Summary: FTC Health Breach Notification Rule

Updated: May 2024

Background

The Federal Trade Commission (FTC) released its finalized Health Breach Notification Rule (HBNR) on April 26, 2024. The rule finalizes proposals from the FTC's May 2023 proposed rule that updated the 2009 Health Breach Notification Rule. The rule seeks to regulate non-HIPAA covered personal health records (PHRs) to notify customers of data breaches. Previously, the HBNR had a narrow definition of PHRs that left out app vendors, wearable technologies, and other direct-to-consumer health technologies. These entities are now included in the 2024 final rule.

Key Provisions

- Updates the definition of "*personal health record (PHR) identifiable health information*" to mean "information (1) provided by or on behalf of the individual; (2) that identifies the individual or with respect to which there is a reasonable basis to believe that 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 healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual; and (4) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse."

- Modifies the proposed definition of "*healthcare provider*" to "covered healthcare provider that provides healthcare services, a provider of medical or other health services, or any other entity furnishing healthcare services or supplies."

- Defines "*healthcare services or supplies"* as "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 clarifies that to be a vendor of PHRs under the Rule, an app, website, or online service must provide an offering that relates more than tangentially to health.

- Clarifies the definition of PHR to state that "an electronic record of PHR identifiable health information on an individual must have the technical capacity to draw information from multiple sources, and must be managed, shared, and controlled by or primarily for the individual."

- Clarifies that a breach of security under the Rule includes unauthorized acquisitions that occur from a data breach or an unauthorized disclosure.
    - The FTC does not define "authorization" as it believes a fact-specific inquiry is needed to determine if a disclosure was authorized.

- Defines PHR related entities to include entities that access or send unsecured PHR identifiable health information to a PHR.

- Clarifications provided by the FTC include:
    - Entities that offer products and services through the website of vendors of PHRs, and through any online service, including mobile apps, are included under the definition.
    - Service providers that access unsecured PHR identifiable health information in the course of providing services are not considered a PHR related entity.

- Finalizes the requirement that "vendors of PHRs or PHR related entities that discover a breach of security must provide written notice at the last known contact information of the individual."

- Written notices may be sent by electronic mail, if the impacted individual has specified electronic mail as their primary contact method or by first-class mail. Electronic mail is defined as email, in combination with one or more of the following: text message, within-app messaging, or electronic banner."

- Updates requirements to the content notice in the event of a breach include:
    - The full name, website, and contact information of any third parties that acquired unsecured PHR identifiable health information.
    - A description of the types of unsecured PHR identifiable health information that were involved in the breach, including data such as health diagnosis or condition, lab results, medications, other treatment information, the individual's use of a health-related mobile app, and device ID.
    - Requires the notice to include a brief description of what the entity is doing to protect impacted individuals, such as credit monitoring.
    - A toll-free phone number, email address, website, within-app contact option or postal address for individuals to contact the impacted entity.

- Revises requirements for the time of notice for breaches involving 500 or more individuals to notify impact parties when they notify the FTC.

If you have additional questions on the contents of this final rule or would like to discuss this FAQ further, please contact advocacy@ahima.org.