HINSHAW

FTC Gives Notice to Health Apps: You're Subject to the Health Breach Notification Rule

Privacy, Cyber & AI Decoded Alert | 3 min read
Sep 28, 2021

On September 15, 2021, the Federal Trade Commission (FTC) issued a policy statement confirming that developers of health apps and other connected devices that collect or use consumers' health data must comply with 16 CFR Part 318, the Health Breach Notification Rule (Rule). The Rule requires notice to consumers and others when their health data is breached. The proliferation of health apps and connected devices prompted the FTC to put entities covered under the Rule on notice of their ongoing obligation to come clean about breaches.

To whom does it apply?

In addition to vendors of personal health records (PHR), PHR-related entities and third-party service providers of PHR vendors, the FTC policy statement confirms that the Rule also applies to developers of mobile health apps and other connected devices. Developers are considered healthcare providers under the Rule if they furnish healthcare services or supplies by offering a health app or other connected device. A mobile health app is covered by the Rule if it is capable of compiling information from multiple sources, even if health information is collected from only one source. However, the Rule does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity.

What types of information does it cover?

The Rule covers personal health records meaning an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual. PHR identifiable health information means "individually identifiable health information," and, with respect to an individual, information that (1) is provided by or on behalf of the individual; and (2) identifies the individual, or if there is a reasonable basis to believe that the information can be used to

identify the individual. The FTC provides as an example a blood monitoring app that collects blood sugar levels from consumers and uses calendar dates from the user's phone calendar.

What obligations does it impose?

The FTC made it clear that developers of health apps and other connected devices must comply with the requirements of the Rule. Upon a security breach, which includes a vendor's unauthorized disclosure of sensitive health information without a user's consent, written notice must be sent to affected individuals without unreasonable delay but no later than sixty (60) calendar days after the breach. However, if a law enforcement official determines that notice would impede a criminal investigation, notice may be delayed. In certain situations, media outlets must be notified if 500 or more individuals in a state or jurisdiction are believed to be affected by the breach. The FTC must be notified within ten (10) days of discovery of the breach if more than 500 individuals are affected, and within sixty (60) days if fewer than 500 are affected.

How is it enforced?

A violation of the Rule is treated as an unfair or deceptive act or practice in violation of the Federal Trade Commission Act. Companies that fail to comply with the rule could be subject to monetary penalties of up to $43,792 per violation per day. However, according to the FTC, the Rule has never been enforced to date.

Where does it stand?

The FTC has put health app and connected device developers on notice that they must comply with the Rule and that firms offering health services should take appropriate care to secure and protect consumer data. Further, the FTC will increase its efforts to enforce the Rule and hold companies accountable for failure to comply.

Related Capabilities

Data Privacy, AI & Cybersecurity