UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

STATEMENT OF THE COMMISSION
On Breaches by Health Apps and Other Connected Devices

September 15, 2021

In recognition of the proliferation of apps and connected devices that capture sensitive health data, the Federal Trade Commission is providing this Policy Statement to offer guidance on the scope of the FTC's Health Breach Notification Rule, 16 C.F.R. Part 318 ("the Rule").[1]

The FTC's 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. Under the Rule's requirements, vendors of personal health records ("PHR") and PHR-related entities must notify U.S. consumers and the FTC, and, in some cases, the media, if there has been a breach of unsecured identifiable health information, or face civil penalties for violations. The Rule also covers service providers to these entities. In practical terms, this means that entities covered by the Rule who have experienced breaches cannot conceal this fact from those who have entrusted them with sensitive health information.

The Rule was issued more than a decade ago, but the explosion in health apps and connected devices makes its requirements with respect to them more important than ever. The FTC has advised mobile health apps to examine their obligations under the Rule,[2] including through the use of an interactive tool.[3] Yet the FTC has never enforced the Rule, and many appear to misunderstand its requirements. This Policy Statement serves to clarify the scope of the Rule, and place entities on notice of their ongoing obligation to come clean about breaches.

The Rule covers vendors of personal health records that contain individually identifiable health information created or received by health care providers. The Rule is triggered when such entities experience a "breach of security."[4] Under the definitions cross-referenced by the Rule, the developer of a health app or connected device is a "health care provider" because it "furnish[es] health care services or supplies."[5] When a health app, for example, discloses

[1] The Rule implements the requirements of the American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115, codified at 42 U.S.C. § 17937.
[2] *Mobile Health App Developers: FTC Best Practices*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices (last visited on Sept. 15, 2021).
[3] *Mobile Health Apps Interactive Tool*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool (last visited on Sept. 15, 2021).
[4] *See* 16 C.F.R. § 318.2(a)
[5] *See id.* § 318.2; 42 U.S.C. § 1320d(6), d(3).

sensitive health information without users' authorization, this is a "breach of security" under the Rule.[6]

The statute directing the FTC to promulgate the Rule requires that a "personal health record" be an electronic record that can be drawn from multiple sources. The Commission 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 ("APIs"). For example, an app is covered if it collects information directly from consumers and has the technical capacity to draw information through an API that enables syncing with a consumer's fitness tracker. Similarly, an app that draws information from multiple sources is covered, even if the health information comes from only one source. For example, if a blood sugar monitoring app draws health information only from one source (e.g., a consumer's inputted blood sugar levels), but also takes non-health information from another source (e.g., dates from your phone's calendar), it is covered under the Rule.

In addition, the Commission reminds entities offering services covered by the Rule that a "breach" is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, including sharing of covered information without an individual's authorization, triggers notification obligations under the Rule.

As 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. Firms offering these services should take appropriate care to secure and protect consumer data. The Commission intends to bring actions to enforce the Rule consistent with this Policy Statement. Violations of the Rule face civil penalties of $43,792 per violation per day.

---

[6] *Id*. § 318.2(a) (defining "breach of security" as "acquisition of [PHR identifiable health information] without the authorization of the individual.").