ROPES & GRAY

ALERT

June 7, 2023

FTC Proposes Changes to Health Breach Notification Rule and Finalizes Second Enforcement Action under the Rule

Attorneys
Christine Moundas
Jenn Romig
Kathleen Swanson
Kris Kenn

On May 18, 2023, the Federal Trade Commission (FTC) announced a Notice of Proposed Rulemaking and a parallel Request for Comment on changes to the Health Breach Notification Rule (HBNR). The HBNR, which has been in effect since 2010, presently requires vendors of personal health records (PHRs) and PHR-related entities not covered by the Health Insurance Portability and Accountability Act (HIPAA) to notify individuals, the FTC, and, in some cases, the media of breaches of unsecured personally identifiable health data. The rule also requires third-party service providers that contract with vendors of PHRs and PHR-related entities to provide notification to such vendors and entities following the discovery of a breach. While the FTC issued a policy statement in 2021 affirming that health apps and connected devices that use or collect consumers' health information must comply with the HBNR, the proposed changes aim to clarify the scope of the rule, eliminating the ambiguity brought on by the advancements in technology seen in today's health-centric apps, wearable tech, and targeted marketing efforts.

The proposed changes come on the heels of a new HBNR enforcement action, only the second to occur in the HBNR's history. On May 17, 2023, the day before announcing the Notice of Proposed Rulemaking, the Department of Justice ("DOJ") filed a complaint on behalf of the FTC against Easy Healthcare Corporation for unauthorized data sharing, as further described below. The proposed changes and use of the HBNR as an enforcement tool demonstrate the FTC's new focus on ending the unauthorized sharing of health data by non-HIPAA-regulated entities and its goal of strengthening the rule's applicability to health information generated by health apps and other evolving technologies.

Proposed Changes

The significant proposed changes to the HBNR are summarized as follows:

- **Modify key definitions to clearly include health data generated by mobile health applications.** The proposed rule clarifies the definition of "PHR identifiable health information" while also adding two new definitions—"health care providers" and "health care services or supplies"—and expanding the definition of "PHR related entity" to clearly include entities that offer products and services through online services, including mobile apps.
    - "PHR identifiable health information" (which is sometimes referred to in the proposed rule as "PHR identifiable information") was previously described as "individually identifiable health information" as defined in § 1171 of the Social Security Act. However, the actual definition was not provided, requiring entities to refer to the Social Security Act for clarification. The FTC's proposed modification spells out the definition to more easily determine the persons or entities that fall within that category, and proposes that "PHR identifiable health information" be defined as information that:
        1. is provided by or on behalf of an individual;
        2. identifies or can be reasonably believed to be used to identify an individual;
        3. relates to an individual's past, present, or future physical or mental health or condition (including provision of and payment for health care services); and

4. is created or received by a health care provider, health plan, employer, or health care clearinghouse.

- After being left undefined in the previous rule, "health care provider" is now defined as "a provider of services, provider of medical or other health services, or any entity furnishing health care services or supplies." While "provider of services" and provider of "medical or other health services" are cross-referenced to definitions in other statutes, "health care services or supplies" is explicitly defined in the proposed rule as including "any online service, such as a website, mobile application, or Internet-connected device" that provides health-related tracking of almost any kind.

- The FTC proposes both (1) expanding the definition of "PHR related entity" to clearly include entities that offer products and services through online services, including mobile applications, and (2) limiting the definition to entities that send *unsecured* PHR identifiable health information to a PHR (rather than send *any* information to a PHR).

- **The definition of a security breach is expanded to include the sending of PHR identifiable health information to third parties.** The proposed changes clarify that security breaches are not limited to cybersecurity intrusions but also include unauthorized acquisitions that occur as a result of unauthorized disclosures. Through this proposed change, the FTC would consider including as a breach any unauthorized disclosure of a consumer's PHR identifiable health information to a third-party company.

