Hashed & Salted | A Privacy and Data Security Update
July 2022

Every Business Is a Health Care Business—Health Data Beyond HIPAA

Health data is front and center as a recent cascade of data leaks concerning potential improper collection, use, and disclosure of this data is hitting the news. The use and disclosure of this sensitive data by hospitals, advertisers and health apps have reinvigorated lawmakers' attempts to regulate the complex collection, use and sharing of health data. The recent decision by the Supreme Court to overturn *Roe v. Wade* in *Dobbs v. Jackson Women's Health Organization* has also increased some lawmakers' focus on the extent to which proposed privacy laws will protect sensitive health information. Many lawmakers are concerned particularly with tracking technologies such as device identifiers, pixels and IP addresses that, when coupled with health data, can reveal sensitive consumer data such as location, treatment, illness and behavior.

Historically, health data has been regulated under the Health Insurance Portability and Accountability Act (HIPAA), which treats this data as protected information subject to HIPAA privacy and security regulations when it is collected, used and shared by covered entities and business associates. HIPAA provides limited protection of health data when the data is collected outside the traditional health care setting, however. In addition, the recent proliferation of personal and connected devices has expanded the collection of health data beyond these settings. The expansion of personal devices has increased access, use and disclosure of health data at the direction of consumers and not the covered entities and business associates that typically provide and assist in health care treatment. This point is of particular importance as HIPAA does not regulate vendors and service providers that are not collecting, using or disclosing health data at the direction of a covered entity or business associate. For example, an IP address that is not collected and shared by a covered entity with its business associate or HIPAA covered entity would not be subject to HIPAA even if the data is coupled with a consumer's health data such as search or web browsing history.

Consistent with lawmakers' concern about HIPAA protections, on June 21, 2022, the My Body, My Data Act of 2022 was introduced in response to the recent Dobbs decision. The act would prohibit companies from collecting, retaining, using or disclosing personal reproductive or sexual health information except with the express consent of the individual or as necessary to provide the product or service requested by the individual. In early July 2022, the Committee on Oversight and Reform issued a request for information on data processing from health apps and data brokers. The committee issued letters to five data broker companies and five personal health application companies, requesting information and documents regarding the collection and sale of personal reproductive health data. Beyond the sale of this information, there has been a recent focus on the circumstances under which this information may be shared with law enforcement.

Attorney Advertising

With all the focus on health data, now is a good time to audit your practices and understand your legal (and ethical) obligations. Below we discuss how HIPAA, the Federal Trade Commission's (FTC) Health Breach Notification Rule, and state privacy laws apply to health data and the implications of these laws on the collection and disclosure of tracking information, including IP address, location and device ID on personal consumer devices.

HIPAA

Our current U.S. privacy regime protects health data at the federal level through HIPAA, which specifically applies to covered entities (health care providers, health plans and health care clearinghouses) and their business associates (service providers) that provide products and services to these covered entities. Specifically, HIPAA applies to a subset of health data called protected health information (PHI), which consists of health data created, received, maintained or transmitted by a covered entity or business associate to provide health care services. Moreover, PHI is defined as individually identifiable health information transmitted in any medium that relates to (i) the past, present or future physical or mental health or condition (including genetic information) of an individual, (ii) the provision of health care to an individual, or (iii) the past, present or future payment for the provision of health care to an individual; is created or received by a health care provider, health plan, employer, public health authority, life insurer, school or university, or health care clearinghouse; and identifies or could reasonably be used to identify the individual. An IP address or device identifier that is associated with an individual's health data that is created, received, maintained or transmitted by a covered entity or its business associate is regulated under HIPAA as PHI.

Most important, but often overlooked, HIPAA does not apply to health data created, received, maintained or transmitted on mobile apps or connected devices at the direction of a consumer regardless of where the health data came from. The Department of Health and Human Services (HHS) through the Office of Civil Rights (OCR) is the enforcer of HIPAA and recently issued instructive guidance concerning this point; HHS personal device guidance specifically provides that the HIPAA rules do not protect the privacy and security of health data accessed or stored on personal devices. More specifically, search history, geographic location and information voluntarily shared on such devices is not protected by the HIPAA rules. Past HHS guidance provides that app developers trying to determine when HIPAA compliance is necessary should understand that, in most cases, they are not subject to HIPAA when they are creating, receiving, maintaining or transmitting PHI not on behalf of a covered entity or business associate but rather primarily at the direction and control of the consumer.

Lawmakers previously identified this gap in the HIPAA regulations, however, and provided the FTC with the authority to create the Health Breach Notification Rule to regulate health data maintained by businesses that predominantly provide products and services to consumers who control and direct access of their health data on their personal devices.

