Overview

Federal Laws and Regulations Applicable to Mobile Health Apps

Janet V. Hallahan, Partner, Practus, LLP

Bloomberg Law

Federal Laws and Regulations Applicable to Mobile Health Apps

Editor's Note: This document provides an overview of federal laws and regulations that may apply to a mobile application that collects, stores, or shares health information from consumers. This document may be used as a companion to the FTC's Mobile Health Apps Interactive Tool, which enables mobile application developers to determine if Food and Drug Administration (FDA), Federal Trade Commission (FTC), or Department of Health and Human Services (HHS) oversight applies to a mobile health application. It may also be used in connection with the HHS's Resources for Mobile Health Apps Developers, which provides, among other guidance, various scenarios regarding the transmission of personal health information through mobile health apps.

Although this document focuses on the regulations promulgated by the three agencies noted above, practitioners should be aware that many other international, federal, and state laws may apply alternatively or in addition to those described herein depending on the type of data, the technology involved, the respective roles of the applicable parties, and the nature of the transmission. Different fact patterns may involve different governing laws and practitioners should assess carefully which laws may apply to their client's particular needs.

For more information on federal, state, and international laws that may apply to mobile applications, refer to the following Bloomberg Law Chart Builders: Health Privacy: Special Protections for Sensitive Health Information; U.S. State Overview: Privacy & Data Security; State Data Breach Notification Requirements; and International Data Protection. To find additional applicable Chart Builders, codified statutes and regulations, news and legal developments, and reference materials on state privacy laws generally, see Comparison Table - State Privacy & Data Security Law Resources.

Updated by Janet V. Hallahan, Partner at Practus, LLP. Janet is also an adjunct professor of law at Rutgers University School of Law, where she teaches Healthcare Data Privacy, Security and Technology.

Introduction

Mobile applications that collect, store, or share health information of consumers, as well as the entities that develop and use such mobile health apps, are subject to a variety of federal and state statutes and regulations, including laws and regulations enforced by, respectively, the Department of Health and Human Services (HHS), the Federal Trade Commission (FTC), and the Food and Drug Administration (FDA).

HIPAA & HITECH Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) governs the dissemination of protected health information (PHI) held by certain health care providers and other covered entities to their business associates, including through a mobile health application owned, used, or developed by a covered entity or its business associate.

In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act, codified at 42 U.S.C. §§ 300jj et. seq and 42 U.S.C. §§ 17901 et. seq, expanded HIPAA liability to apply directly to business associates acting on behalf of a covered entity or another business associate. Accordingly, if an organization is the business associate of a covered entity or a business associate's subcontractor, then the provisions of HIPAA will directly apply to such provider. Conversely, if an organization is not a covered entity or performing services as a business associate, then HIPAA's requirements and protections would not apply to the collection, use, or transmission of data through a mobile app provided by that organization.

HIPAA and the HITECH Act are implemented by the HIPAA Administrative Rules, 45 C.F.R. Parts 160, 162, and 164, promulgated by HHS, significant sections of which are further discussed below.

Practitioners should note that the HIPAA rules specifically exclude individually identifiable health information in other areas, such as in education records and certain other student records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. § 1232g, employment records held by a covered entity in its role as an employer, or

information regarding a person who has been dead for over 50 years. *See* definition of "protected health information" in 45 C.F.R. § 160.103.

HHS has provided in depth guidance on HIPAA and the HIPAA Administrative Rules, including the HIPPA Privacy Rule, HIPAA Security Rule, HIPAA Breach Notification Rule and the HIPAA Enforcement Rule at its website. *See* HHS's HIPAA for Professionals page.

HIPAA Privacy Rule

Under the HIPAA Privacy Rule, 45 C.F.R. §§ 164.500 - 534, a covered entity and its business associates (including those providing mobile health apps) must comply with various notices and non-disclosure requirements as well as certain rights that patients have over their PHI, such as the right to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their PHI, and to request corrections. Covered entities must provide patients with a Notice of Privacy Practices (NPP) (which is different from a privacy notice on a website) to address their privacy practices and the patients' rights. Both covered entities and business associates that are transmitting data through a mobile health app must comply with the disclosures in the NPPs or risk enforcement actions by HHS.

HIPAA Security Rule

In addition, the HIPAA Security Rule, 45 C.F.R. §§ 164.302 - 318, applies to covered entities or business associates that are transmitting data through mobile health apps. It requires them to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI), or again, risk enforcement actions from HHS.

Although there are no hard and fast requirements regarding the steps that a covered entity or business associate must take to comply with the Security Rule, the HITECH Act was amended in 2021 to provide that "recognized cybersecurity practices" be considered by HHS in determining any HIPAA fines. The amendment clarified that "recognized security practices" means "the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology (NIST) Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities." *See* 42 U.S.C. § 17941. Accordingly, organizations that are covered entities or business associates should refer to this amendment for guidance on what measures under HIPAA they should take to meet the requirements of the Security Rule.

