The Computer & Internet Lawyer

Volume 40 ▲ Number 5 ▲ May 2023

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Federal Trade Commission Brings First Enforcement Action of the Health Breach Notification Rule

By Melissa M. Crespo and Libby Strichartz

The Federal Trade Commission (FTC) has enforced its Health Breach Notification Rule (the HBNR) for the first time since it was enacted in 2009. On February 1, the FTC announced[1] a first-of-its-kind proposed order (the Order)[2] with digital health platform GoodRx Holdings Inc. (GoodRx), a telehealth and drug discount provider. The FTC alleged that GoodRx shared users' information with third-party advertising companies and advertising platforms contrary to its privacy promises, notably scrutinizing GoodRx's ad targeting and use of third-party tracking technologies.

Under the Order, GoodRx has agreed to pay a $1.5 million civil penalty and will be prohibited from sharing users' sensitive health data with third-party advertisers.

This action is a reminder to all digital health companies subject to the HBNR to evaluate their online targeting and advertising practices, as well as the promises they make to users around these practices.

Melissa M. Crespo is a partner, and Libby Strichartz is an associate, with Morrison & Foerster LLP. They may be contacted at mcrespo@mofo.com and estrichartz@mofo.com, respectively.

HEALTH BREACH NOTIFICATION RULE

As a refresher, the HBNR,[3] which was issued under the American Recovery and Reinvestment Act of 2009 and became effective on September 24, 2009, applies to:

- Vendors of personal health records (PHRs);[4]
- PHR-related entities that interact with vendors of PHRs or HIPAA-covered entities by offering products or services through their sites or that access information in or send information to a PHR; and
- Third-party service providers for vendors of PHRs or PHR-related entities that process unsecured PHR identifiable health information[5] as part of providing their services.

The HBNR does not apply to HIPAA-covered entities or any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity. Under the HBNR, vendors of PHRs and PHR-related entities are required to report a "breach of security" involving PHRs to the FTC, consumers,

and the media (in some cases). Service providers to such entities that process information contained in PHRs (e.g., for billing or data storage purposes) also have notice obligations to report such breaches to their business customers. The HBNR defines a "breach of security" as the acquisition of unsecured, PHR identifiable health information that is in a PHR, without the authorization of the individual. Notice is required no later than 60 days of discovering the breach, unless more than 500 people are impacted (in which case, the FTC must be notified within 10 business days). If covered entities fail to comply, violations of the HBNR are subject to civil penalties of $50,120[6] per violation per day.

Despite the 14-year period of dormancy since the HBNR was enacted, this enforcement action does not come as a surprise. To the contrary, the FTC has signaled in recent years that enforcement was imminent.

In September 2021, the FTC released a Policy Statement[7] clarifying that developers of health apps or connected devices are covered by the HBNR so long as they "are capable of drawing information from multiple sources, such as a combination of consumer inputs and application programming interfaces ('APIs')." The FTC also noted that a "breach of security" under the HBNR would not be limited to nefarious or malicious intrusions. Rather, even accessing or sharing information without an individual's authorization would qualify as a "breach of security" under the HBNR. The FTC explicitly stated that the Policy Statement was intended to place entities on notice of their ongoing obligation to "come clean" about breaches.

GoodRx Enforcement Action

According to the FTC's complaint,[8] GoodRx violated Section 5 of the FTC Act[9] by sharing users' sensitive information with advertisers and social media platforms contrary to its privacy promises Specifically, the FTC alleged that GoodRx:

- Shared sensitive health information for targeted advertising purposes despite promising in its privacy policy and other public statements that GoodRx never disclosed personal health information to third-party advertising companies and platforms, and allowed these advertising companies to use data GoodRx shared for their own internal purposes;

- Monetized users' personal health information to target users with personalized health advertisements on social media platforms;

- Falsely claimed that it complied with the Digital Advertising Alliance principles, which require companies to get consent before using health information for advertising;

- Misrepresented its HIPAA compliance; and

- Failed to implement polices to protect personal health information.

While the complaint alleges a number of claims based on GoodRx's privacy misrepresentations, which violate Section 5's prohibition against deceptive acts, most notably, the FTC also alleges that GoodRx engaged in unfair acts or practices in violation of Section 5 for failing to provide notice and obtain consent before using and disclosing health information for advertising and for failing to implement sufficient policies or procedures to prevent an unauthorized disclosure of personal health information or notify of breaches of that information.

In addition to these violations, the FTC alleged that GoodRx, as a vendor of personal health records[10] violated the HBNR by failing to report these unauthorized disclosures to the FTC, consumers, and the media.

Under the Order, in addition to the $1.5 million penalty, GoodRx is:

- Prohibited from disclosing user health information to applicable third parties for advertising purposes;

- Required to obtain affirmative express consent before disclosing user health information to applicable third parties for other purposes;

- Required to direct third parties to delete the consumer health data that was shared with them; and

- Required to implement a privacy program with strong safeguards to protect consumer data that will be subject to a biennial assessment from a third-party assessor.

KEY TAKEAWAYS

This enforcement action is a cautionary reminder of the increased scrutiny that targeted advertising and the use of third-party tracking tools have recently come under, particularly in the digital health space. In light of the GoodRx action, digital health companies should:

- *Evaluate Applicability of the HBNR*. As noted, the FTC's Policy Statement makes clear that the HBNR is intended to apply broadly, clarifying that makers

of health and wellness apps that hold health information generated from consumers and connected devices must comply with the HBNR. Digital health companies should review the HBNR and the Policy Statement to determine if they are subject to it.

- *Review Use of Targeted Advertising Technologies*. Companies should understand how and what data is collected and shared with third-party advertising companies and how these companies use the data. Companies should ensure these practices are aligned with representations made in their privacy policies and other public statements. They should also evaluate whether their notice and consent processes are aligned with the FTC's expectations for these activities.

- *Review Privacy Practices Against Privacy Policies and Other Public Statements*. Companies should also periodically evaluate their privacy practices against privacy representations to ensure that these statements are accurate and that companies are being transparent about how they use and disclose information.

Notes

1. https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising.
2. https://www.ftc.gov/system/files/ftc_gov/pdf/goodrxfinalstipulatedorder.pdf.
3. 16 C.F.R. § 318.3.
4. A PHR is an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual. See 16 C.F.R. § 318.2(d).
5. "PHR identifiable health information" includes "individually identifiable health information," as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and, with respect to an individual, information: (1) that is provided by or on behalf of the individual; and (2) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. See 16 C.F.R. § 318.2(e).
6. Based on the FTC's inflation-adjusted civil penalty amounts for 2023.
7. https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.
8. https://www.ftc.gov/system/files/ftc_gov/pdf/goodrx_complaint_for_permanent_injunction_civil_penalties_and_other_relief.pdf.
9. Section 5 of the FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce.
10. The complaint identifies GoodRx as a "vendor of personal health records" and subject to the HBNR because it lets users keep track of their personal health information, drawing information from users, pharmacies, healthcare professionals, and users' geographic location information from a third-party vendor that approximates geolocation based on IP address.