COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 7. July 13, 2023
FTC Wants to Update Its Health Breach Rule to Cover Health Apps

By Jane Anderson

The Federal Trade Commission (FTC) is proposing changes to its 14-year-old Health Breach Notification Rule (HBNR), clarifying that it applies to health apps and other similar technologies. The proposed amendments came as the FTC announced its third and fourth enforcement actions in four months.

"We are witnessing an explosion of health apps and connected devices, many of which aren't covered by HIPAA, collecting vast amounts of sensitive consumer health information," Samuel Levine, director of the FTC's Bureau of Consumer Protection, said in announcing the changes. "The proposed amendments to the rule will allow it to keep up with marketplace trends, and respond to developments and changes in technology."[1]

The FTC's health care breach notification rule, finalized in 2009, requires vendors of personal health records (PHRs) and related entities 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 vendors working with those health record vendors to notify them following the discovery of a breach.

Comments are due Aug. 8 on the FTC's notice of proposed rulemaking, which was published in the *Federal Register* on June 9.[2]

FTC Moves Aggressively

Protecting the privacy and security of personal health data is a high priority for the FTC, which has brought four cases so far this year, including enforcement actions that alleged violations of the HBNR.

In 2020, in what it termed "part of a regular review of commission rules," the FTC sought comment on whether changes were needed to the HBNR. Then, 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 rule.

After reviewing the public comments, the FTC has 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 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.

The commission voted 3-0 to publish the proposed HBNR in the *Federal Register*. The public has 60 days to comment.