VOLUME 78 ◆ NUMBER 9

Employee Benefit Plan Review

Federal Trade Commission's Updated Health Breach Notification Rule Is Now in Effect

By Kathleen Benway, Jennifer C. Everett, Alysa Austin and Kristen Bartolotta

Revisions by the Federal Trade Commission (FTC) to the Health Breach Notification Rule (HBNR) took effect on July 29, 2024, imposing new reporting requirements on health-related vendors and mobile apps not previously covered by the rule. Among other changes, the rule expanded the definition of protected health records (PHRs), clarified that the rule applies to online platforms and mobile apps, and revised the method, time, and content for reporting data breaches to the FTC and impacted individuals.

The revisions to the HBNR follows recent FTC action against companies for violations of the rule, signaling a renewed focus on data breach notifications within the health care marketplace. Key provisions are addressed below.

Expanded Definition of PHR and PHR Identifiable Health Information

The rule expands the definition of PHR to mean "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." The HBNR's emphasis on a product's technical capacity to draw information from multiple sources – such as from a mobile health application rather than from the actual use of the product – significantly expands what information is subject to the rule. For example, a website or app that provides a symptom tracker to individuals who log in with a username or password and input their symptoms would constitute a PHR if the website or app collects geolocation information from an application programming interface (API). This is because it would have the technical capacity to draw information from multiple sources (i.e., consumer-populated data and API data) and contains PHR identifiable health information.

The rule also adds new definitions of "covered health care provider" and "health care services or supplies" to the definition of PHR identifiable health information, notably expanding the scope of the rule. The HBNR defines "covered health care provider" to include vendors of health apps, fitness trackers, other direct-to-consumer devices and technologies, or any other entity providing "health care services or supplies" (i.e., "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").

Expanded Scope and Applicability

The rule revises and adds several definitions to clarify the scope of the HBNR, which applies to:

(1) Foreign and domestic vendors of PHR;
(2) PHR-related entities; and
(3) Third-party service providers not covered by the Health Insurance Portability and Accountability Act (HIPAA).

- A vendor of PHR is an entity that offers or maintains (e.g., sells, markets, provides, or promotes) a PHR, which may include apps, websites, or online services that offer health-related products or services. Organizations that offer services that are only tangentially related to health (e.g., general retailers selling maternity clothing, food products, or children's toys) are not vendors of PHR.
- The rule clarifies the definition of "PHR related entities" to entities that (1) offer products or services through online services of vendors of PHRs, or (2) access or send unsecured PHR identifiable health information in or to a personal health record. This revised definition includes entities that provide, for example, remote blood pressure cuffs and blood glucose monitors when such devices are synced with a health app and share unsecured PHR identifiable health information. The FTC has further pointed to search engines that integrate a search bar branded with its logo into a health tracking app as a PHR-related entity.
- The rule defines third-party service providers as entities that provide services to vendors of PHR or PHR-related entities and further access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHR identifiable health information as a result of such services. Entities are not rendered PHR-related entities when they access unsecured PHR in the course of providing services. Examples of third-party service providers include firms providing attribution and analytics services to a health app or search engines that only provide back-end services (i.e., is not consumer-facing).

These changes make clear that the HBNR is intended to apply to health apps, connected devices, and other online services not covered by HIPAA.

Expanded Definition of a Breach of Security

A "breach of security" under the HBNR now includes any "unauthorized disclosure" of PHR identifiable health information, and not only a result of a cybersecurity incident and intrusion. Rather, any voluntary disclosure of PHR identifiable health information by a vendor of PHR or PHR-related entity that was not explicitly authorized by the individual consumer could constitute a breach of security.

The rule stopped short of defining how covered entities can or should obtain "authorization" but instead looks to the 2009 rule commentary[1] for guidance on "authorized" disclosures as well as the FTC's more recent enforcement actions. Notably, "dark patterns" would not allow for "meaningful choice." Additionally, sharing PHR identifiable health information with third-party advertisers contrary to stated privacy policies and without individual consent may constitute unauthorized disclosures.

Expanded Notification and Timing Requirements

The rule extended the notification deadline for breaches involving 500 or more individuals. While the rule previously required covered vendors of PHR and PHR-related entities to notify the FTC within 10 business days of discovering a breach of security, now such notifications can be made within 60 calendar days of discovering the breach contemporaneously with notifying affected individuals and the media.

Covered entities may now provide written notice via "electronic mail" provided the individual has specified electronic mail as the primary contact method. Email notices can be sent with a text message, in-app message, or electronic banner, effectively creating two-party electronic notice requirements for affected individuals.

The notice to the affected individuals also must adhere to new content requirements. The notice must now include:

(1) The name or identity (or if more appropriate, a description) of any unauthorized recipients of the unsecured PHR identifiable health information giving rise to the breach;
(2) A description of the types of unsecured PHR identifiable health information involved in the breach;
(3) A description of the potential harm that may result;
(4) A brief description of what the entity that experiences the breach is doing to protect the affected individuals (e.g., credit monitoring or similar services); and
(5) Two or more ways to contact the notifying entity.

FTC's Enforcement Efforts

Even before the revised rule was finalized, the FTC used the then 14-year-old previous version

of the rule for the first time, in 2023, against companies in the digital health care space, signaling a renewed focus on consumer privacy and security in the industry.

In its action against GoodRx, the FTC alleged that the company violated the HBNR by sharing health data with third-party digital advertising and analytics providers in a manner that was inconsistent with its own privacy policy.

In its second enforcement action for violations of the HBNR, the FTC similarly alleged that the fertility tracking app Premom's sharing of health-related information with third-party advertisers amounted to a "breach" under the rule.

Finally, the FTC brought an enforcement action against online mental health counseling service BetterHelp, alleging that the company's collection, use, and disclosure of consumer health data without prior affirmative express consent were unfair and deceptive acts and practices under Section 5 of the FTC Act.

Violators of the rule are subject to injunctions and monetary remedies, including consumer redress and civil penalties of up to $51,744 per violation.

Conclusion

- Organizations should consider whether the expanded reach of the rule is applicable to them. In particular, they should assess whether they qualify as a vendor of PHR or a PHR-related entity under the new "covered health care provider" and "health care services or supplies" definitions.

Organizations should consider whether the expanded reach of the rule is applicable to them.

- In-scope companies should review their notice and consent programs to ensure all information that could be considered PHR identifiable health information is shared with the consent of the individual in a way that is consistent with public-facing privacy policies.
- Covered entities should review their incident response plans to ensure the updated notification timelines are reflected, and that there are processes in place that enable the organization to meet the content and timing requirements for reporting an incident to affected individuals and the FTC, as appropriate.

Note

1. https://www.federalregister.gov/documents/2009/08/25/E9-20142/health-breach-notification-rule.

The authors, attorneys with Alston & Bird LLP, may be contacted at kathleen.benway@alston.com, jennifer.everett@alston.com, alysa.austin@alston.com and kristen.bartolotta@alston.com, respectively.