Akin®

# FTC's First-of-Its-Kind Health Breach Notification Rule Enforcement Action

February 14, 2023

Reading Time : **4 min**

By: Natasha G. Kohne, Jo-Ellyn Sakowitz Klein, Caroline D. Kessler

On February 1, 2023, the Federal Trade Commission (FTC) announced that it had taken enforcement action against prescription drug discount company GoodRx, which agreed to injunctive relief and to pay a $1.5 million civil penalty to settle allegations that the company violated the FTC Health Breach Notification Rule and Section 5 of the FTC Act.

This enforcement action represents the first time the FTC has sought to enforce the FTC Health Breach Notification Rule (the "HBNR") and is an important example of the FTC's increasing willingness to wield its authority in the health space. The HBNR, which was first promulgated in 2009 under the Health Information Technology and Economic Health Act of 2009 ("HITECH Act"), focuses on personal health records (PHRs)—electronic records containing individually identifiable health information that are managed, shared and controlled by or primarily for an individual—and requires vendors of PHRs and PHR-related entities to notify affected individuals, the FTC and potentially the media in the event PHR identifiable information is acquired by an unauthorized person as a result of a breach of security. The FTC had issued a request for public comment on the HBNR in May 2020, and the HBNR received renewed attention in late 2021 when the FTC issued a policy statement clarifying that developers of health apps and connected devices are considered "health care providers" for purposes of determining whether data is within the scope of the HBNR, as they "furnish health care services or supplies." The policy statement also reminded entities that a "breach" is not limited to cybersecurity intrusions or nefarious behavior, and encompasses incidents of unauthorized access, including sharing of covered information without an individual's authorization. The FTC also issued additional guidance on the HBNR in

January 2022. This action against GoodRx is the agency's first time alleging a violation of the HBNR.

In its complaint, the FTC alleged that GoodRx violated both the HBNR and Section 5 of the FTC Act. Regarding the HBNR, the FTC asserted that GoodRx included third-party trackers on its platform (e.g., SDKs, pixels, etc.) and subsequently shared customer information with third-party advertising companies and advertising platforms without providing notice to consumers or seeking their consent. This information, which included, for example, the name of a drug for which the user had received a coupon, as well as that user's contact and location information (IP address and zip code), was then shared with certain platforms. The FTC alleged that GoodRx then used third-party platforms to "match specific users to their personal health information and designed campaigns that targeted users with advertisements based on their health information...." In an unusual move, GoodRx publicly responded to the FTC's announcement of the settlement, emphasizing that it did not admit to any wrongdoing and noting that it had proactively "made updates consistent with [its] commitment to being at the forefront of safeguarding users' privacy" three years ago, predating the FTC reaching out to the company. The company took particular issue with the FTC's allegations regarding the HBNR. GoodRx emphasized that this settlement was agreed to in an effort to avoid the expense of protracted litigation.

The complaint also alleged that GoodRx violated Section 5 of the FTC Act by, among other things, sharing personal health information with advertising companies and platforms after promising its users that it would not do so. The FTC claimed that GoodRx misled consumers by displaying a seal at the bottom of its telehealth services homepage attesting to its purported compliance with HIPAA, when in fact GoodRx was not a covered entity subject to HIPAA and its privacy practices did not comply with HIPAA's requirements.

The GoodRx matter is significant for a number of reasons, beyond being the first enforcement action under the HBNR. In addition to the monetary penalty, the proposed order submitted to the U.S. District Court for the Northern District of California would set significant limits on GoodRx's data practices and require GoodRx to establish certain related policies and procedures. Notably, among other things, the proposed order would (i) prohibit GoodRx from sharing health information with third parties for advertising purposes, with limited exceptions; (ii) restrict GoodRx from disclosing user health information to third parties for other purposes without first obtaining the user's affirmative express consent; and (iii) require GoodRx to limit how long it retains personal and health information through a data

retention schedule that is publicly posted. The proposed order would require GoodRx to establish a comprehensive privacy program that includes strong safeguards to protect consumer data and to institute mandatory annual privacy training for employees. GoodRx would be required to allow an independent auditor to review the program every two years for 20 years, and would be subject to detailed recordkeeping requirements.

In its blog post discussing the settlement, the FTC used this opportunity to caution other companies in the industry, emphasizing that transparency with customers regarding information-sharing practices is crucial. The FTC also warned that health app companies handling health data should take special care to protect this information, establish contractual boundaries with third parties regarding the use of information and monitor data flows to these parties.

If you have any questions, please contact a member of the Akin health regulatory or cybersecurity, privacy and data protection teams.

## Categories

FTC | Data Breach | Cybersecurity & Information Security | Health Information Privacy & Security | HIPAA & HITECH

other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.