wiley

NEWSLETTER

FTC Policy Statement Signals Increasing Scrutiny on the Protection of Sensitive Personal Health Information

September 2021

Privacy In Focus®

The billion-dollar connected health and wellness device market has shown no signs of slowing as Americans have widely and rapidly adopted consumer-directed health care apps and devices to monitor their wellness, in place of and in combination with in-person visits to a doctor's office. As the growth of the health Internet of Things (IoT) market continues to rise, operators of health care and wellness apps and devices must give careful consideration to their privacy obligations with respect to sensitive health information collected from consumer-directed health care apps and devices.

Many health apps are not required to be compliant with the privacy and security requirements pursuant to the federal Health Insurance Portability and Accountability Act (HIPAA), because many medical app developers are not "covered entities" or "business associates," as defined under HIPAA. The U.S. Department of Health & Human Services (HHS) Office for Civil Rights, which enforces HIPAA, issued frequently asked questions (FAQs) addressing the applicability of HIPAA to health-related apps. HHS FAQ 572 explains that HIPAA is limited to instances where the app is provided by or on behalf of a "covered entity" in connection with the provision of medical services. Non-HIPAA consumer-directed health care apps and devices may be subject nonetheless to the Federal Trade Commission's (FTC) Health Breach Notification Rule (HBNR), 16 C.F.R. §§ 318.1-318.9, which applies to vendors of personal health records and related entities not covered by HIPAA.

Authors

Antonio J. Reynolds
Partner
202.719.4603
areynolds@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Tawanna D. Lee
Associate
202.719.4574
tdlee@wiley.law

Practice Areas

Digital Health
FTC Regulation
Health Care
Privacy, Cyber & Data Governance

The Health Breach Notification Gains Renewed Attention

In 2009, Congress passed the American Recovery and Reinvestment Act, which contained provisions directing the regulation of electronic protected health information, not only under HIPAA, but also addressed electronic health records maintained for individuals by vendors that are not regulated under HIPAA. Specifically, Congress directed the FTC to promulgate regulations requiring that such vendors notify affected individuals, the FTC, and, in some cases, the media if there has been an unauthorized disclosure of health information. Those regulations, the HBNR, became effective in September 2009.

The HBNR gained traction earlier this year with the FTC settlement with Flo Health, Inc., over claims that the company disclosed consumers' personal health information to third parties without consent. Notably, the FTC did not include alleged violations of the HBNR among its claims, drawing the attention of federal enforcers and lawmakers. In a joint statement concurring in part and dissenting in part, Commissioners Rebecca Slaughter and Rohit Chopra expressed their disappointment that "the Commission is not using all of its tools to hold accountable those who abuse and misuse personal data. We believe that Flo's conduct violated the Health Breach Notification Rule, yet the Commission's proposed complaint fails to include this allegation. The rule helps ensure that consumers are informed when their data is misused, and firms like Flo should not be ignoring it."

Lawmakers also called for the FTC to exercise its authority under the Health Breach Notification Rule. In a letter to then Acting FTC Chairwoman Slaughter, members of Congress urged the FTC to take enforcement actions against companies that fail to notify consumers about unauthorized uses and disclosures of personal health information, specifically calling attention to the FTC's high-profile investigations into the handling of sensitive health information by menstruation tracking mobile app providers – and the enforcement agency's failure to bring a claim under the HBNR. "Stronger [Health Breach Notification Rule] enforcement would be especially impactful in the case of period-tracking apps, which manage data that is both deeply personal and highly valuable to advertisers. Looking ahead, we encourage you to use all of the tools at your disposal, including the Health Breach Notification Rule, to protect women and all menstruating people from mobile apps that exploit their personal data."

The FTC Is Poised to Bring Enforcement Action Under the Health Breach Notification Rule

On September 16, 2021, the FTC issued a Policy Statement affirming that connected device and health app companies that collect user health data must comply with the HBNR. In its statement, the FTC noted that "[a]s many Americans turn to apps and other technologies to track diseases, diagnoses, treatment, medications, fitness, fertility, sleep, mental health, diet, and other vital areas, this Rule is more important than ever."

Who Is Covered Under the HBNR?

The HBNR applies to:

- A **vendor of personal health records (PHRs)**, an entity that "offers or maintains a personal health record" – defined as an electronic record of "identifiable health information on an individual that can

be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."

- A **PHR-related entity**, an entity that interacts with a vendor of personal health records either by offering products or services through the vendor's website – even if the site is covered by HIPAA – or by accessing information in a personal health record or sending information to a personal health record. The FTC guidance makes clear that many businesses that offer web-based apps for health information fall into this category. The Policy Statement provides further guidance 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."
- A **third-party service provider** for a vendor of PHRs or a PHR-related entity, an entity that offers services involving the use, maintenance, disclosure, or disposal of health information to vendors of personal health records or PHR-related entities.

What Triggers the Notification Requirement?

The HBNR requires that "following the discovery of a breach of security of unsecured PHR identifiable health information that is in a personal health record," entities subject to the HBNR provide notice to "each individual who is a citizen or resident of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of such a breach of security" and the FTC. The Policy Statement explains that a "breach" is not just a cybersecurity intrusion, but also "unauthorized access, including sharing of covered information without an individual's authorization."

How Is the HBNR Enforced?

FTC enforcement of the HBNR began on February 22, 2010. The FTC has the authority to assess civil penalties, as high as $43,792 per violation – each day that the notifications have not been issued. To date, the FTC has not brought a public enforcement action under the HBNR and it has received notice of only four breaches involving 500 or more individuals. The September 16 Policy Statement sends a clear signal that the "Commission intends to bring actions to enforce the Rule consistent with this Policy Statement." Companies should carefully review their obligations under the HBNR to protect user data.