akerman

Blog Post

Health Apps Beware: FTC Clarifies Health Breach Notification Rule with Significant Proposed Changes

June 9, 2023

By Jordan T. Cohen and Elizabeth F. Hodge

Direct-to-consumer health and wellness applications are forewarned: the Federal Trade Commission (FTC) is proposing changes to the Health Breach Notification Rule (HBNR), 16 C.F.R. part 318, that, if finalized, would cement the HBNR's applicability to a broad swath of direct-to-consumer health and wellness applications (apps) and confirm that a breach of security includes not only data security incidents, but also unauthorized disclosures of personal health information. The FTC issued the Notice of Proposed Rulemaking on May 18, 2023, and comments are due 60 days after publication in the Federal Register. We have prepared a comparison document illustrating the proposed changes, which can be found here.

Background

The HBNR was first implemented in 2009 in response to the anticipated proliferation of online personal health record (PHR) services — many of which are now defunct (e.g., Microsoft HealthVault) — that offered to store a user's digital medical records. Since such services are not typically covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its breach reporting obligations, the HBNR was meant to fill this void. Fast forward nearly 15 years and the FTC is

Related People

Jordan T. Cohen
Elizabeth F. Hodge

Related Work

Data Privacy and Security
Healthcare
Pharmacy, Drugs, and Medical Devices

Related Offices

New York
Tampa
West Palm Beach

Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

Read blog posts

demonstrating a renewed commitment to protecting consumers' digital health information, as illustrated by the enforcement actions against GoodRx, BetterHelp, and Easy Healthcare for impermissibly sharing consumer health information to assist with advertising and marketing practices. But the agency has struggled to apply the HBNR to newer digital health platforms that are often used on smart phones and utilize technologies, including sophisticated user tracking, that did not exist in 2009. 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, but many observers noted the agency's strained interpretation of the original rule. The agency's current proposal may have been, in part, a response to such feedback.

Overview of the Proposed Rule

Below is a summary of the FTC's central proposals, some of which, if finalized, may be challenged for exceeding the agency's statutory authority:

- **Clarifying Who Is Subject to the HBNR**

The FTC intends to clarify and, arguably, expand the types of actors subject to the HBNR by defining "health care provider" and "health care services or supplies."

The FTC proposes to define "health care provider" to include not only providers of medical services or other health services under the Medicare statute, but also "any other entity furnishing health care services or supplies."

The agency also proposes to define "health care services or supplies" to include any online service, such as a website, mobile app, or Internet-connected device, that provides mechanisms to track, for example, diseases, health conditions, diagnoses, treatments, medications, symptoms, fitness, fertility, or sleep.

This definitional framework would sidestep the messiness of trying to shoehorn app developers into HIPAA's healthcare provider definition, and the combination of the above definitions, if finalized, could implicate a large portion of the mobile app market.

- **Clarifying the Information that is Protected by the HBNR**

The FTC also proposes to redefine "PHR identifiable health information." The proposed rule would remove the current definition's cross-reference to HIPAA's definition of "individually identifiable health information" and add two additional elements (c. and d. in the list below). As revised, "PHR identifiable health information" would be defined to include information:

a. that is provided by or on behalf of the individual;
b. 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;
c. that 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
d. is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse.

This revised definition would capture a broad swath of information. By referencing "health care provider" in the fourth element, the FTC expands the applicability by including anyone offering "health care services or supplies," so that the HBNR would more clearly apply to consumer-facing health apps that are not otherwise regulated by HIPAA.

The FTC confirms its goal of broadening the definition to capture more information in the

commentary to the proposed rule, where it states its belief that the definition:

> "... covers traditional health information (such as diagnoses or medications), health information derived from consumers' interactions with apps and other online services (such as health information generated from tracking technologies employed on websites or mobile applications or from customized records of website or mobile application interactions), as well as emergent health data (such as health information inferred from non-health-related data points, such as location and recent purchases). (citations omitted)."

