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

Scope Of FTC's Health Info Enforcement May Expand

By **Jodi Daniel and Brandon Ge** (June 30, 2023, 5:39 PM EDT)


Jodi Daniel


Brandon Ge

On May 18, the Federal Trade Commission announced a notice of proposed rulemaking to amend the Health Breach Notification Rule, or HBNR.[1] The proposed changes are primarily intended to clarify the scope of entities subject to the HBNR and what constitutes a breach that triggers the rule's notification requirements. Comments on the notice of proposed rulemaking, or NPRM, are due on Aug. 8.

The NPRM comes during a flurry of legislative, regulatory and enforcement activity intended to make entities that are not subject to the Health Insurance Portability and Accountability Act accountable for their practices related to the collection, use and sharing of health information.

These include many health apps and other direct-to-consumer technologies, such as fitness trackers and wearable monitors, which generally handle health information directly on behalf of consumers, not covered entities or business associates, and are therefore outside the scope of HIPAA.

Consumer use of such technologies has increased significantly in recent years, creating swaths of health information that largely remain unregulated. The NPRM, if finalized, would change this regulatory landscape.

Background

In the event of a breach of security of unsecured personal health records, or PHRs, the HBNR requires vendors of PHRs and PHR-related entities to notify consumers, the FTC, and, in breaches affecting 500 or more residents of a state or jurisdiction, prominent media outlets serving that state or jurisdiction.

If a service provider to one of these entities experiences a breach, it must notify the entity, which in turn must carry out its notification obligations.

Notice to individuals must be provided without unreasonable delay and no later than 60 calendar days after discovery of a breach. If a breach affects 500 or more individuals, notice must be provided to the FTC as soon as possible and no later than 10 business days after discovery of the breach.

The HBNR only requires notification for breaches of unsecured health information, which is defined as health information that is not secured through technologies or methodologies specified by the U.S.

Department of Health and Human Services. The HBNR also does not apply to covered entities and business associates subject to HIPAA.

The FTC issued a policy statement in September 2021 that swept in a large number of technology companies and activities, including health apps.[2]

The policy statement also clarified that a breach is not limited to cybersecurity intrusions or nefarious behavior, but also covers incidents of unauthorized access such as sharing of covered information without an individual's authorization.

In addition, the FTC recently started initiating enforcement actions under the HBNR.[3] The FTC also recently took enforcement action against BetterHelp Inc. under Section 5 of the FTC Act for allegedly sharing consumers' health information for advertising purposes.[4]

Key Proposals

The key changes proposed in the NPRM are summarized below.

Clarifications on the HBNR's Scope

To clarify the scope of the HBNR, the FTC proposes to revise the definition of "PHR identifiable health information" and add definitions of "health care provider" and "health care services and supplies" in an effort to clarify and broaden the scope of the rule.

"PHR identifiable health information" would be revised to mean information that:

- Is provided by or on behalf of the individual;
- Identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual;
- Relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; and
- Is created or received by a health care provider, health plan, employer or health care clearinghouse.

This change is not intended to be substantive, and the preamble clarifies that the FTC believes this definition covers traditional health information, e.g., diagnoses or medications; health information derived from consumers' interactions with apps and other online services, e.g., health information created from tracking technologies on websites or mobile apps; and emergent health data, e.g., health information inferred from non-health-related data points such as location and recent purchases.

"Health care provider" would be defined similarly as it is under HIPAA as a provider of services or provider of medical or health services, but would also include any other entity furnishing "health care services or supplies."

"Health care services and supplies" would be defined as any online service, such as a website, mobile

application or internet-connected device, which 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, or diet, or that provides other health-related services or tools.

The result of these changes is that developers of health apps and similar technologies that provide health care services and supplies would constitute health care providers under the HBNR, creating a much more expansive definition of health care provider than that in many other frameworks, including HIPAA.

As a result, any individually identifiable health information collected or used by these products and services would constitute PHR identifiable health information subject to the HBNR. Another result of these changes is that mobile health apps would generally constitute PHRs covered by the rule and developers of such apps would constitute vendors of PHRs.