HIPAA Breach Notification Rule

Under the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400 - 414, covered entities and business associates must provide notification following a breach of unsecured PHI, which may include notice to individuals, the media, and HHS. For example, covered entities must notify an individual upon discovery of a breach of unprotected PHI. *See* 45 C.F.R. § 164.404(a). If a breach affects 500 or more individuals, covered entities must also notify the Secretary of HHS without unreasonable delay and in no case later than 60 days following a breach. *See* 45 C.F.R. § 164.408(b). If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. *See* 45 C.F.R.§ 164.408(c). In addition, covered entities that experience a breach affecting more than 500 residents of a state or jurisdiction must provide notice to prominent media outlets serving the state or jurisdiction. *See* 45 C.F.R. § 164.406. Finally, Section 13402(e)(4) of the HITECH Act requires the Secretary to post a list of breaches of unsecured PHI affecting 500 or more individuals. *See* HHS's Cases Currently Under Investigation chart.

Practitioners should note that the HIPAA Breach Notification Rule applies only to covered entities and business associates, and that breaches by mobile app vendors of personal health records and their third-party service providers should follow the breach notification provisions implemented and enforced by the FTC, as further discussed below, as well as any applicable state breach notification laws.

For Practical Guidance on complying with the HIPAA Breach Notification Rule, *see* Health Form – HIPAA Incident Documentation Form for Suspected or Reported Breaches of Unsecured Protected Health Information (Annotated); Checklist - Checklist for Notifying Individuals When Their Protected Health Information Has Been Improperly Accessed, Used or Disclosed (Annotated); and Sample Letter - HIPAA Breach Notification Template (Annotated).

HIPAA Enforcement Rule

Finally, the HIPAA Enforcement Rule, 45 C.F.R. Part 160, Subparts C, D, and E, addresses compliance and investigations for violations of the HIPAA Administrative Simplification Rules, such as the imposition of civil money penalties for violations procedures for hearings. The HHS Office of Civil Rights is responsible for enforcing the civil monetary penalty provisions, while the U.S. Department of Justice enforces the criminal penalty provisions.

For more information and Practical Guidance on HIPAA enforcement, *see* In-Focus: HIPAA; Step-by-Step: Health Care Cybersecurity; and Checklist – Using Mobile Technology in the Practice of Medicine (Annotated).

FTC Health Breach Notification Rule

The HITECH Act also required the FTC to create a breach notification rule that applies to entities that are not subject to HIPAA but which collect, use or transmit certain identifiable health information of consumers. *See* 42 U.S.C. § 17937. Practitioners should remember that this rule does not apply to covered entities or business associates that are subject to HIPAA, and any breaches through these entities should be addressed through the HIPAA Breach Notification Rule as discussed above.

Under the FTC Health Breach Notification Rule, 16 C.F.R. Part 318, personal health record (PHR) vendors, PHR-related entities, and third-party service providers that have access to PHRs must issue data breach notifications to affected individuals when there has been an unauthorized acquisition of unsecured PHR-identifiable health information contained in a PHR unless they are otherwise subject to HIPAA, generally as business associates. *See* HHS's Resources for Mobile Health Apps Developers for different scenarios when HIPPA may or may not apply to a healthcare app. Section 318.5(c) of the Health Breach Notification Rule requires notice to the FTC, the timing of which depends on whether 500 or more individuals were affected by the breach. A link to the FTC's most current standard form for parties to use to notify the FTC of a breach is available on the FTC's Health Breach Notification Rule page. In addition, Section 318.5(b) requires notice to media in states or jurisdictions where it is reasonably believed that 500 or more residents have been affected by the breach.

In September 2021, the FTC released a policy statement reaffirming that the Health Breach Notification Rule applies to mobile applications that "are capable of drawing information from multiple sources, such as through a combination of consumer inputs and application programming interfaces," regardless of whether "the health information comes from only one source."

For Practical Guidance on the FTC Health Breach Notification Rule, *see* Sample Notice - FTC Health Breach Notification to Individuals (Annotated) and Overview - Complying with FTC's Health Breach Notification Rule.

Section 5 of the FTC Act

Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1)-(2), applies to entities whether or not they are subject to HIPAA. Section 5 authorizes the FTC to prevent "unfair or deceptive acts or practices in or affecting commerce." With regard to mobile health applications, this means that an application owner or developer i) cannot make claims that would likely mislead or deceive reasonable consumers about things that are "material," or important to a consumer's decision; and ii) cannot engage in acts or practices that cause, or are likely to cause, a substantial injury that consumers cannot reasonably avoid and that is not outweighed by countervailing benefits to either consumers or competition.

Mobile health apps, including those that are subject to HIPAA, are required in some jurisdictions to feature a privacy policy and to disclose to the consumer where the data is transmitted or shared. In the event that the mobile health app is used in a way that does not comply with the provisions of the privacy notice, the company may be subject to enforcement actions under Section 5.

For more information on Section 5 of the FTC Act, *see* FTC's guidance titled Mobile Health App Developers: FTC Best Practices and additional FTC guidance on making various Health Claims. For more information on jurisdictions that require website privacy notices, *see* National Conference of State Legislatures' list of state laws requiring privacy policies and practices. *See also* California Online Privacy Protection Act of 2003 (CalOPPA), which was one of the first laws in the nation to require websites operators, including mobile apps, to conspicuously post a privacy policy if they collect personally identifiable information from Californians. Other laws require privacy policies as well, including the Children's Online Privacy Protection Act (COPPA), discussed further below.

