CARLTON FIELDS

4 Tips for Health Tech Apps After the FTC's Revised Breach Notification Rule

May 16, 2024

On April 26, the Federal Trade Commission announced its final rule updating the health breach notification rule. According to the FTC, the update seeks to "clarify" the scope of the rule by adding new definitions and revising certain breach notification requirements. Under the health breach notification rule, vendors of personal health records are required to notify individuals, the FTC, and, in some cases, the media of a breach of unsecured protected health information. The FTC's updates to the rule codify the commission's 2021 policy statement, which explained that health app and connected device developers are vendors of personal health records covered by the health breach notification rule. **Key Definitional Changes** Among other definitional changes, the final rule added a definition of "health care services or supplies." Under the final rule, "health care services or supplies" includes "any online service such as a website, mobile application, or internet-connected device that provides mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet, or that provides other health-related services or tools." According to the FTC, these changes to the rule definitions clarify that developers of health apps and similar technologies providing "health care services or supplies" qualify as covered "health care providers" under the health breach notification rule. The FTC also expanded the definition of a "personal health record." Under the previous rule, a personal health record was, in part, "an electronic record that can be drawn from multiple sources." This definition was expanded under the final rule to electronic records that have "the *technical capacity* to draw information from multiple sources." According to the FTC, this clarifies that an app that has the mere capability of drawing information from multiple sources (e.g., from the consumer itself and via application programming interfaces to other applications) is a personal health record even if the consumer does not opt into the features that would draw information from these other sources (e.g., API driven features). The final rule also changed the definition of "breach of security." Under the final rule, a breach of security includes "an unauthorized acquisition of unsecured PHR identifiable health information in a personal health record that occurs as a result of a data breach *or an unauthorized disclosure*." According to the FTC,

this change was meant to clarify that even the intentional disclosure of identifiable health information by a vendor of personal health records or personal health record-related entity to a third party is a "breach of security" if such disclosure is not authorized by the consumer. Notably, the FTC decided not to define "authorization" under the rule, stating instead that "whether a disclosure is authorized ... is a fact-specific inquiry." This emphasizes the FTC's stress on obtaining valid consent prior to disclosing health-related data to third parties (e.g., adtech vendors). **Context** These changes to the health breach notification rule come less than a year after the FTC took several enforcement actions related to the use of tracking technologies by mobile health apps and health care websites. In May 2023, the commission extracted a $1.5 million settlement from GoodRx for its use of tracking technologies on its mobile app. The commission charged GoodRx with violating the health breach notification rule because its services sent covered health information to advertising companies without authorization and failed to provide the required notifications to individuals, the FTC, and media outlets. Later in 2023, the FTC sent letters to 130 hospital systems and telehealth providers warning that their use of similar tracking technologies without an individual's authorization may violate the FTC Act and constitute a breach of security under the health breach notification rule. **Recommendations for Reducing Risk** While the health care privacy landscape continues to shift, health care organizations can consider the following steps to mitigate their risk:

- Map and monitor data flows of health information to third parties, including via technologies integrated into their website or app.
- Analyze and configure user interfaces and consent dialogues to obtain valid consent and avoid "dark patterns."
- Contractually limit how vendors who handle covered health information can use data.
- Ensure incident response plans align with the FTC's latest notification and reporting requirements.

Authored By

Patricia M. Carreiro

Michael A. Bailey

Related Practices

Cybersecurity and Privacy
Health Care
Technology

Related Industries

Health Care
Technology