GT GreenbergTraurig

Alert | Health Care & FDA Practice

May 2023

FTC Proposes Changes to Health Breach Notification Rule

Go-To Guide:
• The FTC issued a proposed rule updating the Health Breach Notification Rule.
• The proposed rule would expand the Health Breach Notification Rule to cover health applications and similar technologies.
• Key changes under the proposed rule include new and clarified definitions and revised notice requirements.

On May 18, 2023, the Federal Trade Commission (FTC) issued a proposed rule that would expand the existing Health Breach Notification Rule (HBNR) to cover health applications (apps) and other similar technologies. Given the rapid evolution of the health technology industry since the HBNR was issued in 2009, the FTC has expressed concern that the rule fails to cover widely used health apps and connected devices, thereby failing to fully protect the users of these technologies.

The changes under the proposed rule would impact a range of companies, including:

- Retailers and internet companies who collect "interest" information from consumers including health topics and profiles;

- Internet application operators that collect and store health data (such as step counters, weight management applications, fertility-tracking applications, and sleep tracking applications);
- Companies that offer products and services through companies and websites that engage in the above-mentioned activities.

Background

The HBNR in its current form requires vendors of personal health records (PHR) and related entities that are not covered by the Health Insurance Portability and Accountability Act (HIPAA) to notify individuals, the FTC, and, in some cases, the media of a breach of unsecured personally identifiable health data. It also requires third-party service providers to vendors of PHRs and PHR-related entities to notify such vendors and PHR-related entities following a breach discovery. PHR-related entities include companies that offer products and services through PHR websites and access information in or send information to personal health records.

In an effort to align the HBNR with the current technology landscape, in 2020 the FTC sought public comment on whether changes were needed to the rule, and in September 2021, the FTC issued a policy statement affirming that health apps and connected devices that collect or use consumers' health information must comply with the HBNR. The FTC addressed the public comments with the following proposed changes to the HBNR.

Key Changes

I. Revising Definitions and Clarifying Applicability

A. *PHR Identifiable Health Information, Health Care Provider, and Health Care Services or Supplies*

The proposed rule includes revised definitions intended to clarify the HBNR and its application to health apps and similar technologies that HIPAA does not cover. First, under the proposed rule, "PHR identifiable information" would be defined as information that:

1) is provided by or on behalf of the individual;

2) identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual;

3) 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

4) is created or received by a health care provider, health plan (as defined in 42 U.S.C. 1320d(5)), employer, or health care clearinghouse (as defined in 42 U.S.C. 1320d(2)).

A new term—"health care provider"—is also included, and defined as 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 health care services or supplies. The proposed rule also adds a new definition for the term "health care services or supplies" to include 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.

These changes specifically clarify that developers of health apps and similar technologies that provide these types of "health care services or supplies" qualify as "health care providers" under the proposed rule. Since they would qualify as health care providers, any individually identifiable health information that these products collected or used would constitute "PHR identifiable health information," which the proposed rule covers. The changes also clarify that mobile health applications are considered a "personal health record" covered by the proposed rule (so long as other conditions included in the definition of "personal health record" are met), and accordingly, the developers of these applications are "vendors of personal health records."

B. *Breach of Security*

The proposed rule would amend the definition of "breach of security" to include unauthorized acquisitions that occurred as a result of a data breach or unauthorized disclosure. The HBNR currently defines "breach of security" as the acquisition of unsecured PHR identifiable health information of an individual in a personal health record without the authorization of the individual. The proposed rule would add the following sentence to the end of the definition: "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."

C. *PHR-Related Entity*

The proposed rule would revise the definition of "PHR-related entity," which is currently defined in the HBNR 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 of a vendor of personal health records; (2) offers products or services through the websites of HIPAA-covered entities that offer individual personal health records; or (3) accesses information in a personal health record or sends information to a personal health record.

The proposed updates include language to clarify that PHR-related entities include entities offering products and services not only through the websites of vendors of personal health records but also through any online service, including mobile apps. In addition, the proposed rule would narrow the scope of the rule's applicability and revise the third prong of the definition so that only entities that access or send unsecured PHR identifiable health information to a personal health record (rather than entities that access or send any information to a personal health record) would qualify as PHR-related entities.

D. *Personal Health Record*

Under the current HBNR, a personal health record is defined as an electronic record of PHR identifiable health information that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual. To clarify what it means to "draw information from multiple sources," the proposed rule would define "personal health record" 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.

II. Modernizing Method of Notice and Expanding Notice Content

The current HBNR permits notice of breach to consumers by postal mail, and in limited circumstances, email. Past comments on this requirement noted that it is inefficient, costly, and does not reflect the realities of modern communication. To address these concerns, the proposed rule would revise this provision to specify that vendors of personal health records or PHR-related entities that discover a breach of security must provide written notice using the last known contact information of the individual, and the required written notice may be sent by electronic mail if an individual has specified electronic mail as the primary contact method, or by first-class mail. In addition, "electronic mail" would be revised to mean email in combination with one or more of the following: text message, within-application messaging, or electronic banner. This two-part notice is intended to increase the likelihood that consumers will actually see the notice.

In addition to modifying the method of notice, the proposed rule would also include modifications to the content of required notices. Currently, the HBNR requires a breach notice to a consumer to contain:

- A description of the breach and the types of unsecured PHR identifiable health information involved in the breach;
- Steps individuals should take to protect themselves from potential harm stemming from the breach;
- A description of steps the vendor of personal health records or PHR related entity is taking to address the breach;
- Contact procedures for individuals to ask questions and learn additional information.

The proposed rule would include several changes to the content of the notice, including:

- In addition to including a description of the breach, the notice must also include a brief description of the potential harm that may result from the breach;
- The notice must include the full name, website, and contact information of any third parties that acquired unsecured PHR identifiable health information as a result of a breach (if this information is known to the vendor of personal health records or PHR related entity);
- The list of the types of health information that may be involved in the breach has been expanded to include health diagnosis or condition, lab results, the individual's use of a health-related mobile application, and device identifier;
- In addition to describing what the vendor or PHR-related entity is doing to investigate the breach, the notice must also include a description of what is being done to protect affected individuals (such as credit monitoring).

Looking Forward

The proposed changes follow a period of increased enforcement activity from the FTC aimed at addressing privacy concerns from health-related applications and companies. Notably, in February 2023, the FTC announced its first enforcement action under the HBNR against telehealth and prescription drug discount provider GoodRx Holdings, Inc, and on May 17, 2023, announced a proposed order settling allegations against Premom, a fertility-tracking app. Both companies were accused of selling user's data to third-party companies without consumers' consent.

The FTC's recent enforcement actions are occurring in tandem with increased legislative and regulatory activity at the state level to address privacy and consumer protections. Companies may wish to review the potential impact of this increased enforcement and oversight and determine whether operational changes are needed.

For companies interested in responding to the proposed rule, comments are due 60 days following publication in the Federal Register.

Authors

This GT Alert was prepared by:

- Eleanor (Miki) A. Kolton | +1 202.331.3134 | koltonm@gtlaw.com
- Tess Dillon Meyer | +1 202.533.2319 | Tess.Meyer@gtlaw.com