FTC Health Breach Rule

While HIPAA specifically applies to covered entities and business associates that create, receive, use and disclose PHI, the Health Breach Rule applies to vendors of personal health records (PHRs), PHR-related entities and third-party service providers of such entities that offer products or services that maintain PHR data. PHR data is defined as an electronic record of PHR identifiable health information that can be drawn from multiple sources and is managed, shared and controlled by or primarily for the individual. Finally, PHR identifiable health information is defined the same as PHI under HIPAA. This means a business and service providers of a business that collect health data provided by the consumer via inputs and also collect IP addresses and device identifiers, or have the capability to do so, and are not covered by HIPAA would be subject to the Health Breach Rule.

More important, the Health Breach Rule applies when health data is managed, shared and controlled primarily by the consumer and requires regulated businesses to notify individuals, the FTC and sometimes the media if there is a breach of security of unsecured PHR data. A recent policy statement issued by the FTC provides that a "breach of security of unsecured PHR data" means the disclosure of PHR data without an individual's consent. In June 2021, the FTC entered into a settlement agreement with Flo Health Inc., a period and ovulation tracker app, and required Flo to provide notice to all affected users

and delete all health information obtained without user consent, including health data collected inconsistent with Flo's privacy policy. The FTC did not use the Health Breach Rule to bring its action against Flo, but instead opted to use its Section 5 authority prohibiting unfair and deceptive practices. While the FTC did not use its authority under the Health Breach Rule in the Flo case, it did put businesses on notice of compliance requirements in a press release issued Sept. 15, 2021, concerning health apps and connected devices.

Based on the Health Breach Rule's incorporation of HIPAA's PHI definition to PHR data, recent critics of the FTC's policy statement have argued that it was not Congress' intent to regulate health apps, websites and connected technologies that are not accessing health data from covered entities and business associates. Despite this interpretation, businesses must determine whether they are collecting this data from multiple sources as interpreted under the Health Breach Rule regardless of the source of this data. If they are, they must consider whether they have obtained consent from the consumer when disclosing PHR data to third parties and confirm that their third-party contracts have restrictions in place concerning use of this data. If businesses use tracking technologies to collect IP addresses and various device identifiers coupled with health data and then disclose this data inconsistent with their privacy notice and without consumers' consent, this may be considered a "breach of security" requiring notice to the consumers and the FTC. We are likely to see the implications of this FTC enforcement priority soon. And if not the FTC, state privacy laws could certainly implicate health data because of their definition of personal information, including sensitive personal information.

State Privacy Laws

The California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Utah Consumer Privacy Act and the Connecticut Data Privacy Act all provide an exemption for health data, particularly PHI that is collected by a covered entity or business associate and collected, used, maintained and disclosed pursuant to HIPAA. However, to the extent that a business is not a covered entity or business associate under these respective laws and is not collecting, using and receiving PHI pursuant to HIPAA, the respective state privacy laws will apply. For example, if a business is collecting health data that would otherwise be considered PHI under HIPAA but is not being maintained, used or transmitted for a covered entity or the business associates or subcontractor of such entity, the business will be subject to state privacy laws when collecting health data from consumers in one of these regulated states.

Looking at the CCPA as amended by the CPRA, for example, businesses that collect personal information, which includes health data of California residents, will be subject to some heightened requirements that do not exist under HIPAA or the Health Breach Rule. These requirements include (i) certain vendor contract provisions, (ii) conducting data impact assessments, (iii) providing consumers with opt-out rights in addition to consumer access, correction, deletion and limitation rights, and (iv) forthcoming consumer automated decisions rights.

For all businesses, we recommend the following best practices to better assess your business's risk profile under current laws and regulations concerning how these laws apply to health data.

Key Questions

1. Is any of the health data the business accesses or uses created, received, maintained or transmitted on behalf of a covered entity or business associate subject to HIPAA?
2. What forms of health data are collected, and how sensitive is the data collected?
3. Are tracking technologies such as device identifiers, pixels or IP addresses used to obtain the health data?
4. If so, are the tracking identifiers shared with third parties?
5. Are contracts in place with these third parties to restrict how they use the identifiers and/or health data that is shared with them?
6. Does the business operate in and/or target consumers in California, Virginia, Colorado, Utah or Connecticut?

7. Has the business identified how these states' privacy laws apply to its collection, use and disclosure of health data?
8. Does the business have in place with vendors contracts that are consistent with the requirements of these state privacy laws?
9. Does the business have a retention policy in place or a practice of de-identifying data once it is no longer needed in identifiable form?
10. Does the business have a policy and process for responding to warrants, subpoenas and other law enforcement requests?

Related Professionals

Jessica B. Lee . . . . . jblee@loeb.com
Eric Cook . . . . . ecook@loeb.com

7025 REV1 07-29-2022