Blogs
June 06, 2024
FTC Expands Health Breach Notification Rule

The Federal Trade Commission (FTC) announced on April 26, 2024, that a final rule modifying its Health Breach Notification Rule (HBNR) adopted on a 3-2 vote along party lines.

The final rule caps the FTC's transformation of the HBNR into a broad privacy and data breach notice rule widely applicable to health and wellness apps and websites from a traditional cybersecurity data breach notice rule applicable to a limited set of companies that offer online personal health record repositories or applications and those companies' service providers. That transformation began in 2021 when the FTC issued a policy statement that interpreted the rule to apply to the disclosure of covered information without an individual's authorization and to a broad range of health and wellness apps. The final rule codifies the interpretations in the 2021 policy statement and several subsequent enforcement actions to apply the HBNR to a broad range of health and wellness apps and to require "breach" notification when consumer identifiable health data is disclosed without consumer authorization, even outside of traditional cybersecurity intrusions. The final rule goes into effect on July 29, 2024.

Summary of Key Provisions and Updates

The HBNR requires "vendors of personal health records" (PHRs) and "PHR related entit[ies]" to notify affected individuals, the FTC, and in some cases the media following the discovery of a "breach of security" of "unsecured PHR identifiable health information." Violations can be subject to civil penalties of up to $51,744 per violation (indexed annually for inflation).

Expansion of covered entities. As under the previous version of the rule, the final rule carves out HIPAA-covered entities and HIPAA-covered activities of business associates from its scope. At the same time, the final rule changes and adds new definitions to codify the FTC's view that the rule broadly applies to health and wellness apps and websites. Notably:

- The final rule defines PHR as "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" (emphasis added). Whereas the prior rule provided that an electronic record qualified as a PHR only if it could draw identifiable *health information* from multiple sources, the FTC explains that, under the modified language, "a product is a personal health record if it can draw *any* information from multiple sources, even if it only draws *health* information from one source." As an example, the FTC describes a diet and fitness app that would be covered by the final rule because it has the technical capacity to draw identifiable health information from the user (e.g., name, weight, height, age) and non-health information (e.g., calendar entry info, location, and time zone) from the user's calendar. Importantly, the ability to "draw information from multiple sources" means the *technical capacity* to do so (e.g., via an application programming interface).
- The FTC expands the definition of "PHR identifiable health information" to include certain information if created or received by what it calls a "covered health care provider.". A "covered health care provider" is defined to include *any* entity that furnishes "health care services or supplies," which includes "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." According to the FTC, this expansion of the definition of PHR identifiable health information clarifies that the HBNR "covers online services related not only to medical issues" but also to "wellness issues (by including in the definition terms such as 'fitness, sleep, and diet')."
- At the same time, the notice obligations in the HBNR apply only to *vendors* of PHRs, their service providers, and "PHR related entities" (all defined separately from a "covered health care provider"), and the FTC explains that being a vendor of PHRs requires providing "an offering that relates *more than tangentially* to health" (emphasis added). As such, the FTC states that "a general retailer (one that sells food products, children's toys, garden supplies, healthcare products (such as pregnancy tests), or apparel (such as maternity clothes)) offering consumers an app to purchase and access purchases of these products – by itself – would not make the retailer a vendor of personal health records." However, as the dissent of Commissioners Holyoak and Ferguson notes, it is unclear when an app would cross the line from "tangentially related to health" to "more than tangentially related to health."
- As before, the rule applies to companies that access or send individually identifiable health information to PHRs or offer products or services through the website of such a vendor ("PHR related entit[ies]") as well as certain service providers of PHR vendors and PHR related entities. The FTC explains that the final rule clarifies that PHR related entities include only those that access or send "unsecured PHR identifiable health information to a personal health record" (not *any* information or *secured* PHR identifiable health information). For example, according to the FTC, the definition could include fitness trackers or remote blood pressure cuffs that sync to a health app but not a grocery delivery service that sends information about food purchases to a diet and fitness app if it does not access unsecured PHR identifiable health information in a PHR or transmit unsecured PHR identifiable health information to a PHR.

Broad definition of "breach of security." The final rule is triggered when a covered entity discovers a "breach of security," defined to include "unauthorized acquisition of unsecured PHR identifiable health information in a personal health record" that occurs as a result of a "data breach" or an "unauthorized disclosure." The final rule reflects the FTC's view that the rule should apply to "both cybersecurity intrusions as well as a company's intentional but unauthorized disclosure of consumers' PHR identifiable health information to third party companies." Unlike HIPAA and many state laws, there is no threshold risk of harm or any exceptions for situations like good faith inadvertent access by an employee. The FTC also suggests that there may be circumstances where unauthorized *use* of health data or derived or inferred health data can constitute a "breach of security" if a covered entity "exceeds unauthorized access to use PHR identifiable health information, such as

where it obtains the data for one legitimate purpose but later uses that data for a secondary purpose that was not originally authorized by the individual."

No definition of "authorization." The FTC declined to include in the rule a definition of what it means for a consumer to "authorize" the acquisition of their PHR identifiable health information. It instead explained that what constitutes authorization will be fact-specific and that any data use must be "consistent with a company's disclosures and consumers' reasonable expectations." Consistent with its recent enforcement activity in this area, as one of several examples provided, the FTC explained that disclosure of PHR identifiable health information for purposes of ad targeting without disclosure or affirmative express consent would be unauthorized as a deceptive omission.

Notice obligations. At a high level, the rule requires vendors of PHR records and PHR related entities to notify affected individuals and the FTC following the discovery of a breach affecting 500 or more individuals "without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach of security" and annually in the case of breaches affecting less than 500 individuals. These entities must also notify prominent media outlets of a state or jurisdiction if the information of 500 or more residents of the state or jurisdiction has been or is reasonably believed to have been acquired during the breach. The final rule also requires service providers to notify the vendor of PHR records or the PHR related entity following the discovery of a breach. Notice of a breach of security sent by email (allowed where the individual has selected email as their primary means of communication) must also be sent by text message, in-app message, or electronic banner. If email is not available, notice must be provided by first-class mail at the individual's last known address, and if contact information for ten or more individuals is insufficient or out of date, substitute notice is permissible, to consist of either posting the notice on the entity's website for 90 days or in major print or broadcast media. Key content of which the final rule requires notice includes, to the extent possible, the date of the breach and the date of discovery, a description of any third parties that acquired unsecured PHR identifiable health information resulting from the breach, the types of such information involved in the breach, the steps that the affected entity is taking to investigate the breach and protect affected individuals, and two contact methods for individuals to learn more.

Takeaways

Health privacy is a priority at the FTC, as evidenced not only by the final rule but also by the five cases brought by the FTC in the last year and a half alleging unauthorized sharing of consumer health data for advertising purposes. These cases include two announced this year (Cerebral and Monument Health) and two that allege violations of the previous version of the HBNR (GoodRx and Easy Healthcare). Developers of health and wellness apps and websites not subject to HIPAA and those entities that support or engage with them should evaluate whether they fall under the expanded scope of the HBNR to address how to proactively manage their legal risk in connection with a traditional cybersecurity intrusion or other potentially unauthorized disclosure or access. Despite significant questions about the full reach of the HBNR and the breadth of its enforcement in future administrations given the Republican commissioners' strong dissent, the rule is an attractive tool for the agency under its current leadership to seek civil penalties in its ongoing efforts to protect health data.

Authors

Explore more in

Privacy & Security