The FTC also proposes to revise the definition of "PHR-related entity," which is currently defined as an entity, other than a HIPAA-covered entity or business associate, that: (1) offers products or services through the website of a vendor of PHRs; (2) offers products or services through the websites of HIPAA-covered entities that offer individuals PHRs; or (3) accesses information in a PHR or sends information to a PHR.

The FTC proposes to revise this definition as follows:

- The first prong would be revised to clarify that PHR-related entities include entities that offer products and services not only through the websites of vendors of PHRs but also through any online service, including mobile apps.

- The third prong would be revised so that it only covers an entity that accesses or sends unsecured PHR identifiable health information — not simply any information, as it is under current HBNR regulations — to a PHR. This change is intended to eliminate confusion and narrow the scope of the term "PHR-related entity."

The FTC also notes in the preamble that certain businesses may be considered both a PHR-related entity and a third-party service provider depending on the circumstances. For example, a firm that performs attribution and analytics services may be a PHR-related entity to the extent it accesses unsecured PHR identifiable health information in a PHR, but a third-party service provider in other arrangements.

This is not the FTC's intent, so it proposes to amend the HBNR such that a third-party service provider is not a PHR-related entity when it accesses unsecured PHR identifiable health information in the course of providing services.

Clarifications Regarding Breaches of Security

Building on the policy statement and its recent enforcement actions, the FTC proposes to expressly clarify in the HBNR that a breach of security encompasses unauthorized acquisitions that occur as a result of a data breach or an unauthorized disclosure.

This change is intended to clarify that breaches include voluntary disclosures by PHR vendors or PHR-related entities where such disclosure was not authorized by the consumer.

Clarifications Regarding Drawing PHR Identifiable Health Information from Multiple Sources

Currently, the HBNR defines a PHR as an electronic record of PHR identifiable health information that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual.

The FTC proposes to revise this definition such that it means 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 change is intended to clarify two points: (1) a product is a PHR if it can draw information from multiple sources, even if the consumer elects to limit information from only a single source; (2) a product is a PHR if it can draw any information from multiple sources, even if it only draws health information from one source.

Ultimately, it is the FTC's intent to further clarify the HBNR's applicability to developers and purveyors of products that are merely technically capable of drawing information from more than one source.

Changes to Requirements Regarding the Method and Content of Notices

The FTC proposes to permit notification of a breach by electronic mail if the individual has specified electronic mail as the primary contact method. The FTC proposes to define electronic mail to mean email in combination with one or more of text message, in-app messaging or electronic banner.

The FTC also proposes five changes to the HBNR's notice content requirements:

- Notices must include a brief description of the potential harm that may result from the breach, e.g., medical or other identity theft.

- Notices must include the full name, website and contact information of any third parties that acquired unsecured PHR identifiable health information as a result of the breach, if this information is known.

- The HBNR currently requires that notices describe the types of unsecured PHR identifiable health information that were involved in the breach. The FTC proposes to expand the sample list of types of PHR identifiable health information in the regulations.

- Notices must include a brief description of what the entity is doing to protect affected individuals, e.g., offering credit monitoring.

- Currently, the HBNR only requires one of a toll-free telephone number, email address or postal address. The FTC proposes to require that the contact procedures specified in the notice include two or more of the following: toll-free telephone number, email address, website, within-application message or postal address.

Takeaways

The FTC has been taking on a larger role in regulating the use of consumer health information and has been using the tools at its disposal — namely, the HBNR and FTC Act — to enforce against businesses that misuse or share health information without individuals' authorization.

The NPRM is just the latest in the FTC's efforts to regulate this space and ensure that businesses not regulated by HIPAA do not use and share health information in contravention of consumers' wishes and expectations.

Ultimately, the NPRM proposes to codify an expansion of scope and other clarifications, some of which were first articulated in the FTC's 2021 policy statement.

One of the more noteworthy clarifications made in that policy statement, which is echoed in the NPRM, is that reportable breaches under the HBNR include not only cybersecurity intrusions or nefarious behavior, but also voluntary disclosures by vendors of PHRs or PHR-related entities that are not authorized by the consumer.

