Federal Trade Commission Finalizes Updates to the Health Breach Notification Rule

May 17, 2024

On April 26, 2024, the Federal Trade Commission (the "FTC") issued a controversial final rule (the "Final Rule") that, among other things, expands the scope of the Health Breach Notification Rule (the "HBNR" or the "Rule") to apply to health apps and related technologies. Driven by the popularity and increasing variety of direct-to-consumer healthcare technologies, many companies that do not fall within the ambit of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") now routinely collect and possess large quantities of sensitive consumer health data (e.g., fertility, fitness, glucose levels, heart rate). The Final Rule will impose reporting obligations on newly covered entities, considerably limit how all covered entities may share sensitive health data and create updated reporting obligations for traditional security breaches.

Adopted in 2009 to protect consumer health information that falls outside the scope of HIPAA, the HBNR requires vendors that collect or have access to identifying health information to alert individuals, the FTC and, in some cases, the media when such information is disclosed without authorization. In addition, third-party providers to such vendors are required to notify vendors if a breach is discovered. Failure to comply with the HBNR can result in penalties of up to $51,744 per violation. Until recently, the requirements of the Rule were largely unenforced and thought to apply only when a covered entity experienced a data breach. However, the FTC's 2021 policy statement and several recent enforcement actions that followed indicate the agency's intent to expand the scope of the HBNR to: (a) treat as a breach of security so-called "unauthorized disclosures" (i.e., disclosures without consumer consent) of personal health record ("PHR")-identifiable information; and (b) treat health apps and connected devices as "vendors" of PHRs subject to the requirements of the Rule. In May 2023, the FTC issued a Notice of Proposed Rulemaking and a parallel Request for Comment on the proposed changes to clarify its application and the circumstances that constitute an unauthorized disclosure under the Rule.

The Final Rule largely adopts the changes from the proposed rule. Below, we summarize key provisions of the Final Rule.

Expanded Scope & Applicability

The Final Rule expands the scope of applicability of the HBNR, and it is limited to entities that: (1) are not covered by HIPAA and (2) offer or maintain PHRs (i.e., PHR-identifiable health information). While this language may appear exceedingly broad at first glance, certain definitions limit the scope of the HBNR to businesses whose services involve offering or maintaining (e.g., selling, marketing, providing or promoting) a health-related product or service, meaning the entity's business must be more than tangentially related to health; the HBNR would not apply to companies that simply possess PHR-identifiable health information incident to non-health-related services or general retailers with a website or app that simply provides the ability to access or purchase health-adjacent products (e.g., sellers of healthcare products such as pregnancy tests, sellers of apparel such as maternity clothes).[1] However, newly confirmed Commissioners Melissa Holyoak and Andrew Ferguson expressed skepticism in their dissenting statement and warned that the Rule's expansive definitions work to significantly expand its scope.

- PHR Identifiable Health Information. PHR identifiable health information consists of individually identifiable health information created or received by a covered *healthcare provider*, health plan, employer or healthcare clearinghouse. The definition of "covered healthcare provider" expands the scope by including entities that provide "services," "medical or other health services" or "healthcare services or supplies." Such terms draw on existing definitions in federal statutes and capture healthcare-related services (e.g., hospital, skilled nursing facilities, outpatient rehabilitation facilities).[2] The FTC defines "healthcare services or supplies" in the Final Rule to include any online services that provide a mechanism to track a wide range of health-related metrics (e.g., disease, health conditions, diagnoses or diagnostic testing, medications, vital signs, mental health, fitness, fertility).

The expansion of "covered healthcare provider" to include entities that furnish "healthcare services or supplies" reinforces the FTC's strong stance on protecting sensitive health information created and maintained by health apps, websites and similar technologies that are not covered by HIPAA and attempts to capture such entities within the ambit of the HBNR. The Final Rule also confirms that the HBNR

---

1 Note, however, that a general retailer may become a vendor of personal health records where a website or application offers features or functionalities that are sold, marketed or promoted to consumers as having more than a tangential relationship to health. Health Breach Notification Final Rule at 28 (Apr. 26, 2024) (available here).

2 For the definition of "provider of services" as used in the Final Rule, *see* 42 U.S.C. § 1395x(u). For the definition of "medical or other health services" as used in the Final Rule, *see* 42 U.S.C. § 1395x(s).

covers information such as unique device and mobile advertising identifiers that, when combined with health information, can be used to identify an individual.

- PHR-Related Entity. The HBNR also imposes breach notification obligations on "PHR-related entities." The Final Rule clarifies that a "PHR-related entity" includes entities that offer products and services through any online service of vendors of personal health records, including mobile applications. It also makes clear that only entities that access or send *unsecured* (i.e., unencrypted) *PH-identifiable health information* to a PHR qualify as a PHR-related entity. Mere access to PHR-identifiable health information does not render a third-party service provider a PHR-related entity.

