



Feb 23, 2023

Categories:

[E-Commerce](#)

[Gibbons](#)

[Privacy and Data](#)

[Security](#)

[Privacy Class Actions](#)

[Regulatory Counseling](#)

[and Departmental](#)

[Action](#)

Authors:

[John T. Wolak](#)

GoodRx Fined \$1.5 Million for Disclosure of Users' Personal Information to Third Parties Without Notice or Consent

On February 1, 2023, the Federal Trade Commission (FTC) filed a "first of its kind" enforcement action under the FTC's [Health Breach Notification Rule](#), 16 CFR Part 318, which offers several useful takeaways for *all* companies that collect and process a consumer's personal information – not just companies that handle health-related data. The FTC's proposed order seeks to impose a \$1.5 million civil penalty against GoodRx, a digital health platform, for sharing the sensitive personal health and other information of millions of GoodRx users with various advertising platforms, including Facebook and Google, and failing to report these disclosures to consumers.

According to the FTC [complaint](#), GoodRx collects sensitive personal information from users and represents that it will treat users' information in accordance with its privacy policies. Since at least 2017, the GoodRx privacy policy specifically stated that GoodRx "would never disclose personal health information to advertisers or any third parties." Yet for several years, GoodRx allegedly violated these promises "by sharing information with Advertising Platforms, including Facebook, Google and Criteo, about users' prescription medications or personal health conditions" and "did so without notice to users, and without obtaining consent." In addition, GoodRx monetized the personal health information it collected through the creation of advertising campaigns on Facebook and Instagram that targeted GoodRx users. In August 2019, for instance, GoodRx created ad campaigns based on medication purchase data it had collected in order to target users with advertisements that featured the purchased prescriptions.

Based on these schemes, the FTC alleged that GoodRx allowed third parties, such as Facebook, to use GoodRx consumers' personal information "for its own purposes, including its own research and

development and ad optimization purposes.” GoodRx’s alleged violations were compounded by the fact that it “did not have sufficient formal, written, or standard internal data sharing policies or procedures that governed how all types of health and personal information could be shared.” Finally, GoodRx allegedly misrepresented its compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), when it displayed a seal at the bottom of its telehealth services homepage “signal[ing] to users that it is a HIPAA-covered entity, and that its practices complied with HIPAA’s requirements.”

In addition to the \$1.5 million civil penalty, the FTC’s [proposed order](#) would prohibit GoodRx from disclosing its users’ personal health information to third parties for advertising purposes and without notice and the affirmative express consent of its users. The order would also require GoodRx to: (1) direct third parties to delete any and all consumer health information that was provided to them; (2) inform its users about the unauthorized disclosures and the FTC’s enforcement action; (3) implement “a retention schedule” limiting the retention of personal information to “only as long as is reasonably necessary” to achieve the purpose of collection; and (4) implement a comprehensive privacy program, within 180 days of the entry of the proposed order, that safeguards its users’ personal information.

The action against GoodRx represents yet another step by the FTC to assert its authority in privacy cases, this time alleging violations of the Health Breach Notification Rule, as well as activities that the FTC alleges were unfair or deceptive under Section 5 of the FTC Act. As a result, the FTC’s enforcement action serves as a cautionary tale for all businesses – not just health-related businesses – to:

- accurately and completely describe data-handling practices in their privacy policy
- ensure that ongoing operations are consistent with those data-handling practices
- implement and enforce policies for retention of personal information for only as long as is reasonably necessary given the business purpose of collecting the personal information

- include use limitations and restrictions on the personal information shared with third parties that are consistent with the nature of the data being shared
- provide notice (and obtain consent if necessary) before collecting and processing personal information, especially for advertising purposes

Please contact the firm's data privacy attorneys if you require assistance or advice regarding your data-handling practices.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.