Federal Food, Drug & Cosmetic Act

The Federal Food, Drug & Cosmetic Act (FDCA) established the FDA and its authority to provide oversight of medical devices. Whether the FDA has oversight of a mobile application depends on whether the mobile application can be considered a medical "device" under FDA regulations. Even then, the extent to which a medical device requires FDA oversight relates to its risk category, ranked from Class I (least risk) to Class III (most risk). FDA oversight of a mobile application may therefore arise from the purpose for which the mobile application is to be used and its associated risk, as opposed to merely the fact that the application collects, stores, or uses health information.

Section 3060(a) of the 21st Century Cures Act amended section 520 of the FDCA by excluding certain software functions from the definition of a device. *See* 21 U.S.C. §360j(o). In accordance, the FDA released a non-binding guidance document titled Policy for Device Software Functions and Mobile Medical Applications.

The FDA and the FTC generally encourage developers to contact the FDA to determine what, if any, regulatory requirements may apply to a mobile application. A developer may seek a Request for Designation (RFD) from the FDA if the applicability of the FDCA to a mobile application is unclear. The FDA also provides guidance on How to Determine If Your Product is a Medical Device as part of its Device Advice: Comprehensive Regulatory Assistance.

Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA) imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. Therefore, if a mobile app provider knows that it collects information from users younger than 13 years of age, COPPA will apply.

The FTC has published guidance on compliance with COPPA and enforces the law through its Children's Online Privacy Protection Rule, which requires, among other things, online notice of a website or online service operator's privacy policies. *See* 16 C.F.R. § 312.4(d).

For more information on COPPA, *see* Bloomberg Law's Fast Answers to common COPPA questions of interest to practitioners.

Other Laws

Practitioners should be aware that there are many other laws that may apply to the collection, use and transmission of data through a mobile health app. These laws include:

FCC Rules

The Federal Communications Commission (FCC) rules relate to interstate and international communications by radio, television, wire, satellite, and cable. The FCC is the federal agency responsible for implementing and enforcing its communications law and regulations. *See* 47 C.F.R. Chapter 1.

Healthcare Fraud and Abuse Laws

General healthcare fraud and abuse laws include the False Claims Act (FCA), the Anti-Kickback Statute (AKS), the Physician Self-Referral Law (Stark Law), and the Civil Monetary Penalties Law (CMPL). These laws may impact the use of mobile health apps, and healthcare organizations should be cautious in providing access to mobile health apps or platforms to healthcare practitioners because violations of these laws could result in criminal penalties, civil fines, exclusion from federal health care programs. *See* HHS guidance on fraud and abuse laws.

Marketing Laws

General marketing laws include the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act and Telephone Consumer Protection Act (TCPA), including the FCC's TCPA Healthcare Rule. These laws may also apply to mobile health care devices, including with respect to healthcare marketing, and practitioners should carefully review these laws to ensure their clients are in compliance.

Federal Privacy Laws

Other federal privacy laws may also apply to specific types of data with additional privacy and cybersecurity requirements. *See, e.g.*, Substance Abuse and Mental Health Services Administration (SAMHSA), the federal agency that has promulgated regulations relating to the disclosures of data relating to certain substance abuse and mental health services, which are often referred to as "Part II." For more information on disclosures and privacy under Part II, *see* 42 C.F.R. Part 2 and SAMHSA fact sheets located at the agency's Substance Abuse Confidentiality Regulations page.

State Privacy Laws

State privacy laws may also apply to mobile health apps. For example, although in most cases HIPAA will preempt any conflicting state law, it may not if the state law is more stringent than HIPAA. *See* 45 C.F.R. § 160.203. In addition, mobile health apps that are not covered by HIPAA may also be directly subject to the protections of state privacy laws.

Currently, five states—California, Connecticut, Colorado, Utah, and Virginia—have enacted broad consumer data privacy laws that may apply to mobile health apps. For Practical Guidance on the various requirements of these laws, *see* Table - State Privacy Laws: Contracting Requirements; Table - State Privacy Laws: De-Identified Data; Table - CCPA: Contracting Requirements; and Practical Guidance: California Privacy (CCPA/CPRA).

Other states, like Illinois, have passed narrow privacy laws governing the disclosure of healthcare data in areas such as genetics and biometrics, which also may apply to mobile health apps. *See, e.g.,* Illinois Biometric Information Privacy Act (BIPA). For additional information on biometric privacy laws and regulations, *see* In Focus: Biometrics.

Other state laws may impose additional requirements on mobile health apps, such as California's Confidentiality of Medical Information Act (CMIA), which applies to any business that offers software or hardware that is designed to allow individuals to maintain their own medical information, and CalOPPA, California's law regarding privacy policies, discussed above.

For more information and a list of broad and narrow state privacy laws, *see* National Conference of State Legislatures' list of state laws related to digital privacy.