akerman

Practice Update

FTC's Updated Health Breach Notification Rule Puts Health App Developers on Notice

June 12, 2024

By Jordan T. Cohen and Elizabeth F. Hodge

The Federal Trade Commission's (FTC) years-long effort to modernize its Health Breach Notification Rule (HBNR) in the midst of a swiftly changing technological landscape appears to be coming to an end. On Thursday, May 30, 2024, the FTC published its final rule implementing the HBNR. And so begins a new robust enforcement landscape for health and wellness app developers and vendors.

As we have discussed in a prior blog, the HBNR was first implemented in 2009 in response to the anticipated proliferation of online personal health record (PHR) services that offered to store a user's digital medical records. Many of these services are now defunct (e.g., Microsoft HealthVault). Since such services are not typically covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its breach reporting obligations, the HBNR was meant to fill this void.

Fast forward nearly 15 years and, as we previously noted, the FTC is demonstrating a renewed commitment to protecting consumers' digital health information, as illustrated by the enforcement actions against GoodRx, BetterHelp, and Easy Healthcare for impermissibly sharing consumer health information to assist with advertising and marketing practices. But the agency has struggled to

Related People

Jordan T. Cohen
Elizabeth F. Hodge

Related Work

Data Privacy and Security
Digital Health
Healthcare

Related Offices

Miami
New York
West Palm Beach

apply the HBNR to newer digital health platforms that are often used on smartphones and utilize technologies, including sophisticated user tracking, that did not exist in 2009.

In September 2021, the FTC issued a policy statement affirming that health apps and connected devices that collect or use consumers' health information must comply with the HBNR. However, many observers noted the agency's strained interpretation of the original rule. In what was widely considered (and discussed by us) as an effort to respond to the clunkiness of the original rule, the FTC issued a proposed rule in May 2023. Over a year later, the FTC is finalizing its attempt to modernize the rule and respond to such feedback. The Final Rule becomes effective July 29, 2024.

Below we describe the core updates and clarifications contained in the Final Rule, as well as some of the nuances that health and wellness app developers and vendors face with its implementation.

Clarification of Who Is Subject to the HBNR

The Final Rule expands the types of actors subject to the HBNR to include mobile health applications and similar technologies. The FTC does this by defining a "covered health care provider" (referred to as a "health care provider" in the Notice of Proposed Rulemaking) to include not only providers of medical services or other health services under the Medicare statute, but also "any other entity furnishing health care services or supplies." The Final Rule defines "health care services or supplies" to include any online services such as "a website, mobile application, or internet-connected device that provides mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet, or that provides other health-related services or tools."

The FTC explains in the preamble that the term "covered health care provider" is unique to the HBNR and does not bear on the meaning of "health care provider" as used in other regulations enforced by other government agencies.

While some commenters expressed concern that the broad definitions of "covered health care provider" and "health care services or supplies" would make sellers of products such as tennis shoes, shampoo, and vitamins subject to the HBNR, the FTC disagreed, explaining that the threshold inquiry is whether an entity is a "vendor of personal health records." Entities that are not in the business of offering or maintaining a health-related product or service are not vendors of PHRs, and, therefore, not subject to the rule. The FTC goes on to say that an app, website, or online service "must provide an offering that relates *more than tangentially* to health" to be considered a vendor of PHRs and subject to the HBNR. While the FTC includes a few examples of when an offering is more than tangentially related to health in the commentary, it does not provide a bright line test, thereby leaving businesses to guess where the Commission will draw the line. It is worth underscoring that the definition of vendor of personal health records specifically excludes HIPAA-regulated covered entities as well as entities to the extent they engage in activities as a HIPAA-regulated business associate.

Revised Definition of "Personal Health Record

The FTC revised the definition of a "personal health record" (PHR) to clarify what it means for a PHR to draw PHR identifiable health information from multiple sources. The 2009 HBNR said a PHR was an electronic record of PHR identifiable health information *that can be drawn from multiple sources.* Under the Final Rule, a PHR is an electronic record of PHR identifiable health information on an individual that *has the technical capacity to draw information from multiple sources* and that is managed, shared, and controlled by or primarily for the individual. This new definition means that an

app's status as a PHR depends solely on whether it has the technical means to draw information from multiple sources — regardless of whether a customer actually uses the technical means to sync the data with another app or tracker.

Revised Definition of "PHR Identifiable Health Information"

The Final Rule adopts the definition of "PHR identifiable health information" in the Proposed Rule with non-substantive changes. As such, the term means information that:

1.) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual; and

a. Identifies the individual; or

b. With respect to which there is a reasonable basis to believe that the information can be used to identify the individual; and

2.) Is created or received by a:

a. Covered health care provider;

b. Health plan;

c. Employer; or

d. Health care clearinghouse; and

3.) With respect to the individual, includes information that is provided by or on behalf of the individual.

The FTC rejected requests to further expand the definition, saying in the commentary that this definition is already quite broad. For example,

unique, persistent identifiers (such as unique device and mobile advertising identifiers), when combined with health information, constitute PHR identifiable health information if the identifiers can be used to identify or re-identify an individual. Also, PHR identifiable health information includes information about sexual health and substance use disorders because the information relates to the past, present, or future physical or mental health or condition of an individual. The FTC notes that if data has been de-identified according to standards set forth in the HIPAA Privacy Rule, then it is not PHR identifiable health information.

