Updates
February 09, 2023
FTC Claims Sharing User Health Data With Advertising Platforms Is a “Security Breach”

For the first time, the Federal Trade Commission has brought an enforcement action under its 2009 Health Breach Notification Rule (HBNR). The case was brought against a digital health company, GoodRx Holdings, Inc., for sharing users' health information with third-party advertising platforms without the authorization of the users whose data was being shared.

While the HBNR sounds like a security breach notification regulation and was traditionally viewed as such, the FTC foreshadowed in a 2021 policy statement that it would use the HBNR to address privacy claims in this new way. In this statement, the FTC announced that a "breach" under the HBNR "is not limited to cybersecurity intrusions or nefarious behavior" but also includes "[i]ncidents of unauthorized access, including sharing of covered information without an individual's authorization." In the FTC's view, this includes—as with GoodRx—a company's *intentional* sharing with contractual third parties without sufficient consent from users. More broadly, the FTC's case against GoodRx reinforces that digital health companies, even when not regulated by the Health Insurance Portability and Accountability Act (HIPAA), need to treat health information as sensitive and subject to heightened requirements, and must comply with FTC-enforced laws, such as the HBNR and Section 5 of the FTC Act.

Background on the Health Breach Notification Rule

The HBNR was promulgated by the FTC over a decade ago. The HBNR:

- **Applies to digital health companies that are not covered by HIPAA.** The HBNR expressly carves out HIPAA-covered entities and HIPAA-covered activities of business associates from its reach. Instead, it

applies to companies with various roles related to a "personal health record," which is an electronic record of individually identifiable health information that can come from multiple sources and is managed, shared, and controlled by or primarily for the individual. "Vendors" of personal health records are subject to the HBNR, as are companies that access or send information to personal health records or offer products or services through the website of such a vendor ("PHR related entit[ies]"), and certain other types of companies and service providers. 16 C.F.R. § 318.1(a), 318.2(d)-(f), (h), (j).

- **Facially applies to any "unauthorized acquisition" of user health information, regardless of whether there was a "breach of security" in the traditional data security sense.** The HBNR defines "breach of security" as, simply, "acquisition of [information in a personal health record] without the authorization of the individual." Further, "access[ing]" such health information in a personal health record without authorization is also a presumed "breach of security." 16 C.F.R. § 318.2(a). Thus, in the FTC's view, an intentional sharing without sufficient consent of the individual—normally thought of as a privacy issue, not a security incident—is a "breach of security" under the HBNR.
- **Requires companies to give notice of a "breach of security" to affected individuals and the FTC.** The HBNR requires companies to notify affected individuals and the FTC of a "breach of security" as defined above. The rule has requirements for content, method, and timeliness of notifications, and it requires media notice if the contact information for 10 or more of the individuals is out of date or if the health information of 500 or more individuals in a single state or "jurisdiction" is reasonably believed to be subject to a breach. 16 C.F.R. §§ 318.3-318.6.
- **Subjects violators to civil penalties and injunctions.** Violations of the HBNR can subject the violator to penalties of up to $50,120 per violation and to permanent injunctive relief relating to the practices giving rise to the violation, such as a permanent prohibition on business practices involving the sharing or disclosure of personal health information.

The FTC's Complaint and Stipulated Order Against GoodRx

GoodRx is a digital health company that provides discounts on prescription drug purchases and telemedicine services.

In its complaint, the FTC alleges that beginning in 2017, GoodRx shared user information, including contact information, identifiers, and medication and health condition information, with third-party advertisers and advertising platforms without users' knowledge or consent. The FTC alleges that this conduct violated the HBNR because the sharing was unauthorized and GoodRx did not provide HBNR notifications to users or the FTC. The FTC also alleges a bevy of claims under Section 5 of the FTC Act on the basis that these sharing practices were unfair and rendered deceptive various statements in GoodRx's privacy policy, a "HIPAA Secure" seal on its telehealth services webpage, and its representations that it was in compliance with the Digital Advertising Alliance (DAA) Principles.

The FTC's action includes a proposed stipulated order and judgment against GoodRx that provides for $1.5 million in penalties for the HBNR violation. It also includes a permanent injunction barring GoodRx from *ever* sharing user health information with third parties for advertising purposes, *regardless* of whether it obtains user consent; and barring GoodRx from sharing user health information with third parties for non-advertising purposes unless it first obtains affirmative express consent. The permanent injunction also adds additional requirements to any future HBNR notifications GoodRx might need to make; requires GoodRx to seek third-party deletion of data shared with and to inform consumers about the "breach" and enforcement action; requires GoodRx to limit retention of health and personal data according to a publicly posted retention schedule detailing

what information is collected and for what purpose; and requires GoodRx to implement a mandated privacy program.

The Commission voted 4-0 to refer the order to the U.S. Department of Justice (DOJ) for filing. GoodRx issued a public response, noting that it ceased the practices at issue years ago before the FTC investigation began.

Takeaways

The FTC's action against GoodRx is exactly the type of scenario it warned consumer-facing "health apps and connected devices" about in its 2021 policy statement that signaled likely enforcement activity under HBNR. While it may be head-scratching to think of an intentional sharing of data with contractual third parties as a "breach of security," the language of the HBNR is unusual as compared to most other breach notification laws. As applied to fact patterns such as GoodRx's alleged sharing practices, the HBNR is perhaps better thought of as a regulation that the FTC will seek to apply in an expansive manner to privacy *or* security issues for digital health companies. Companies operating in the digital health space should consider their privacy policies and data sharing practices carefully in light of the FTC's heightened scrutiny of consumer health information disclosures.

The HBNR claim also is significant because it (unlike the Section 5 claims) allows the FTC to obtain civil penalties. The inclusion of the claim here further underscores the FTC's recent interest in pursuing claims for which it can seek monetary relief in the wake of the U.S. Supreme Court's ruling that it lacks the power to obtain disgorgement or restitution for Section 5 violations under Section 13(b) of the FTC Act.

Finally, the case is a reminder that the FTC views consumer health information, whether or not covered by HIPAA, as "sensitive" information and applies exacting standards under its deception and unfairness authority to companies' representations and practices regarding such data. It is noteworthy that the FTC alleged GoodRx's disclosure of health information to advertising platforms without providing notice to users or obtaining their affirmative express consent was an unfair practice. This not only reflects the FTC's growing willingness to use its unfairness authority in the privacy arena, but also suggests that the FTC expects businesses to obtain specific, opt-in consent before sharing health data for advertising purposes.

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law Healthcare Technology & Communications

Related insights

Update

The FY 2025 National Defense Authorization Act: What's New for Defense Contractors

Update

January Tip of the Month: Trump Executive Orders Challenge DEI Programs