- **Clarify that apps that can aggregate health information qualify as "personal health records" regardless of whether or not the function is utilized.** Currently a "personal health record" is defined as an electronic record of PHR identifiable health information that can be drawn from multiple sources and is primarily used by an individual. The FTC proposes a change to note that the record need only have the *technical* capacity to be drawn from multiple information sources. Accordingly, a depression management app that allows the input of mental health symptoms and has the technical capacity to be synced with a sleep tracker would qualify as a personal health record, even if the user does not use the syncing function. As such, whether apps qualify as "personal health records" would not depend on consumers' use of the app but only on its technical specifications.

- **Facilitate providing electronic notice to individuals, expand notice requirements, and offer a model notice.** The proposed changes would permit vendors of PHRs or PHR related entities to provide clear and conspicuous written notice by electronic mail, if an individual has specified electronic mail as the primary contact method, or by first-class mail. Additionally, the FTC expanded what is required in the post-breach notice, requiring that it include information on potential harms that could result based on the information breached, the contact information of any third parties that acquired unsecured PHR identifiable health information, and a description of the types of information breached. The FTC has also offered a model notice for entities to use to notify individuals following a breach.

- **Seek comment on a variety of considered changes not proposed.** Additional areas for comment include clarifications to the defined terms "authorization," "affirmative express consent," and "third party service provider," as well as extension of the required notice period to the FTC of a breach from 10 days to the HIPAA standard of 60 calendar days.

The public has 60 days to submit comments on the proposed changes to the rule, which will then be posted on Regulations.gov for public viewing. Entities should keep abreast of these upcoming changes and reflect on what they may mean for their business and compliance.

Second Enforcement Action against Easy Healthcare Corporation

The day before announcing the proposed changes to the HBNR, the DOJ filed a complaint against Easy Healthcare Corporation on behalf of the FTC alleging that the corporation's fertility app, Premom, deceived users by violating their promise to not share health information with third parties without the user's knowledge or consent, failed to implement reasonable privacy and data security measures, and failed to provide notice following a breach of unsecured health information in violation of the HBNR.

Specifically, the FTC claims that Easy Healthcare Corporation "repeatedly and falsely promised Premom users in their privacy policies that [Premom]: (a) would not share health information with third parties without users' knowledge or consent; (b) to the extent [Premom] collected and shared any information, it was non-identifiable data; and (c) the data was used only for [Premom]'s own analytics or advertising." The FTC alleges these representations were "false or deceptive," stating that since 2018, Easy Healthcare Corporation has shared Premom users' identifiable health information with Google, AppsFlyer, Inc., and two foreign mobile analytics companies. These actions constituted a "breach of unsecured health information that requires notice to Premom users under the [HBNR]." In total, the FTC alleges eight counts of violating the FTC's prohibition against "unfair or deceptive acts or practices in or affecting commerce."

Although it admitted no wrongdoing, under the stipulated order filed with the complaint, Easy Healthcare Corporation agreed not to share user health information with third parties for advertising purposes, to obtain users' consent before sharing health data for any other purpose, to disclose to consumers how their personal data will be used, and to pay a $100,000 civil penalty. As part of a related action, Easy Healthcare Corporation has also agreed to a $100,000 settlement with Connecticut, Oregon, and the District of Columbia, which worked with the FTC, for violating their respective laws.

Key Takeaways

Non-HIPAA-covered entities that interact with health information should take care to review whether the HBNR presently—or the HBNR as revised—applies to their business, products, or services. While the FTC is moving to clarify the breadth of the HBNR in today's tech-heavy health world, it is also moving forward with present enforcement as seen in the action against Easy Healthcare Corporation. The proposed changes and the recent enforcement of the HBNR demonstrate the FTC's goal of curbing the unauthorized sharing of health data by non-HIPAA-regulated entities and its intent to strengthen the rule's applicability to continually evolving technologies.

* * *

If you have any questions concerning this Alert, please do not hesitate to contact one of the authors or your regular Ropes & Gray advisor.