wiley

ALERT

FTC Issues Policy Statement on Privacy Breaches by Connected Health Apps and Signals Greater Enforcement

September 16, 2021

In a 3-2 vote, the Federal Trade Commission (FTC) adopted a Policy Statement emphasizing that vendors who operate health apps and other connected devices that collect or use consumers' health information must comply with the Health Breach Notification Rule (HBNR). In its statement, the FTC noted that its "Health Breach Notification Rule helps to ensure that entities who are not covered by the Health Insurance Portability and Accountability Act (HIPAA) nevertheless face accountability when consumers' sensitive health information is compromised." Not only does the Policy Statement signal the FTC's commitment to use additional enforcement tools when consumers' sensitive health information is at issue, it also expresses the FTC's intent to use the HBNR against vendors of personal health records and related entities in instances where consumers' health information has been compromised.

Among other things, the Policy Statement provides more guidance on which health-related apps are subject by the Rule, noting that the FTC "considers apps covered by the Rule if they are capable of drawing information from multiple sources, such as through a combination of consumer inputs and application programming interfaces." The Statement also notes that, under the Commission's interpretation, a "breach" is not just a cybersecurity intrusion, but also "unauthorized access, including sharing of covered information without an individual's authorization." The Statement concludes by noting that the "Commission intends to bring actions to enforce the Rule consistent with this Policy Statement."

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Tawanna D. Lee
Consulting Counsel
202.719.4574
tdlee@wiley.law

Practice Areas

Digital Health
Health Care
Privacy, Cyber & Data Governance

Commissioners Christine Wilson and Noah Phillips dissented from issuing the Statement. While both Commissioners stressed during the hearing that they also have a desire to protect sensitive health information, they took issue with the majority's process. Both orally at the hearing and in written dissents, they expressed concern with what, in their view, represents unilateral action to expand the FTC's authority contrary to existing guidance, arguing that the FTC's interpretation end runs ongoing rulemaking processes and should have been made in coordination with other agencies, the Social Security Administration and Health and Human Services, which have overlapping or related enforcement authority.

The FTC has never brought a public enforcement action enforcing the HBNR, but Commissioners Rebecca Slaughter and Rohit Chopra have identified enforcement as a priority. In the context of the Flo Health settlement earlier this year, in a joint statement, Commissioners Slaughter and Chopra argued that a HBNR count should have been included, emphasizing that the FTC expects that companies handling sensitive health information will prioritize privacy and security and arguing that with respect to the HBNR, "[w]here Congress has given us rulemaking authority, we should use it."

The HBNR, which applies to vendors of personal health records and related entities not covered by HIPAA, requires notice to individuals, FTC, and, in some cases, the media, if there has been an unauthorized disclosure of health information. If more than 500 individuals are affected by a breach, for example, entities must notify the FTC within 10 business days. The FTC can assess civil penalties of up to $43,792 per violation.

The Wiley Privacy, Cyber & Data Governance team advises clients on privacy, cybersecurity, and FTC regulations across industries, including in the area of health applications. Please reach out to the authors with any questions.