app developer hired by, or paid for services or products by, a Covered Entity, or by another entity that has contracted with a Covered Entity?

- Does an entity with whom the app developer is contracting direct the developer to create, receive, maintain or disclose PHI?

Direct-to-Consumer (DTC) Applications

If the app developer is offering services directly to consumers and collecting health information from consumers or on their behalf, i.e., DTC, and not on behalf of a Covered Entity or other healthcare provider, the app is likely not subject to HIPAA.

Key Questions

- Is the app independently selected by a consumer?
- Does the consumer control all decisions about whether to transmit his or her health information to a third-party, such as to a healthcare provider or health plan?
- Does the developer have any relationship with a healthcare provider, health plan or other Covered Entity (other than an interoperability relationship)?

WHAT IF HIPAA DOES APPLY TO THE MHEALTH APPLICATION?

If the mHealth app is developed by or for a Covered Entity, the mHealth app developer may be required to comply with HIPAA's Privacy, Security and Breach Notification Rules.

Privacy Rule

A Covered Entity is permitted, but not required, to use and disclose PHI without patient authorization for treatment, payment and healthcare operations, as those terms are defined by the Privacy Rule, and for other purposes required by law or otherwise permitted or required by the Privacy Rule.[1]

For all other disclosures, the Covered Entity must obtain the patient's (or the patient's legal representative's) written authorization. For most cases of access, use and disclosure of PHI, the Covered Entity must make reasonable efforts to access, use or disclose only the minimum amount needed to accomplish the intended purpose of such access, use or disclosure.[2] Covered Entities must provide a Notice of Privacy Practices (as defined by HIPAA) to patients, which outlines how patient data is used and must comply with certain regulatory requirements.[3] Covered Entities also must assure that required policies are in place at an organizational level, and must assure that its Business Associates also comply with Privacy Rule requirements in the access, use and disclosure of PHI.

Business Associate Agreement (BAA)

With some exceptions, where a third-party is providing services to a Covered Entity and the provision of services requires accessing or using the Covered Entity's PHI, HIPAA requires that the parties execute a BAA.[4] The BAA must include certain elements, as outlined in HIPAA's Security Rule. For example, the BAA must: describe the Business Associate's permitted and required uses of PHI; provide that the Business Associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law; and require the Business Associate to use appropriate safeguards to prevent an impermissible use or disclosure of PHI.[5]

In addition, Covered Entities often require that Business Associates indemnify the Covered Entity and maintain certain levels of insurance with the Covered Entity as a named insured, including cyber liability insurance. A

Business Associate is directly liable under HIPAA for its actions or inactions related to the Covered Entity's PHI, as well as contractually to the Covered Entity.[6]

If an mHealth application developer is a Business Associate of a Covered Entity, it must enter into a BAA with the Covered Entity, and it must enter into agreements with all subcontractors that will access the PHI to ensure the subcontractors' compliance with the BAA specifically and with HIPAA in general. Subcontractor agreements must be at least as restrictive as the primary BAA, and generally should contain strong indemnification and cyber liability insurance provisions.

Security Rule

HIPAA's Security Rule requires Business Associates to implement certain security standards, including initial and as-needed risk assessments, implementation of workforce and other policies, and processes and policies that protect the integrity and confidentiality of ePHI.[7] Business Associates also must maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting ePHI, including identifying and protecting against reasonably anticipated threats to the security or integrity of ePHI and against reasonably anticipated, impermissible uses or disclosures of ePHI.[8]

Breach Notification Rule

Business Associates are responsible for breaches of PHI and must notify the applicable Covered Entity if a breach occurs at or by the Business Associate. A “breach”, pursuant to HIPAA, is an impermissible use or disclosure of PHI that compromises the security or privacy of the PHI. Whether a particular set of circumstances is a breach is always a case-by-case analysis and will involve a risk analysis that includes several factors outlined in the regulation, including: the nature and extent of the PHI involved, the unauthorized person to whom the disclosure was made, if the PHI was accessed or viewed and the extent to which any risk has been mitigated.

Following a breach of unsecured PHI, Covered Entities must provide notification of the breach to affected individuals, to the OCR and, in certain circumstances, State attorneys general and the media. Where the Business Associate is responsible for the breach, the Covered Entity may prefer to manage all breach notification requirements directly, but it likely would seek indemnification from the Business Associate for all costs and expenses. Alternatively, the Covered Entity may require the Business Associate to manage all notifications and to incur all costs and expenses. When a breach is reported to OCR or to State attorneys general, both the Covered Entity and the Business Associate may be subject to investigation at the State or Federal level.[9]

ADDITIONAL PRIVACY CONSIDERATIONS

In addition to HIPAA, many States have enacted health information privacy and security laws, some of which are more restrictive than HIPAA or add additional requirements. Additionally, these State laws may be applicable to the consumer data used in an mHealth application, even where HIPAA is not. Accordingly, any mHealth application developer will require a State-by-State analysis of applicable State laws for any State in which a consumer may reside.

