COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 10. October 05, 2023 Some Praise FTC Health Breach Rule Update, While Others Accuse Agency of Overreach

By Jane Anderson

Some organizations praised the Federal Trade Commission's (FTC) proposed changes to its Health Breach Notification Rule (HBNR),[1] saying the update will protect consumer data within health apps that HIPAA does not cover. But other stakeholders said they believe the FTC has gone too far in revising its 14-year-old rule, potentially overstepping its authority.

The 117 comments on the FTC's proposed amendments run the gamut from enthusiastic backing of the proposal to concerns about the FTC getting too far ahead of Congress regarding data privacy. In addition, some comments asked for additional information on what specific forms of "health data" would be covered if the rule is finalized.

The FTC unveiled the proposed amendments in May; the announcement came as the agency announced its third and fourth enforcement actions under the HBNR in four months.[2] Samuel Levine, director of the FTC's Bureau of Consumer Protection, said the proposed amendments to the HBNR will allow it to keep up with marketplace trends and respond to developments in technology in the wake of "an explosion of health apps and connected devices, many of which aren't covered by HIPAA, collecting vast amounts of sensitive consumer health information."

The agency proposed several changes to the HBNR:

- It would revise several definitions to clarify the rule's application to health apps and similar technologies not covered by HIPAA. This includes modifying the definition of "PHR [personal health record] identifiable health information" and adding two definitions for "health care provider" and "health care services or supplies."
- It would clarify that a "breach of security" under the rule includes an unauthorized acquisition of identifiable health information that occurs due to a data security breach or an unauthorized disclosure.
- It would revise the definition of "PHR-related entity" in two ways that pertain to the rule's scope. For example, it makes clear that only entities that access or send unsecured PHR identifiable health information to a PHR—rather than entities that access or send any information to a PHR—qualify as PHR-related entities.
- It would clarify what it means for a PHR to draw PHR identifiable health information from multiple sources.
- It would authorize the expanded use of email and other electronic means to provide consumers with clear and effective notices of a breach.
- It would expand the required content that should be provided in the notice to consumers. For example, the notice would be required to include information about the potential harm stemming from the breach and the names of any third parties who might have acquired any unsecured personally identifiable health

information.

- It would make changes to improve the rule's readability and promote compliance.