Now & Next
Healthcare Alert

May 22, 2024

FTC amends and broadens Health Breach Notification Rule

By Julia E. Cassidy and Freddy R. Lopez

The amendments clarify the Rule's scope to apply to health apps and similar technologies, revise key definitions, modernize the method and content of notice, and alter the timing requirement for notifying the FTC.

What's the impact?

- The FTC's Health Breach Notification Rule (the HBN Rule) aims to protect consumers' health data from unauthorized access or disclosure by requiring vendors of personal health records and related entities not covered by HIPAA to notify individuals, the FTC, and, where applicable, the media, of a breach.
- Lawmakers have responded to the widespread use of apps that track health biometrics by assessing the application of health privacy and security laws to these new modalities and advocating for wider consumer protections.

The Federal Trade Commission (FTC) has issued a final rule modifying the HBN Rule (the Final Rule), which broadens the scope of entities subject to the HBN Rule, including many mobile

health applications (apps) and similar technologies, and clarifies that breaches subject to the HBN Rule include not only cybersecurity intrusions but also unauthorized disclosures, even those that are voluntary. The HBN Rule does not apply to covered entities under the Health Insurance Portability and Accountability Act (HIPAA) or their business associates, which remain subject to the US Department of Health and Human Services' (HHS) Breach Notification Rule. The Final Rule is effective on July 29, 2024.

While there have been recent breaches affecting well-known healthcare entities that are subject to HIPAA, such as the United Healthcare/Change Healthcare breach, the widespread use of apps that track biometrics, user health, and fitness has forced lawmakers to reassess the application of health privacy and security laws to new modalities, and in light of these changing complexities, consider wider consumer protections. COVID-19 and the ensuing years have functioned as accelerants, encouraging further adoption of health-related technologies.

The HBN Rule was originally adopted in 2009 to require vendors of personal health records (PHRs) and similar entities that are not regulated by HIPAA to notify consumers, the FTC, and, in some cases, the media, in instances where there was a breach of unsecured personally identifiable information. In September 2021, the FTC issued a Policy Statement that provided guidance on the scope of the HBN Rule. The Policy Statement made clear that the FTC had a much broader interpretation of the HBN Rule, which it has now codified through the Final Rule. The FTC's refresh of this rule sheds a clarifying light on its posture on the subject, stretching the scope of its rulemaking authority to offer more scrupulous observance on an aspect outside the scope of HIPAA.

FTC changes to the HBN Rule

CLARIFICATION OF ENTITIES COVERED

The Final Rule revises several definitions and also adds new defined terms. Specifically, the Final Rule revises the definitions of "PHR identifiable health information" and "PHR related entity" and adds definitions of "covered health care provider" and "health care services or supplies" to broaden the scope of the HBN Rule.

The Final Rule defines "PHR identifiable health information" as information that "(1) 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 (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual; and (2) is created or received by a: (i) covered health care provider; (ii) health plan (as defined in 42 U.S.C. 1320d(5)); (iii) employer; or (iv) health care clearinghouse (as defined in 42 U.S.C. 1320d(2)); and (3) with respect to an individual, includes information that is provided by or on behalf of the individual."

"Covered Health care provider" means a provider of services (as defined in 42 U.S.C. 1395x(u)), a provider of medical or other health services (as defined in 42 U.S.C. 1395x(s)), or any other entity furnishing healthcare services or supplies.

"Health care services or supplies" means 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.

The FTC explained that the changes to the definitions clarified that developers of health apps and similar technologies providing "health care services or supplies" qualify as "health care providers" so that any individually identifiable information these products collect or use would constitute "PHR identifiable health information" covered by the Final Rule. Therefore, the developers of these types of apps and technologies can be vendors of PHRs subject to the Final Rule.

In addition, the Final Rule defines a "PHR related entity" as an entity, other than a HIPAA covered entity or a business associate of a HIPAA covered entity, that: (1) offers products or services through the website, including any online service, of a vendor of personal health records; (2) offers products or services through the websites, including any online service, of HIPAA covered entities that offer individuals' personal health records; or (3) accesses *unsecured* PHR identifiable health information in a personal health record or sends *unsecured* PHR identifiable health information to a personal health record.

The FTC explained that the change to cover online services was necessary as websites are no longer the only means through which consumers access health information online. The FTC stated that narrowing the scope of "PHR related entities" to entities that access or send *unsecured PHR identifiable health* information was intended to eliminate potential confusion about the Final Rule's breadth and promote compliance by narrowing the scope of entities that qualify as PHR related entities.

CLARIFICATION REGARDING TYPES OF BREACHES SUBJECT TO THE HBN RULE

The Final Rule changes the definition of "breach of security" to clarify that a breach of security under the Final Rule includes unauthorized acquisitions that occur as a result of a data breach *or* an unauthorized disclosure. The changes highlight the fact that a breach of security is not limited to data exfiltration, and includes unauthorized disclosures or unauthorized uses of data (such as a company's unauthorized sharing or selling of consumers' information to third parties that is inconsistent with the company's representations to consumers).

REVISIONS AND UPDATES TO METHOD OF NOTICE

The Final Rule modernizes the method of notice to consumers of a breach to allow notice by electronic mail so long as the consumer has consented to receive electronic communications. The Final Rule defines electronic mail as email in combination with a text message, within-application messaging, or electronic banner so long as the notice is conspicuous. The Final Rule also modifies the required content of the notice to include additional information, including the full name or identity of the third parties that acquired the PHR identifiable information as a result of the breach, a brief description of what the notifying entity is doing to protect the affected individuals, and contact procedures that must include at least two of the following: toll-free phone number, email address, website, in-app, or postal address.

REVISIONS AND UPDATES TO FTC NOTIFICATION AND PUBLICATION

The Final Rule aligns the FTC's notification timeline with the timeline required by HIPAA's Breach Notification Rule. Entities that experience a breach of security involving the unsecured PHR identifiable health information of 500 or more individuals must notify the FTC contemporaneously with the notice required to the affected individuals. The notice to the FTC must be sent "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security." Previously, the FTC required such notice to be provided "as soon as possible and in no case later than ten business days" after the breach's discovery.

In enacting this change, the FTC believes that this new notice requirement will allow parties sufficient time to provide more complete notifications. The change to the timing of notice to the FTC does not affect the timing of the notice to the FTC for breaches involving fewer than 500 individuals, which may still be sent annually to the FTC no later than 60 calendar days following the end of the calendar year.

Complying with the breach notification Final Rule

The Final Rule clarifies the definitions and scope of the entities and information subject to the rule, modernizes the methods and content of the breach notifications, and aligns the timing for notifying the FTC with the HIPAA breach notification rule. The rule is a response to the changing landscape of health-related technologies and the need to extend consumer protections to non-HIPAA covered entities that handle sensitive health information.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Julia E. Cassidy
212.940.3137
jcassidy@nixonpeabody.com

Freddy R. Lopez
213.629.6038
flopez@nixonpeabody.com