BURR FORMAN LLP

# FTC Accelerates Enforcement Actions to Protect Consumer Digital Health Information

Articles / Publications
*Reprinted with permission from Birmingham Medical News*
09.15.2023

The Federal Trade Commission (FTC) has been aggressively pursuing enforcement actions that involve companies using applications that share consumer personal health information with third parties in violation of the Health Breach Notification Rule.

**What is the Health Breach Notification Rule?**

The Health Breach Notification Rule (HBNR) was issued more than a decade ago to ensure even HIPAA-exempt entities that maintain personal health records notify affected consumers following a breach involving unsecured information. The HBNR applies to (1) vendors of personal health records (PHR), (2) PHR-related entities, and (3) third-party service providers for vendors of PHRs or PHR-related entities. A PHR vendor is a business that offers or maintains PHRs. A common FTC example of a PHR vendor is a health app that collects information from consumers and has the ability to sync with a consumer's fitness tracker. PHR-related entities sell products or services through the vendor's website, such as a company that operates a fitness tracker and relays information to health apps. A third-party servicer uses, maintains, discloses, or disposes of health information to vendors or related entities.

If a breach occurs, a business must provide notice to: (1) each affected person who is a citizen of the United States; (2) the FTC using a Notice of Breach of Health Information form found on the FTC website; and (3) in some cases, the media. Provisions include specific time frames when notice must be issued based on the date of discovery of the breach, which may be as short as 10 business days.

RELATED PROFESSIONALS

Robin Beardsley Mark

RELATED CAPABILITIES

Health Care

# FTC Accelerates Enforcement Actions to Protect Consumer Digital Health Information

**FTC Escalates HBNR Enforcement**

The HBNR was dormant for years. However, the upsurge in health apps and digital health companies led the FTC in October 2021 to issue a policy statement warning health apps and connected device companies that collect health information to comply with the HBNR. The FTC issued its first enforcement action in February 2023 by imposing a significant $1.5 million civil penalty on telehealth company Good Rx for its failure to notify consumers and others of the unauthorized disclosure of personal health information to third party advertising companies and advertising platforms, such as Facebook, Google and other companies.

Even more recently in May 2023, the FTC settled with Illinois-based Easy Healthcare Corporation in an action related to its fertility-tracking app known as Premom. Easy Healthcare developed, advertised, and distributed a mobile application called Premom Ovulation Tracker that allows users to input and track personal health information.

FTC's complaint alleged that Easy Healthcare deceived users by disclosing sensitive health data to third parties without notifying consumers of these unauthorized disclosures. The FTC alleged that Easy Healthcare promised Premom users in its privacy policies that: (1) it would not share health information with third parties without users' knowledge or consent, (2) that the shared information would not be identifiable data since only users' IP addresses were given, and (3) information would only be used for the companies' own analytics or advertising.

The FTC further alleged that Easy Healthcare failed to take reasonable steps to address the privacy and security risks created by using software development kits ("SDKs") that shared consumers' health information with third parties. In reality, the SDKs allowed Easy Healthcare to track and analyze Premom users' interactions with the app and to transfer the data, including information about users' fertility and pregnancies, to the publisher of each SDK. The FTC concluded this violated the unfairness and deception prongs of Section 5 of the FTC Act and the HBNR.

In both the Good Rx and the Easy Healthcare enforcement actions, the FTC alleged that the companies shared sensitive health data for advertising purposes in violation of promises they would not do so. In addition to significant civil monetary penalties, both companies are required to alert their customers to the unauthorized disclosures and to comply with extensive remedial obligations and restrictions.

**FTC Proposes HBNR Rule Changes**

On June 9, 2023, the FTC published a Notice of Proposed Rulemaking in the Federal Register that would revise the HBNR to clarify its application to health apps and other similar technology. The FTC proposed introducing a broader definition of covered entities and an expansion of the types of activities that trigger the rule's notification obligations. Specifically, the proposed changes would add "health care provider" and "health care services or supplies" to the definition of "PHR identifiable information." The proposed changes would also expand the use of email for providing breach notices to consumers. If these changes are

# FTC Accelerates Enforcement Actions to Protect Consumer Digital Health Information

approved, health tech companies must evaluate how best to comply with the revamped HBNR. Regardless, the FTC is expected to continue enforcing the rule and looking out for consumers whose data may be at risk.

**Key Take Away for Businesses Maintaining Digital Health Information**

Companies using applications that collect, use, or store personal health data should review the proposed amendments carefully including, but not limited to, some of the following provisions:

Many health apps and other similar technology are not covered by HIPAA, but under the proposed amendment, they would be covered by the HBNR.

Companies that offer wellness services should take note because they are likely within the scope of the proposed amendments.

The proposed changes expand the definitions beyond “websites” to include online services, including mobile applications. The FTC recognizes that consumers are increasingly using mobile applications to access their health information online.

Companies should monitor the use and disclosure of personal health information to third-party service providers and consider removing any personally identifying information before sharing the information with a third-party service provider.

Companies sharing information with any third party should ensure that the disclosures are authorized by the consumer. Under the proposed amendments, an unauthorized disclosure would explicitly qualify as a security breach, which is consistent with the most recent FTC enforcement actions.