In addition to US State laws, the European Union's general data protection regulation (GDPR) and similar data protection laws in foreign jurisdictions may be applicable to consumer data. An analysis on whether and how foreign data protection laws apply may be required where an mHealth application developer or its business, including consumers or patients, has any nexus to foreign jurisdictions.

What if the mHealth application developer violates HIPAA?

For violations of HIPAA, OCR may impose CMPs from US$100 to not more than US$50,000 per violation, not to exceed US$1.5 million for identical violations in a calendar year.[10] Factors determining the amount per violation include if the Covered Entity or Business Associate did not know and, by exercising reasonable diligence, would not have known that it violated HIPAA; if the violation was due to reasonable cause or willful neglect; and if the entity corrected the violation within 30 days of when it knew, or by exercising reasonable diligence, would have known that the violation occurred.[11]

Potential fines and settlements with OCR can be costly and OCR's website is replete with examples of recent enforcement actions and multimillion-dollar settlements involving breaches.[12] HIPAA does not grant a private right of action to individuals affected by a violation, but the Health Information Technology for Economic and Clinical Health Act (HITECH) gave State attorneys general the authority to bring civil actions on behalf of State residents impacted by a HIPAA violation.[13]

A person or entity, including an mHealth application developer, who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule also may face a criminal penalty of up to US$50,000 and up to one-year imprisonment. The criminal penalties increase to US$100,000 and up to five years imprisonment if the wrongful conduct involves false pretences, and to US$250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer or use identifiable health information for commercial advantage, personal gain or malicious harm.[14]

HIPAA and COVID-19

OCR has issued some guidance and announced some notifications of enforcement discretion in relation to HIPAA flexibilities that apply during the Covid-19 emergency. For example, on 2 April 2020, OCR announced notification of enforcement discretion to allow uses and disclosures of PHI by Business Associates for public health and health oversight activities during the pandemic.[15] The HIPAA Privacy Rule already permits Covered Entities to provide this data for such purposes. Under this announcement, Business Associates now are allowed to share PHI for public health and health oversight activities without risk of a HIPAA penalty.[16]

In our next article, we discuss relevant provisions of the Federal Food, Drug and Cosmetic Act (FDCA) and its application to mHealth application developers, including issues unique to non-US companies.

FOOTNOTES

1. 45 C.F.R. § 164.506.
2. 45 C.F.R. § 164.502(b).
3. 45 C.F.R. § 164.520.
4. 45 C.F.R. §§ 164.314, 164.504(e).
5. Id.
6. 45 C.F.R. § 164.104(b).
7. 45 CFR, Subtitle A, Subchapter C, Part 164, Subpart C, Security Standards for the Protection of Electronic

Protected Health Information.

[8.] Id.

[9.] 45 C.F.R. §§ 160.400-414.

[10.] 45 C.F.R. § 160.404(b).

[11.] 45 C.F.R. §§ 160.401, et seq.

[12.] See, e.g., Press Release, HHS, Health Insurer Pays $5.1 Million to Settle Data Breach Affecting Over 9.3 Million People (Jan. 15, 2021), https://www.hhs.gov/about/news/2021/01/15/health-insurer-pays-5-1-million-settle-data-breach.html.

[13.] HITECH was enacted as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 42 U.S.C. § 17934. HITECH applies to certain of HIPAA's privacy and security provisions and creates liability for business associates under HIPAA's Privacy and Security Rules. Prior to passage of HITECH, HIPAA did not grant a private right of action to individuals affected by a violation, but the HITECH Act gave State attorneys general the authority to bring civil actions on behalf of state residents impacted by a HIPAA violation.

[14.] 42 U.S.C. § 1320d-6.

[15.] https://www.hhs.gov/about/news/2020/04/02/ocr-announces-notification-of-enforcement-discretion.html.

[16.] https://www.hhs.gov/about/news/2020/04/02/ocr-announces-notification-of-enforcement-discretion.html.

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

KEY CONTACTS

GINA L. BERTOLINI
PARTNER

RESEARCH TRIANGLE PARK
+1.919.466.1108
GINA.BERTOLINI@KLGATES.COM

MICHAEL H. HINCKLE
PARTNER

RESEARCH TRIANGLE PARK
+1.919.466.1115
MICHAEL.HINCKLE@KLGATES.COM

AIKO YAMADA
COUNSEL

TOKYO
+81.3.6205.3630
AIKO.YAMADA@KLGATES.COM

