LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Parsing Through The FTC's Proposed Health Privacy Updates

By **Jami Vibbert, Nancy Perkins and Dani Elks** (August 2, 2023, 5:32 PM EDT)

Jami Vibbert

Nancy Perkins

Dani Elks

The Federal Trade Commission, which only recently commenced enforcing the Health Breach Notification Rule it adopted over a decade ago,[1] is now proposing significant regulatory amendments, including clarifying the rule's applicability to health apps and other similar technologies.

Upon **issuing** its notice of proposed rulemaking to make these amendments,[2] the FTC stated that "it is more vital than ever that mobile health app developers and others covered by the Health Breach Notification Rule provide consumers and the FTC with timely notice about what happened," and "[t]he proposed amendments to the rule will allow it to keep up with marketplace trends, and respond to developments and changes in technology."[3]

The HBNR requires notification to individuals, the FTC and in some cases the media of breaches of security affecting information in personal health records, or PHRs. Such notification is to be provided by vendors of PHRs and PHR-related entities, which in turn are to be notified of breaches experienced by their third-party service providers.

Although for many years the types of entities subject to the HBNR were understood to be quite limited, the FTC provided a new interpretation of the HBNR's scope in a policy statement issued in 2021.

In that statement, the FTC opined that "many appear to misunderstand [the HBNR's] requirements," and asserted that "the explosion in health apps and connected devices makes [the HBNR]'s requirements with respect to them more important than ever."[4]

The currently proposed amendments are intended to codify the FTC's interpretations expressed in the September 2021 policy statement regarding the HBNR's application to mobile apps and similar technologies. These interpretations are also clearly revealed in the two HBNR enforcement actions the FTC has taken to date — both in 2023 — both of which involved mobile app developers.[5]

The FTC is inviting comments on the proposed modifications until Aug. 8.

Background

The HBNR implements provisions of the Health Information Technology for Economic and Clinical Health Act, which requires, in relevant part, both the FTC and the U.S. Department of Health and Human Services to promulgate regulations requiring notification of security breaches involving individually identifiable health information.

The HHS regulations apply to entities subject to the privacy and security rules implementing the Health Insurance Portability and Accountability Act, and those entities are exempt from the HBNR.

And while the HIPAA breach notification rules apply to medical records held by or on behalf of health

care providers or health plans, the HBRN applies to records containing individually identifiable health information that is "managed, shared, and controlled by or for the individual to whom the information pertains."[6]

Under both the HHS and FTC rules, a notification obligation is triggered when a regulated entity discovers a breach of security affecting unsecured, i.e., unencrypted, individually identifiable health information.

Under the HBNR, a "[b]reach of security means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual."[7]

The FTC, through the NPRM, seeks to clarify the HBNR's scope by amendments to particular relevant terms, and also proposes changes to the procedural requirements for notification.

Proposed Amendments

Regulatory Scope

The significance of many of the proposed HBNR modifications lies in subtle changes to key terms used in the rule.

As noted, the HBNR applies to vendors of PHRs and PHR-related entities, and their respective third-party service providers. PHR vendors are entities that hold PHR identifiable health information that is, among other things, information created or received by a health care provider.

To highlight that certain developers of mobile apps and similar technologies are health care providers and thus PHR vendors under the HBNR, the FTC proposes to newly add definitions of "health care provider" and "health care services or supplies."

Any mobile app developer meeting the definition of a "health care provider" and providing health care services or supplies will, to the extent it collects or uses identifiable health information, be a PHR vendor.

As proposed in the NPRM, "health care services or supplies" would include

> any online service, 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.[8]

Mobile apps and other technologies providing these types of health care services or supplies would be deemed health care providers under the HBNR, and the individually identifiable health information collected through these technologies would constitute PHR identifiable information.[9] These definitional modifications would clarify that developers of these types of technologies are PHR vendors under the HBNR.

