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

Office of the Chair

Remarks by Chair Lina M. Khan on the
Health Breach Notification Rule Policy Statement
Commission File No. P205405

September 15, 2021

The global pandemic has hastened the adoption of virtual health assistants, with Americans placing their trust in various technologies to track and manage their personal health. As we have seen, however, digital apps are routinely caught playing fast and loose with user data, leaving users' sensitive health information susceptible to hacks and breaches. Given the rising prevalence of these practices, it is critical that the FTC use its full set of tools to protect Americans.

In 2009, Congress instructed the FTC to issue a rule protecting the public from breaches of personal health data. This Health Breach Notification Rule is among a small set of privacy laws covering users' health information, and it requires vendors of unsecured identifying health information to notify users, the FTC, and, in some cases, the media if there is an unauthorized disclosure.[1] Although the Rule was first issued over a decade ago, the Commission has not brought any enforcement actions under it.

While users have been adopting health apps at a rapid rate,[2] the commercial owners of these apps too often fail to invest in adequate privacy and data security, leaving users exposed. For example, one recent peer-reviewed study found that these health apps suffer from "serious problems," ranging from insecure transmission of user data (including geolocation) to unauthorized dissemination of data to advertisers and other third parties in violation of the apps' own privacy policies.[3] In my view, these problems stem in part from a gap: health apps are

---

[1] 85 Fed. Reg. 31,085, 31,087 (codified at 16 C.F.R. pt. 318) ("the Rule"). The Rule implements the requirements of the American Recovery & Reinvestment Act of 2009, 42 U.S.C. §§ 17937, 17953.

[2] See, e.g., Elad Natanson, *Healthcare Apps: A Boon, Today and Tomorrow*, FORBES (July 21, 2020), https://www.forbes.com/sites/eladnatanson/2020/07/21/healthcare-apps-a-boon-today-and-tomorrow/?sh=21df01ac1bb9; Emily Olsen, *Digital health apps balloon to more than 350,000 available on the market, according to IQVIA report*, MOBIHEALTHNEWS (Aug. 4, 2021), https://www.mobihealthnews.com/news/digital-health-apps-balloon-more-350000-available-market-according-iqvia-report; Lis Evenstad, *Covid-19 has led to a 25% increase in health app downloads, research shows*, COMPUTERWEEKLY (Jan. 12, 2021), https://www.computerweekly.com/news/252494669/Covid-19-has-led-to-a-25-increase-in-health-app-downloads-research-shows (finding that COVID-19 has led to a 25% increase in health app downloads and that of the 350,000 health apps available on the market, 90,000 of which were introduced in 2020 alone, an average of 250 per day); *Digital Health Habits in the UK: a Quin nationwide survey*, QUIN (Oct. 2, 2020), https://quintech.io/what-do-the-uk-public-think-about-health-apps/ (finding that usage of health apps has increased by 37% in the U.K. since the start of the pandemic).

[3] Gioacchino Tangari et al., *Mobile health and privacy: cross sectional study*, 373 BRITISH MED. J. 1, 11 (June 17, 2021), https://www.bmj.com/content/373/bmj.n1248.

generally not covered by HIPAA, and some may mistakenly believe that they are not covered by the Commission's Rule.

Today we are clarifying that the Health Breach Notification Rule applies to connected health apps and similar technologies. Notably, the Rule does not just apply to cybersecurity intrusions or other nefarious behavior; incidents of unauthorized access also trigger notification obligations under the Rule. It is particularly important to note that the Rule extends to evolving technologies, an interpretation that is a logical reading of its language. Contrary to my dissenting colleagues' suggestion, today's statement is entirely consistent with—and, in fact, serves to clarify—the FTC's earlier guidance.[4] Consistent with that guidance, health apps that are capable only of collecting data from users directly—in other words, apps that are *not* capable of drawing data from multiple sources—are not covered by the Rule. I will also note that there is no notice of proposed rulemaking pending on this Rule. We have solicited comments as part of our general periodic review and have reviewed those comments as part of our analysis here.

The Commission will enforce this Rule with vigor. Violations of the Rule carry civil penalties of $43,792 per violation per day, and the Commission should not hesitate to seek significant penalties against developers of health apps and other technologies that ignore its requirements.

Lastly, I believe our efforts to protect Americans from abusive data practices must extend beyond this Rule. While this Rule imposes some measure of accountability on tech firms that abuse our personal information, a more fundamental problem is the commodification of sensitive health information, where companies can use this data to feed behavioral ads or power user analytics. Given the growing prevalence of surveillance-based advertising, the Commission should be scrutinizing what data is being collected in the first place and whether particular types of business models create incentives that necessarily place users at risk.

In the meantime, it is vital that the Commission use the full suite of its authorities to protect Americans from abusive data practices. Today's action will be a step in the right direction.

***

[4] The dissenters point to existing guidance about the term "Personal Health Record related entity," but the Policy Statement issued today addresses an entirely different set of entities covered by the Rule—vendors of personal health records.