STINSON

News & Insights

Health App Vendors Be Warned: You Could Be Subject to FTC's Health Breach Notification Rule

Alert

10.05.2021

By Tricia Kaufman, Steve Cosentino, CIPP & Sheva Sanders

The surge in new health apps and connected devices, which only increased during the pandemic, continues to raise many legal and ethical questions. As a result, lawmakers have been scrambling to define the obligations applicable to these digital products and their developers. On the other side, many health app developers might be unaware of new and existing laws that accompany the development and marketing of certain health-based digital products. For instance, a health app could be an FDA-regulated medical device if it is promoted as diagnosing, mitigating, curing, treating or preventing a disease or condition, such as sleep apnea. So, too, app developers could be subject to HIPAA if they are, or their customer base includes, healthcare providers or health insurance companies and they receive HIPAA protected health information. In addition, health app developers that sell products directly to consumers might be subject to state privacy laws, such as the California Consumer Privacy Act (CCPA), new privacy laws in Virginia and Colorado, or international laws such as the European Union's General Data Protection Regulation (GDPR).

Adding to this complex regulatory scheme, last month the Federal Trade Commision (FTC) published a policy statement asserting that vendors of certain mobile health apps and connected devices, including those that track things such as fitness, sleep, mental health and diet, may be subject to the FTC's Health Breach Notification Rule. The policy statement also serves as "notice" that FTC intends to start bringing actions under the rule, which can result in fines of up to $43,792 per violation per day.

Who is Covered by the Health Breach Notification Rule?

The rule covers vendors of electronic personal health records (PHRs), related entities and their service providers, which the FTC interprets broadly as covering developers of mobile health apps and connected devices, such as wearables, that sell or maintain PHRs.

Health App Vendors Be Warned: You Could Be Subject to FTC's Health Breach Notification Rule

PHRs contain information relating to a consumer's physical or mental health, or the provision of health care, together with identifying information. Identifying information includes not only things like name, email address and phone number, but also information that reasonably can identify the individual, such as IP address, credit card number or health plan ID number.

To be covered by the rule, a PHR also must be capable of drawing information from multiple sources. For instance, a mobile health app that collects information directly entered by the consumer and has the capability of automatically uploading information through an API, i.e., an application-programming interface, would be a PHR. However, if information can only be manually entered into the app, it would not be a PHR. Examples of PHRs provided in the policy statement include:

- An app that allows consumers to input information directly and that has the capability of collecting information through an API that enables syncing with a fitness tracker
- An app that monitor blood sugar through a consumer's input of blood glucose levels that also collects information from the consumer's phone calendar

One important distinction is that the rule applies to apps that pull information from multiple sources even though only one of those sources provides personal health information, for example, an app that collects information that a consumer inputs where that app also gathers non-health information from a different source.

What Does the Health Breach Notification Rule Require?

The rule requires notification to individuals, the FTC and in some cases the media when there has been a breach of identifying health information contained in a PHR. Service providers only would need to notify the company for which they work.

What Constitutes a Breach of PHR Identifying Information that Requires Notification under the Rule?

Not all breaches of information will be a breach of PHR-identifiable information requiring notification. Whether a reportable breach occurred is a very fact-specific inquiry. For example, a breach of health information together with the phone numbers of the associated individuals likely could constitute a reportable breach. On the other hand, a breach of credit card information by itself would not require notification under the rule, though it may require reporting under other laws. However, if the information also identified an individual as using an app developed specifically for patients suffering with a certain disease or condition such as cancer or depression, the combination of credit card information and the fact that the individual has an account with that app vendor could constitute PHR identifiable health information requiring a breach notification.

Health App Vendors Be Warned: You Could Be Subject to FTC's Health Breach Notification Rule

The policy statement interprets "breach" to include not only incidents involving malfeasance, such as hacking, laptop theft, or unauthorized downloading of PHRs by an employee; the rule's notification requirement also might be triggered by providing access to sensitive health information without an individual's authorization. In fact, FTC Commissioners in support of the policy statement indicated that a breach might include the unauthorized sharing of covered information with advertisers.

Regarding the type of authorization that would be needed, the policy statement is silent. However, commentary to the final rule indicates that the FTC might expect more than an embedded disclosure in the vendor's privacy policy for many types of information sharing. According to the commentary, consumers should be given "meaningful choice" when consenting to certain types of information sharing, (e.g., disclosure in a manner that is likely to be noticed and understood). Whether the FTC will apply this standard to health app vendors in its future enforcement of the rule is yet to be seen.

What Next Steps Should Vendors of Health Apps and Their Service Providers Take?

It is unclear if, when and how FTC will begin enforcing the breach notification requirement against health app vendors. However, in light of the policy statement's warning about impending enforcement, health app developers might want to start taking steps to:

- Determine whether they fall within the scope of the rule as interpreted in the policy statement
- Establish policies and procedures addressing obligations under the rule, including what to do in case of a suspected breach
- Establish a Privacy by Design policy where privacy and security is embedded into products and services from the outset
- Develop a Cybersecurity Incident Response Plan that includes pre-established contacts with insurance carriers, forensics investigators and legal support
- Train staff on the SOPs and document the training
- Ensure that their contracts with service providers who have access to PHR identifiable health information contain a breach notification requirement
- Determine whether and how PHR identifiable health information is shared with third parties
- Review how individual authorizations allowing disclosure of health information are obtained and whether the method used provides "meaningful choice" to the consumer

In addition, although the rule preempts conflicting state law, it does not preempt state laws that impose additional requirements. For instance, some states might require breach notifications to include contact information for consumer reporting agencies or advice on credit monitoring. Vendors also will want to be aware of these laws if a breach occurs. Finally, vendors of health apps also should determine whether other

laws that might affect their products and decide how they want to address each of their obligations.

CONTACT

Stephen J. Cosentino, CIPP

RELATED CAPABILITIES

Cybersecurity & Data Privacy

Health Care & Life Sciences

Life Sciences