The FTC also proposes amendments to clarify that "PHR identifiable health information" encompasses:

- Traditional health information, e.g., diagnoses, medications;
- Health information derived from consumers' interactions with mobile apps and other online services, e.g., health information generated from tracking technologies used by websites or mobile app interactions; and

- Emergent health data, e.g., health information inferred from non-health-related data points, like location or recent purchases.[10]

In connection with these proposed modifications, the FTC raised, among others, the following questions:

- Do the proposed changes clarify for the market which entities are covered by the HBNR, and under what circumstances?

- Would the proposed changes and added definitions apply to entities that offer other technologies and, if so, is such application appropriate? If not, how could the scope be limited?

- Should any adjustments be made to the proposed definition of "health care services or supplies?"

PHR Functionality

Currently, a record of personal health information is a PHR only if it not only contains an individual's electronic personally identifiable health information and is primarily managed, shared and controlled by the individual, but also if that information can be drawn from multiple sources.[11]

The FTC proposes to revise this definition to refer to records that have the technical capacity to draw information from multiple sources.[12] This change would bring technologies that are capable of drawing information from multiple sources, regardless of whether they actually do that. Apparently recognizing that this could be deemed a questionable approach, the FTC is seeking public comment on the following questions:

- Should the proposed definition be adjusted to take into account consumer use, e.g., where no or de minimis customers use a feature?

- How likely it is that an app would have the technical capacity to draw information from multiple sources, but have that capacity entirely or mostly unused, either because it remains a beta feature, has not been publicized, or is not popular?

If the FTC moves forward with this proposed amendment, PHR developers will need to consider the consequences of making their PHRs capable of drawing information from multiple sources.[13]

Breaches

A major purpose of the NPRM is to underscore, as the FTC made clear in its recent HBNR enforcement actions, that the agency will treat an unauthorized disclosure of unsecured PHR identifiable health information, however it occurs, as a breach of security for HBNR purposes.

Under the current rule, it is a breach if there is an acquisition without authorization of unsecured PHR identifiable health information. To underscore that a breach of security under the HBNR is not limited to cybersecurity intrusions or nefarious behavior of an external actor, the FTC proposes to amend "breach of security" to include any unauthorized acquisition that occurs as a result of a data breach or an unauthorized disclosure.[14]

This subtle proposed change is intended to encompass in the "breach of security" definition disclosures that may be made voluntarily, i.e., not as the victim of theft or intrusion, but without obtaining the consent of the individual to whom the disclosed information pertains.

Notice Requirements

The NPRM also proposes several modifications to the HBNR's procedural requirements for notification of breaches.

First, the FTC proposes allowing vendors of PHR or PHR-related entities to provide notice via electronic mail, if specified by the consumer, rather than only by first-class mail.[15]

Electronic mail would be defined to include "email in combination with one or more of the following: text message, in-app messaging, or electronic banner."[16] Vendors would be required to (1) secure consumer consent before adopting electronic mail as the vendor's notification method and (2) enable consumers to opt out of electronic mail notifications.[17]

Second, the FTC proposes adding several elements to the required content of breach notifications, including "a brief description of the potential harm that may result from the breach (e.g., medical or other identity theft)."[18]

The requirement to include such a description could be difficult to fulfill without speculation, as the FTC appears to acknowledge in requesting comments on these questions, among others:

- Are notifying entities able to assess the potential harms to individuals following a breach, and if not, can notifying entities minimize the potential risks by informing individuals that they are unaware of any harms that may result from the breach?

- In the absence of known, actionable harm resulting from a breach, what would be the best way for notifying entities to describe to individuals the potential harms they may experience?

- Might additional and more specific data elements overwhelm or confuse recipients?

These questions suggest that the FTC is open to suggestions as to how to make breach notifications meaningful to consumers, in practical terms. Comments based on experience in preparing breach notification letters, which generally entails consideration of how to give individuals useful information about a security breach, would likely be welcomed by the FTC.

Changes Considered Subject to Public Comment

The NPRM also calls for comments on changes that the FTC considered but has not actually proposed. For example, the FTC considered defining "authorization" — relevant to whether a disclosure was unauthorized — to mean affirmative express consent of the individual, where affirmative express consent is consistent with state laws that define consent. The FTC is soliciting comments on, among other things, the following questions:

- What constitutes acceptable methods of authorization?