PHRs That Draw Information from Multiple Sources

The Final Rule clarifies that the definition of a PHR includes an electronic record of PHR-identifiable health information with the "technical capacity" to draw information from multiple sources. This definition is exceedingly broad and could cause numerous websites and health apps that retrieve data from several sources to be labeled PHRs. One example provided in the Final Rule is a depression-management app that allows consumers to input mental health states and has the technical capacity to sync with a sleep monitor. Even if consumers choose only to use the app to track mental health states and do not sync a wearable sleep monitor to the app, the app has the capacity to draw information from both customer input and the sleep monitor. Therefore, the app has the technical capacity to draw information from multiple sources.[3]

Broad Definition of Breach of Security Encompasses Some Voluntary Disclosures

A "breach of security" continues to be defined as any acquisition of unsecured PHR-identifiable health information without an individual's authorization. The Final Rule adds "[a] breach of security includes an 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." This appears intended to ensure that the definition extends beyond a cybersecurity incident to include *voluntary disclosures* of PHR-identifiable health information—such as sales of that data or provision of that data to certain third parties for services such as online advertising. This closely tracks the approach taken by the U.S. Department of Health and Human Services Office of

[3] Health Breach Notification Final Rule at 32 (Apr. 26, 2024), available here.

Civil Rights with respect to online tracking technologies and HIPAA.[4] This will necessarily require many entities to obtain individuals' consent before sharing health data in many circumstances. This matches the FTC's approach in recent enforcement actions against Premom, BetterHelp and GoodRx—the companies in each action were penalized for failing to obtain individuals' affirmative consent prior to sharing health information with third parties.

Revised Breach Notification Requirements

The Final Rule expands the timelines for notification of a breach under the HBNR. Previously, for breaches involving at least 500 individuals, the HBNR required notice to the FTC "as soon as possible and in no case later than ten business days following the date of the discovery of the breach." The amended Rule matches the requirements set out under the HIPAA Breach Notification Rule:

- Breaches Involving Fewer Than 500 Individuals. Notice to affected individuals must be provided without unreasonable delay and no later than 60 days following the discovery of the breach. The entity may maintain a log of such breaches and submit such log annually to the FTC no later than 60 calendar days following the end of the calendar year, documenting breaches from the preceding calendar year.

- Breaches Involving 500 or More Individuals. Notice must be provided simultaneously to the FTC and affected individuals without unreasonable delay and no later than 60 calendar days after the discovery of the breach.

The Final Rule also requires a breach notification to include the name or identity of third parties that acquired unsecured PHR-identifiable health information and the types of health information involved in the breach. As a practical matter, the identity of the third party that acquired covered data will only be known when a covered entity has made a voluntary disclosure of such data. Further, the Final Rule breaks from longstanding tradition that required notification to be sent by first-class mail and only allowed notification by email in limited circumstances; now notice of a breach can be sent by email in the first instance so long as individuals have specified that email is their preferred form of contact.

---

[4] We previously discussed guidance issued by the U.S. Department of Health and Human Services Office of Civil Rights concerning the use of online tracking technology by HIPAA-covered entities and their business associates. *See* Debevoise Update, Proceed with Caution: Online Tracking Technologies Pose HIPAA Compliance Risks (Mar. 2, 2023), available here.

Key Takeaways

The controversy of the Final Rule is underscored by the split 3-2 decision to finalize the changes. Commissioners Lina Khan, Rebecca Kelly Slaughter and Alvaro Bedoya emphasized, in their joint statement, that the Final Rule modernizes the HBNR and will allow it to "keep pace with the rapid proliferation of digital health records." Commissioners Holyoak and Ferguson, however, expressed concern that the scope of regulated entities remains unclear and that the changes imposed by the Final Rule could exceed the Commission's statutory rulemaking authority.

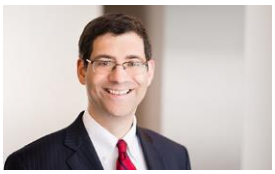
The Final Rule is the culmination of the FTC's increasingly aggressive approach towards protecting non-HIPAA-regulated health data and shaping health technology data practices. Given the potential far-reaching scope of the HBNR as revised, companies and other stakeholders should take protective steps to address compliance concerns:

- Evaluate potential exposure under the HBNR by identifying what health information is being collected and shared with third parties and whether proper consents are being collected;
- Review and update internal policies related to health data collection and sharing;
- Ensure that compliance programs are appropriately resourced and prioritize a compliance-focused approach to health data collection and sharing;
- Engage counsel to timely assess notification requirements in the event that a company becomes aware of a potential breach; and
- Monitor enforcement precedent, legal developments across U.S. jurisdictions and guidance from the FTC.

We will continue to monitor the FTC's enforcement of the HBNR and related developments. Please do not hesitate to contact us with any questions.

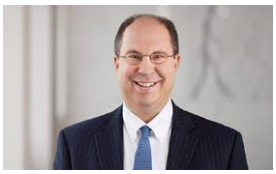
* * *

Please do not hesitate to contact us with any questions.



Andrew L. Bab
Partner, New York
+1 212 909 6323
albab@debevoise.com

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com



Paul D. Rubin
Partner, Washington D.C.
+1 202 383 8150
pdrubin@debevoise.com

Kim T. Le
Counsel, San Francisco
+1 415 738 5706
kle@debevoise.com

Melissa Runsten
Counsel, Washington D.C.
+1 646 988 5217
mrunsten@debevoise.com

Johanna N. Skrzypczyk
Counsel, New York
+1 212 909 6291
jnskrzypczyk@debevoise.com

Michael L. Cederblom
Associate, New York
+1 212 909 6043
mlcederb@debevoise.com

Hannah R. Levine
Associate, New York
+1 212 909 6095
hrlevine@debevoise.com

Kaitlyn McGill
Associate, New York
+1 212 909 6817
kemcgill@debevoise.com

Annabella M. Waszkiewicz
Law Clerk, New York
+1 212 909 7484
amwaszki@debevoise.com