FTC Updates Health Breach Notification Rule: New Requirements for Health Apps and Online Services

August 6, 2024

By: Alfred Brunetti

What Happened?

On July 29, 2024, substantial updates to the Federal Trade Commission's Health Breach Notification Rule (HBN Rule) took effect, which squarely address the constantly evolving landscape of connected devices and creative technologies deployed in the health-related sector by non-HIPAA regulated entities. The updates generally (a) expand the HBN Rule's scope to expressly cover the developers and providers of more modern technologies like health-related apps and online services, and (b) add several requirements to the notification process triggered when a consumer's health data has been breached.

What Do We Need to Know?

The HBN Rule regulates the collection, storage, and sharing of sensitive health information and applies to vendors of Personal Health Records (PHR), i.e., websites, online services, or apps whose offering "relates more than tangentially to health," as well as PHR-related entities and third-party service providers. Personal Health Records are electronic records of personally identifiable health information with the "technical capacity" to pull information from one or more sources (e.g., connected devices, health-related apps, and online services). The HBN Rule expressly applies to the growing number of entities in the health-related space that are not regulated by HIPAA.

Adopted in 2009, the HBN Rule largely laid dormant until February 2023 when, for the first time, the FTC brought an enforcement action under it against *GoodRx*, a well-known digital health and pharmaceutical tracking platform, followed less than three months later by a second enforcement against *Premom*, an ovulation-tracking app. Both enforcement actions imposed civil penalties and centered upon the entities' less-than-forthright sharing of personal health information with other companies for advertising purposes via the use of tracking pixels and Software Development Kits (SDKs).

Found at 16 CFR Part 318, the HBN Rule now includes updates that:

1. Clarify that it applies to online services that provide health care services and supplies as well as to the developers of health apps and similar technologies.
2. Expand the definition of "PHR identifiable health information" to include health information resulting from the consumer's interaction with online services or apps that are facilitated by tracking technology, as well as health information "inferred from non-health related data points, such as location and recent purchases."
3. Specify that a PHR is an electronic record of identifiable health information that has the "technical capacity" to pull information from multiple sources, even if it actually pulls only from a single source.

4. Specify that a defined “PHR-related entity” includes products and services offered through any online service, website, or mobile app.

5. Expand the definitional scope of the term “breach of security” beyond the realm of a data security incident to expressly include an unauthorized acquisition of PHR health information resulting from an unauthorized disclosure, whether voluntary or not. By way of provided examples, the updates specify that breaches may include an entity's unauthorized selling or sharing of a consumer's information to third parties or an app's sharing of PHR health information for use in targeted advertising in a manner inconsistent with the entity's representations.

6. Provide new requirements for the breach of security notification process. These new requirements include timely identifying the actual third parties that acquired PHR identifiable health information, describing the types of unsecured PHR identifiable health information that was exposed in the event, detailing what is being done to protect those affected by the event, and clarifying that voluntary disclosures contrary to an entity's representations constitute a breach of security.

What Do We Need to Do?

With these new amendments and its purposeful track record of recent enforcements, the FTC has made clear that the Health Breach Notification Rule will no longer be allowed to gather dust. Rather, the FTC intends to keep pace with the development and deployment of emerging and novel technologies, especially where the privacy of sensitive data could be at stake.

So, if you are an entity that handles or interacts with health information to any degree and you are not regulated by HIPAA, the new HBN Rule may very well apply to you. Now is the time to assess and evaluate your existing privacy and data security policies, practices, and relevant business relationships to ensure that the FTC's freshly expanded toolkit of measures aimed at enforcing consumer rights in the sensitive and health data space does not ruin what's left of your summer.