- Is it acceptable to obtain an individual's authorization to share PHR information through an individual's click in connection with a prechecked box?

    - Is it sufficient if an individual agrees to terms and conditions disclosing such sharing but that individual is not required to review the terms and conditions?

- Or is it sufficient if an individual uses a health app that discloses in its privacy policy that such sharing occurs, but the app knows via technical means that the individual never interacts with the privacy policy?

- Are there certain types of sharing for which authorization by consumers is implied, because such sharing is expected and/or necessary to provide a service to consumers?

And with respect to the timing of required notices, the FTC's questions for public comment are:

- Would earlier notification to consumers better protect them, or would that instead lead to partial notifications because the entity may not have had time to identify all relevant facts?

- Should the timeline for notices to the FTC be extended to give entities more time to investigate breaches and better understand the number of individuals affected, or would an extension instead facilitate dilatory action and minimize opportunity for important dialogue with the FTC?

Implications

While the FTC has already been using the HBNR in its recent enforcement actions consistent with its 2021 policy statement, the NPRM comment period gives interested parties an opportunity to provide the FTC with relevant insight on what should be included in the final amended HBNR.

Furthermore, the FTC seeking comment on changes not yet proposed provides relevant stakeholders the opportunity to educate the FTC in complex virtual health care technological platforms in advance of future enforcement actions and rulemaking.

Jami Vibbert is a partner and chair of the privacy, cybersecurity and data strategy group at Arnold & Porter.

Nancy Perkins is counsel at the firm.

Dani Elks is an associate at the firm.

[1] Health Breach Notification Rule, 74 Fed. Reg. 42,962 (2009), codified at 16 C.F.R. Part 318.

[2] 88 Fed. Reg. 37,819 (Jun. 9, 2023) available at https://www.federalregister.gov/documents/2023/06/09/2023-12148/health-breach-notification-rule.

[3] FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule, Federal Trade Commission (May 18, 2023), available at https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-amendments-strengthen-modernize-health-breach-notification-rule.

[4] Id.

[5] See Arnold & Porter, FTC Fines GoodRx $1.5 Million in First Enforcement Action Brought Under Health Breach Notification Rule (Feb. 15, 2023), available at https://www.arnoldporter.com/en/perspectives/blogs/enforcement-edge/2023/02/ftc-fines-goodrx; and Arnold & Porter, FTC Settles With Premom App Developer for Privacy and Security Violations

(Jun. 1, 2023), available at https://www.arnoldporter.com/en/perspectives/blogs/enforcement-edge/2023/06/ftc-settles-with-premom-app-developer.

[6] 16 C.F.R. § 318.2(d).

[7] Id. § 318.2(a).

[8] Id.

[9] Id.

[10] See 88 Fed. Reg. at 37,822-23 ("PHR identifiable information" encompasses identifiable health information provided by or on behalf of an individual and received by a health care provider, health plan, employer, or health care clearinghouse).

[11] 16 C.F.R. § 318.2(d).

[12] 88 Fed. Reg. at 37,826 (emphasis added).

[13] Indeed, the fact that the FTC chose not to allege breaches of the HBNR in its case against BetterHelp, Inc., because that app did not collect information from multiple sources is telling in the FTC's current limitation in the definition of PHR.

[14] 88 Fed. Reg. at 37,824 (emphasis added).

[15] Id. at 37,827.

[16] Id.

[17] Id.

[18] Id. at 37,828 (The Proposed Rule also seeks comment related to potential other content requirements, including (1) the full name, website, and contact information of any third parties that acquired unsecured PHR identifiable health information as a result of a breach of security; (2) a brief description of what the entity is doing to protect affected individuals (e.g., offering credit monitoring); and (3) the contact procedures specified by the notifying entity, including two or more of the following: toll-free telephone number, email address, website, in-app messaging, or postal address.).