This means that any disclosures of consumer health information generally must be made consistent with consumers' reasonable expectations and the regulated entity's public disclosures about its privacy practices.

The FTC has clarified that it expects any sharing of consumer health information beyond this to be limited unless consumers exercise meaningful choice in consenting to such sharing, and burying disclosures in verbose, lengthy privacy policies will not suffice to meet this meaningful choice standard.

Vendors of PHRs and PHR-related entities will need to closely examine their public disclosures, including their privacy policies, to assess whether their sharing of consumer health information might constitute breaches under the HBNR's rather expansive and unique interpretation of the term.

In addition, according to the preamble of the NPRM, the FTC considers certain onward disclosures to be breaches.

For example, if a third-party service provider, e.g., an analytics firm, receives PHR identifiable health information from a vendor of PHRs or PHR-related entity and then sells it without consumers' authorization, the FTC considers that to be a breach requiring notification by the third-party service provider to the relevant vendor of PHRs or PHR-related entity, which would then be responsible for notifying individuals, the FTC and potentially media outlets in accordance with the HBNR.

Such an interpretation of the HBNR could create significant liability for vendors of PHRs and PHR-related entities for the activities of independent third-party service providers.

The FTC requests comment on this approach, but if it remains in the final regulations, then it would underscore the need for vendors of PHRs and PHR-related entities to improve their vendor diligence processes and strengthen contractual language with third-party service providers to limit liability and obligations under the HBNR that might result from onward disclosures.

With the FTC's renewed interest in enforcing the HBNR, the NPRM should pique the interest of many businesses in the health care space, and such businesses should take the time to review the NPRM, including the FTC's requests for comment, and submit a comment to help shape the final modifications to the HBNR.

We expect to see more activity on this front in the near future, not only from the FTC but also from states, which are increasingly trying to regulate businesses that process health information.

Most recently, Washington enacted the My Health My Data Act to impose requirements on entities that collect, use or share health information, including a requirement to obtain opt-in consent prior to collecting health information.[5]

Another area of focus to watch is protecting the confidentiality of information related to reproductive health care.

Since the U.S. Supreme Court's 2022 decision in Dobbs v. Jackson Women's Health Organization, various states have imposed criminal, civil or administrative liability for, or created private rights of action against, individuals who obtain certain reproductive health care such as pregnancy termination, as well as the health care providers who provide such services.

In response, the U.S. Department of Health and Human Services recently issued a notice of proposed rulemaking to amend HIPAA regulations in an effort to strengthen the confidentiality of reproductive health care information.

In addition, what ultimately became the My Health My Data Act originally began as an effort by Washington state legislators to bolster protections for reproductive health care information.

Lastly, the FTC itself has signaled that this may be an area of enforcement focus as it recently took enforcement action against a developer of an ovulation tracker application for allegedly violating the FTC Act and HBNR.

Jodi Daniel is a partner at Crowell & Moring LLP and a managing director at the firm's consulting practice, Crowell Health Solutions.

Brandon Ge is counsel at the firm and a director at Crowell Health Solutions.

[1] https://www.ftc.gov/system/files/ftc_gov/pdf/p205405_proposed_hbnr_for_posting_only_.pdf.

[2] https://www.crowell.com/a/web/voAxhYZ9Wdd8tKSSJLv257/4Ttkbh/20211001-ftcs-hasty-health-data-rule-change-could-cause-confusion.pdf.

[3] https://www.crowell.com/en/insights/client-alerts/ftc-imposes-dollar15-million-civil-penalty-in-first-of-its-kind-health-breach-notification-rule-enforcement-action. See also https://www.crowellhealthsolutionsblog.com/2023/05/ftc-continues-to-enforce-against-data-practices-of-healthcare-apps/.

[4] https://www.crowell.com/en/insights/client-alerts/ftc-enforcement-against-sharing-consumer-health-information-continues.

[5] https://www.crowell.com/en/insights/client-alerts/washington-enacts-my-health-my-data-act-to-strengthen-protections-for-health-data.