COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 7. July 11, 2024 Final FTC Health Breach Notification Rule Indicates Agency Focus on Data Privacy

By Jane Anderson

Digital health entities offering personal health records (PHR) and other health apps will need to closely examine their privacy practices and potentially update their consent policies to comply with the final health breach notification rule released by the Federal Trade Commission (FTC).

The rule—finalized April 26 by the commission—is the first update to the Health Breach Notification Rule (HBNR), which took effect in 2009.[1] The updated rule clarifies the rule's applicability to health apps and other similar technologies, and also expands the information that entities covered by the rule must provide to consumers when notifying them of a breach of their health data, according to the FTC.

The FTC rule requires PHR vendors and related entities that are not covered by 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 notify PHR vendors after discovering a breach at the third party.

"HIPAA…HHS' Health Insurance Portability and Accountability Act – addresses privacy and security for most doctors' offices, hospitals, and insurance companies. But with advances in monitoring and technology, a lot of health-related information doesn't fall within HIPAA. That's where the FTC's Health Breach Notification Rule comes in," the FTC wrote in its Business Blog.[2]

Rule Incorporates Changes

Protecting the privacy and security of personal health data is a high priority for the FTC, which has brought multiple cases in the past several years, including two enforcement actions that alleged violations of the HBNR—against GoodRx[3] and Easy Healthcare Corp. (publisher of the Premom app). The commission announced its proposed changes to the breach notification rule in May 2023 and sought comments on those changes.[4]

"Until companies keep health data secure and private, we'll continue to update and enforce the Health Breach Notification Rule to protect consumers and keep up with the digital revolution in health information," according to FTC's Business Blog.

The FTC "received approximately 120 comments" from a broad range of individuals and stakeholders, the commission said.

The rule incorporates numerous changes, including:

- **Revising definitions**: The commission revised several definitions to underscore the final rule's application to health apps and similar technologies not covered by HIPAA. This includes modifying the definition of "PHR identifiable health information" and adding two new definitions for "covered health care provider" and "health care services or supplies."
- **Clarifying breach of security**: The rule clarifies that a "breach of security" includes the unauthorized

acquisition of identifiable health information that occurs due to a data security breach or an unauthorized disclosure.

- **Revising the definition of "PHR related entity"**: The definition of PHR related entity has been revised in two ways that pertain to the rule's scope. The revised definition makes clear that the rule "covers entities that offer products and services through the online services, including mobile applications, of vendors of personal health records." It also makes clear 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—qualify as PHR-related entities.
- **Expanding use of electronic notification**: The rule authorizes the "expanded use of email and other electronic means of providing clear and effective notice of a breach to consumers."
- **Expanding consumer notice content**: The rule expands the required content that must be provided in the notice to consumers. For example, the notice would be required to include the name or identity (or, where providing the full name or identity would pose a risk to individuals or the entity providing notice, a description) of any third parties that acquired unsecured PHR identifiable health information as a result of a breach of security.
- **Changing timing requirement**: The rule modifies when the FTC must be notified under the rule. For breaches involving 500 or more individuals, covered entities (CEs) must notify the FTC at the same time they send notices to affected individuals, which must occur "without unreasonable delay and in no case later than 60 calendar days" after the discovery of a breach of security.
- **Expanding penalties for noncompliance**: The rule makes clear that a violation of the HBNR will be treated as "a violation of a rule promulgated under section 18 of the FTC Act" regarding unfair or deceptive acts or practices, meaning violators are subject to civil penalties.
- **Improving readability**: The rule also includes changes to improve the rule's readability and promote compliance.

The FTC voted 3-2 to approve the rule.