akerman

Blog Post

FTC Warns Health App Vendors: Comply with the Health Breach Notification Rule or Pay the Penalty!

September 27, 2021

By Elizabeth F. Hodge and Christy S. Hawkins

Vendors of health applications (health apps) and connected devices that collect or use individuals' health information, along with their service providers, are now on notice that they must provide timely notice to consumers and the Federal Trade Commission (FTC) when there is a security breach compromising health information. In response to the proliferation of health apps and connected devices that gather large volumes of individually identifiable health information, the FTC recently issued a Policy Statement explaining the scope of its Health Breach Notification Rule (the Rule or HBNR), the types of incidents that may trigger notice obligations, and that it intends to bring actions to enforce the Rule consistent with the Policy Statement. Specifically, certain health apps may be subject to the Rule, and sharing covered information without an individual's authorization may trigger the Rule's breach notification requirements.

The Health Breach Notification Rule

The FTC issued the HBNR in 2009 and it was intended to address certain entities that collect or use personal health information but are not regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Rule applies to vendors of personal health records (PHRs), i.e., an

Related People

Christy S. Hawkins
Elizabeth F. Hodge

Related Work

Data Privacy and Security
Healthcare
Healthcare Licensure and Compliance

Related Offices

Dallas
West Palm Beach

Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

Visit this Akerman blog

electronic record of an individual's identifiable health information that can be drawn from multiple sources and is managed, shared, and controlled by or primarily for the individual. The HBNR requires that PHR-related entities notify U.S. consumers, the FTC, and in some cases, the media, if there has been a breach of unsecured identifiable health information. Violations of the Rule are treated as an unfair or deceptive act or practice, and entities subject to the Rule may face civil penalties of up to $43,792 per violation per day. The HBNR does not apply to HIPAA-covered entities or any other entity to the extent it engages in activities as a business associate of a HIPAA-covered entity, but its requirements are similar to those of the HIPAA Breach Notification Rule. To date, the FTC has not brought an enforcement action under the HBNR.

The Policy Statement

The Policy Statement states that the FTC considers health apps that are capable of drawing information from multiple sources to be PHRs subject to the HBNR. Examples of such apps include:

- an app that collects information directly from consumers and can draw information through an application programming interface (API) that enables syncing with a person's fitness tracker; and
- an app that draws information from multiple sources even if the health information comes only from one source, such as a blood sugar monitoring app that draws health information from the individual's inputted blood sugar levels and draws dates (non-health information) from the individual's calendar on his/her phone.

Also, the FTC says that a breach of security triggering the Rule's notice requirements includes not only a cyber event involving health information, but also when a health app discloses or shares sensitive health information without the individual's authorization.

The Policy Statement's indication that health apps may be PHRs is noteworthy because last year the Commission began the rulemaking process to update the HBNR by issuing a Request for Public Comment soliciting input about the Rule, including whether the Rule does and should apply to health-related apps. The Commission has reviewed comments but has not yet issued a notice of proposed rulemaking. Also, the U.S. Department of Health and Human Services is engaged in rulemaking to update the HIPAA Privacy Rule, including defining the term "personal health application" in connection with revisions to the right of access.

The dissenting FTC commissioners said that the Policy Statement impermissibly expands the scope of the HBNR beyond vendors of personal health records and conflicts with business guidance that the FTC previously published regarding compliance with the Rule, including who is a PHR-related entity. The dissenting commissioners also maintained that the Policy Statement interferes with the ongoing FTC and HHS rulemaking processes, especially since addressing privacy issues related to health apps requires a coordinated approach among federal agencies.

As a result of the Policy Statement, the vendor or its service providers could be subject to the HBNR, HIPAA, and various state data breach notification laws in the event of a cybersecurity breach involving health information. Indeed, health app vendors and their service providers may find that the HBNR, HIPAA, and state data breach notification laws may vary in application, and even overlap, depending on who is using the apps and for whose benefit.

Next Steps

To minimize exposure under the FTC's Policy Statement and other breach notification laws, health app and connected device vendors and their service providers should:

1. Ensure that they have in place policies and procedures to comply with notice and reporting requirements of the Rule and that they obtain proper authorization from individuals to use and share health information;
2. Implement recognized industry standard data security practices to minimize the risk of a security breach under any applicable breach notification law and require their service providers to do the same;
3. Consider data security and privacy by design practices that may function as a "safe harbor" under different rules, such as encryption, anonymization, or pseudonymization;
4. Assess whether they may also be subject to the HIPAA Breach Notification Rule and state breach notification requirements; and
5. Monitor developments with the HBNR rulemaking process, the pending HIPAA Privacy Rule rulemaking with respect to requirements for mobile health apps, and FTC enforcement activity with respect to the Policy Statement.