Revised Definition of "Breach of Security"

The Final Rule amends the definition of a "breach of security" to clarify that breaches include unauthorized disclosures of PHR identifiable health information in a PHR, in addition to a data breach involving exfiltration of consumers' data. An example of an unauthorized disclosure is a company's unauthorized sharing or selling of consumers' information to third parties that is inconsistent with the company's representations to consumers. This revision will allow the HBNR to more squarely apply to mobile app developers that intentionally share data in violation of the developer's privacy policies and other promises to its users.

The FTC decided not to define the term "authorization" as it is used in the definition of "breach of security," noting that requiring affirmative express consent is not appropriate in all cases. As a result, which types of disclosures are considered "authorized" requires a fact-specific analysis based on the interactions between the company and the consumer, the reasons why the disclosure was made, any representations the company made to the consumer, and other applicable laws. The FTC's recent enforcement actions (e.g., GoodRx and Easy Healthcare) illustrate the circumstances under which the Commission may find a disclosure to be unauthorized, thereby triggering the HBNR.

Revised Definition of "PHR Related Entity"

The FTC adopted its proposed clarification of the definition of a "PHR related entity" so that the term now includes entities that offer products or services not only through the website of a PHR vendor, but also through a PHR vendor's other online services, including mobile applications. This change recognizes the various ways in which consumers now access health information online, including through platforms that involve multiple vendors. The FTC also narrowed the scope of PHR related entities so that the term applies to an entity that accesses or sends *unsecured* PHR identifiable health information — rather than entities that access or send *any* information — to a PHR.

Revised the Methods for Providing Notice of a Breach

The Final Rule authorizes expanded use of email and other electronic means to provide effective notice of a breach to consumers. Specifically, vendors of PHRs or PHR related entities that discover a breach of security must provide written notice at the last known contact information of the individual. This written notice may be sent by electronic mail if an individual has specified electronic mail as the primary contact method, or by first-class mail. The FTC defines "electronic mail" as *email in combination with one or more of the following*: text message, within-application messaging, or electronic banner.

Further, any notice sent via electronic mail must be "clear and conspicuous," i.e., the notice is reasonable, understandable, and designed to call attention to the nature and significance of the information in the notice.

Expanded Content for Breach Notices

The Final Rule expands the information that must be provided in notices to individuals, including:

- a description of what the notifying entity is doing to protect affected individuals, such as offering credit monitoring or other services;
- the full name or identity of any third parties that acquired unsecured PHR identifiable health information or where providing a name or identity would pose a risk to individuals or the entity providing notice, a description, e.g., a hacker;
- a description of the types of unsecured PHR identifiable health information involved in the breach; and
- additional means for the affected individual to contact the notifying entity, including *two or more* of the following: a toll-free telephone number, email address, website, within-application mechanism, or postal address.

In response to public comment, the FTC declined to finalize its proposal that breach notices include a description of potential harm that might result from the breach. Commenters expressed concerns that providing such information might cause consumers needless anxiety or result in very generic descriptions of potential harms that offer no value to the consumer.

The Final Rule, as published in the Federal Register, contains exemplars for notification to individuals by text message, website banner, and email. Entities covered by the HBNR are not required to use the exemplars, but any notice must contain all elements set forth in the Final Rule.

Revised the Timing of Notice to the FTC

The Final Rule extends the time that covered companies have to notify the FTC of a breach of security involving 500 or more individuals from no later than 10 business days following discovery of the breach to *no later than 60 calendar days after discovery of the breach of security*. This new timeframe aligns with the timing of providing notice

to affected individuals and gives companies time to investigate incidents and better understand the facts.

Next Steps

Vendors of health and wellness apps and similar technologies should assess whether they may be vendors or PHRs, PHR related entities, or third party service providers under the HBNR. If they are, they should consider developing policies and procedures to implement the applicable breach notification requirements and train their workforce members on the policies before the July 29, 2024, effective date.

Additionally, although the FTC states in the commentary that the HBNR is only a breach notification rule and not a privacy rule, health app developers and vendors may want to consider implementing robust data privacy and data security practices such as:

- Imposing data retention limits
- Enabling data deletion options
- Reducing the amount of unsecured PHR identifiable health information they access and maintain (e.g., encrypt PHR identifiable health information at rest and in transit)
- Collecting and maintaining the minimum necessary PHR identifiable health information
- Implementing administrative, physical, and technical safeguards to protect the confidentiality, availability, and integrity of PHR identifiable health information
- Ensuring the company obtains appropriate consent or authorization from individuals for the use and disclosure of their PHR identifiable health information, including sharing data with tracking technology companies
- Appropriately de-identifying PHR identifiable health information where possible
- Reviewing cyber insurance policies to determine if such policies would cover a breach that

implicates the HBNR

Based on the FTC's recent settlements, guidance documents, and public statements, health and wellness app developers should prepare for robust enforcement of the HBNR. Akerman's healthcare attorneys continue to monitor the FTC's enforcement activities in this area and are available to assist health app developers in determining how the HBNR may apply to them and how to proceed moving forward.