- **Revised Definition of "Breach of Security"**

The FTC proposes to revise the definition of "breach of security" to clarify that breaches include unauthorized disclosures of PHR identifiable health information and not just security intrusions in the traditional sense. This definition would more clearly capture instances where PHR vendors and other entities subject to the HBNR impermissibly disclose PHR identifiable health information to third parties for advertising or other purposes.

- **Revised Definition of "PHR related entity"**

The FTC proposes to clarify that the definition of a "PHR related entity" includes entities that offer products or services not only through the website of a PHR vendor, but also through any online services, including mobile applications, of a PHR vendor. The FTC also proposes to limit the scope of the third prong of the definition of "PHR related entity" to entities that access or send *unsecured PHR identifiable health information* to a PHR, rather than entities that access or send any other type of information to a PHR.

- **Clarifying What It Means to "Draw Information from Multiple Sources"**

The FTC proposes revising the definition of "PHR" to clarify what it means to draw PHR identifiable health information from multiple sources. Under the revised definition, a PHR would need only have the "technical capacity" to draw information from multiple sources. This revision is intended to include products that can draw information from more than one source even where the end user elects to limit information from a single source, such as an app that accepts user-inputted health information (e.g., name, weight, height, age) and has the technical capacity to sync with a wearable monitor, even if some users chose not to sync the app with the monitor. The agency also believes that the added language would more clearly capture products that have the ability to draw *any* information from multiple sources, even if it only draws *health* information from one source.

- **Modernizing the Method for Breach Notification**

The FTC proposes to modernize the method of notice (currently limited to mail or email in some circumstances). The proposal would authorize electronic notice under additional circumstances by adding a definition for the term "electronic mail," which it proposes to define as email in combination with one or more of the following: text message, within-application messaging, or electronic banner. This proposed amendment would allow vendors of PHRs, or PHR related entities that discover a breach, to provide notice of the breach by electronic mail if the individual has specified electronic mail as the primary contact method.

Further, to assist with providing notice, the FTC has prepared a model notice that entities may use.

- **Expanding the Content of Breach Notices**

The proposed revisions would also expand the required content of the notice to individuals. The proposal would require additional information, such as: (a) a description of the potential harm that may

result from the breach, such as medical or other identity theft; (b) a description of what the notifying entity is doing to protect affected individuals, such as offering credit monitoring or other services; (c) the full name, website, and contact information for any third parties that acquired unsecured PHR identifiable health information; (d) a description of the types of unsecured PHR identifiable health information that were involved in the breach; and (e) additional means for the affected individual to contact the notifying entity, including two or more of the following: toll-free telephone number, email address, website, within-application mechanism, or postal address.

- **Improving the Readability of the Rule**

The FTC proposes to improve the clarity of the HBNR by including explanatory parentheticals for cross references and statutory citations in relevant locations, consolidating notice and timing requirements in single sections, and adding a new section that plainly states the penalties for non-compliance.

- **Changes Considered But Not Proposed**

The FTC also seeks comments on revisions that it considered but did not propose, such as defining "authorization" and "affirmative express consent," modifying the definition of "third party service provider," and altering notification timing requirements.

Response to the Proposed Revisions

The FTC's proposal demonstrates that it is staking an aggressive position on its authority to fill a burgeoning gap in the protection of non-HIPAA regulated digital health information. Questions have already been raised about whether some of the proposed amendments might exceed the FTC's statutory authority by, for example, applying the HBNR to data held by health and wellness

applications. Though the FTC could roll back or revise certain proposed amendments in response to comments or threatened challenges, app developers should at least consider the steps needed to comply with the proposed rule should it be finalized. These changes could include rebuilding certain app or website functionality to comply with the revised breach notification requirements. Even if the proposal is not finalized in its current form, developers should prepare to create or revise their internal policies and procedures to address their breach notification obligations.

Akerman's Health Law Rx blog will continue to monitor the progress of this proposed rule and the FTC's enforcement activities related to the privacy of personal health information.
