CLIENT ALERTS & INSIGHTS

Warning from FTC Regarding Scope of Health Breach Notification Rule

SEPTEMBER 29, 2021

Authors: Ryan T. Sulkin

As the collection and use of health data drastically expands, the agency issued a recent guidance to officially put health apps and connected medical devices "on notice."

On September 15, the Federal Trade Commission ("**FTC**") held a meeting and published a policy statement to put connected medical device and health application ("**app**") providers on notice that they are subject to the ongoing obligations of the Health Breach Notification Rule (the "**Rule**") and that the FTC intends to begin enforcing the Rule. The Rule was first published in 2009, but the FTC has never enforced it and there are few examples of businesses providing breach notices pursuant to it.

The Rule was implemented to require certain businesses that are not subject to the Health Insurance Portability and Accountability Act ("**HIPAA**") to nevertheless follow breach notification standards. The Rule does not expand or modify the types of entities that are subject to HIPAA or change any requirements for HIPAA compliance.

The FTC's policy statement serves two purposes. First, to provide notice to connected medical device and health app providers who collect or use electronic personal health records ("**PHR**"), that the FTC will start enforcing the Rule. Second, to clarify who is subject to the Rule.

Background

Specifically, the Rule applies to all entities that offer or maintain PHRs about U.S. citizens. Before the FTC's recent policy statement, it was an open question as to what entities were actually subject to the rule because the lack of enforcement left entities in the dark as to what the Rule's scope and who it applied to.

The Guidance

The FTC's policy statement clarified that the Rule broadly applies to any business collecting or maintaining PHRs regardless of how they are collecting that information, and that the FTC intends to broadly enforce the Rule.

Specifically, the kinds of technology that could fall within the Rule's scope include, but are not limited to: (1) synched fitness or health devices and their respective apps; (2) application programming interfaces ("**APIs**"); (3) consumer inputted information; or (4) other synched devices or apps.

For example, a blood sugar monitoring app that collects and maintains PHRs from a user's manual entry of their blood sugar levels that also collects information from synched cell phone data or APIs

(such as calendar dates) is subject to the Rule. Another example the FTC cited of an entity that is subject to the Rule is any app synched to a fitness tracking device that also collects information from synched cell phone data or APIs.

The FTC's policy statement now makes clear that an entity ***cannot*** avoid the Rule's scope merely because they only collect or maintain PHRs that were created from user inputted data or from synched fitness or health devices.

Breach Notification Standards

It is important to remember that "breach" is not solely limited to actual cybersecurity incidents or malicious behavior. Under the Health Breach Notification Rule, any unauthorized access-including the sharing PHRs with a third party before getting the consumer's consent-triggers the Rule. Any unauthorized use is then presumed to be a breach unless the affected entity conducts a security risk assessment that shows there is a low likelihood the PHR is compromised.

However, not all PHRs are treated equally under the Rule. It is only triggered if the breach involved unsecured PHR, meaning the information was readable or usable.

When triggered, the Rule requires entities to provide some form of individual notice to affected consumers and media notice to a prominent media outlet within a state if the breach affected more than 500 consumers in that state.

Individual notices must include brief descriptions of (1) the breach (including time of breach and date of discovery, if known); (2) the types of health-related information that was involved; (3) steps a consumer can and should take to protect themselves from any resulting harm; (4) any investigative, mitigation, or remedial steps being taken; and (4) contact information that includes a toll-free telephone number, email, website, or address. Finally, entities must notify the Department of Health and Human Services ("**HHS**") through the HHS website.

Entities that fail to comply face $43,792 fines per violation, per day. The FTC offers interactive tools and best practices to help guide entities who collect or use health-related information.

As access and processing of health data exponentially increases, and the obligations your business is required to take on continue to grow, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients. We are available to assist you with any compliance efforts.

Ryan T. Sulkin at rsulkin@beneschlaw.com or 312.624.6398.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.