ROPES & GRAY

ALERT

February 8, 2023

FTC Enforces Health Breach Notification Rule against GoodRx in First of its Kind Enforcement Action

Attorneys
Deborah L. Gersh
Jennifer L. Romig
Christine Moundas
Winnie Uluocha

On February 1, 2023, in a first-of-its-kind enforcement action, the Federal Trade Commission ("FTC") alleged that GoodRx Holdings Inc. ("GoodRx"), a telehealth and prescription drug discount provider, violated multiple laws, including the agency's Health Breach Notification Rule ("HBNR"), by sharing sensitive customer information with Facebook, Google, Criteo, and other advertising platforms without its users' knowledge or consent. The proposed order, brought by the U.S. Department of Justice on behalf of the FTC, is the FTC's first action under the HBNR,[1] which took effect on September 24, 2009.

Since 2009, healthcare innovation has led to continued growth in the digital health space, with new health apps, wearables, and connected devices coming to market every day. As discussed in our prior Alert, federal agencies are taking note of – and attempting to protect consumers from – the growing use of tracking technologies embedded in health apps and healthcare-related websites that share sensitive user health information for advertising and other purposes without proper notice, consent, or authorization. Below, we provide an overview of the HBNR, a summary of the FTC's recent enforcement against GoodRx, and critical takeaways for businesses operating in the digital health and wellness space.

Health Breach Notification Rule

In February 2009, former President Obama signed into law the American Recovery and Reinvestment Act of 2009,[2] which directed the FTC to ensure that those companies not required to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") notify consumers in the event of a security breach. Shortly thereafter, the FTC issued the HBNR, which (as defined below) requires each "*vendor of personal health records ("PHR")*" and each "*PHR related entity*" to notify impacted individuals, the FTC, and, in some cases, the media, in the event of a breach of security[3] of unsecured[4] PHR identifiable health information contained in a "*personal health record*" (*i.e.*, an electronic record of PHR identifiable health information drawn from multiple sources and managed, shared, and controlled by or primarily for an individual[5]) that is maintained or offered by such entity or through a product or service provided by such entity.[6] The HBNR also requires that any "*third party service providers*" notify the vendor of personal health records or the PHR related entity in the event of a discovery of such a breach.[7] The HBNR defines these key players as follows:

- A "**vendor of personal health records**" is an entity that offers or maintains a personal health record.[8] The FTC has said that a health app that collects information from consumers and can sync with a consumer's fitness tracker is likely a vendor of personal health records.[9]

- A "**PHR related entity**" is an entity that interacts with a "vendor of personal health records" by either offering products or services through the vendor's website, offering products or services through a HIPAA covered entity's website that offers individual's health records, or by accessing information in a personal health record or sending information to a personal health record.[10] The FTC has said that a company that offers a fitness tracker and sends information to health apps is likely a PHR related entity.[11]

- A "**third party service provider**" is a company that provides its services involving the use, maintenance, disclosure, or disposal of health information to vendors of personal health records or PHR related entities.[12] The FTC has said that a company that provides billing, debt collection, or data storage services relating to health information for a vendor of personal health records is likely a third party service provider.[13]

On September 15, 2021, more than a decade after the HBNR's establishment, the FTC issued a short policy statement (the "Statement"), ostensibly designed to provide clarifying guidance on the scope of the HBNR. The Statement, however, appeared to broaden the types of entities and information that would be subject to the HBNR by clarifying that (1) the developer of a health app or connected device is, in fact, a "health care provider" under definitions cross-referenced[14] by the HBNR and therefore can be said to create PHR identifiable health information in a personal health record subject to the HBNR, and (2) an app that draws information from multiple sources is subject to the HBNR, even if the health information comes from only one source.[15] Finally, the FTC warned that the Statement was intended to "place entities on notice of their ongoing obligation to come clean about breaches" and noted that "the [FTC] intends to bring actions to enforce the [HBNR] consistent with this Policy Statement." This FTC warning came to fruition with its enforcement action against GoodRx.

GoodRx Enforcement Action

The FTC's recent enforcement action against GoodRx is notable for many reasons. GoodRx is a digital healthcare platform that advertises, distributes, and sells health-related products and services directly to consumers, including telehealth services, prescription medication discount cards, and the ability to compare prescription drug prices. To provide these products and services, GoodRx collects personal and health information from users, healthcare professionals (including pharmacies) and pharmacy benefit managers. According to the FTC, more than 55 million people have used or visited GoodRx's mobile application or website since 2017.[16]

In its complaint, the FTC alleged that GoodRx promised users that it would share their personal and health information with limited third parties and for limited purposes and that it would never share personal health information with advertisers or other third parties.[17] Instead, according to the FTC, GoodRx repeatedly violated these promises by sharing sensitive personal and health information with third-party advertising companies and platforms (like Facebook, Google, and Criteo) and other third parties (like Branch and Twilio) and permitted the third parties to use such information for their own business purposes.[18] The FTC further alleged that GoodRx itself exploited user personal and health data to conduct targeted ad campaigns through Facebook and that, in doing so, GoodRx disclosed information about individual health conditions and prescription medications to Facebook.[19] Finally, the FTC alleged that GoodRx misrepresented its compliance with HIPAA and Digital Advertising Alliance principles and that GoodRx failed to implement policies to protect user health information.[20]

Given the above, the FTC charged that GoodRx violated the HBNR by failing to notify the appropriate parties of a breach of unsecured PHR identifiable health information and participated in deceptive and unfair acts or practices in violation of Section 5 of the FTC Act. Although GoodRx admitted no wrongdoing, under the stipulated order, GoodRx agreed not to share user health information with third parties for advertising purposes and to pay a $1.5 million civil penalty.

Key Compliance Considerations

The growing use of online tracking technologies and their intersection with the healthcare ecosystem means that federal and state regulators will continue to look for novel ways to protect consumers' sensitive health information through enforcement. In light of this enforcement action, digital health players (including those involving healthcare apps, connected devices, and wearables) and other companies in the healthcare and wellness industry should consult the FTC HBNR resource page and consider taking the following steps:

- Reassess whether HIPAA, the HBNR, and state data breach notification laws apply to your business, products, and services. Of note, a company may be subject to all three sets of laws.
- Carefully review any external privacy notices or policies, as well as internal policies and procedures, to ensure that your company's privacy practices (including its consent process) accurately reflect its current data-sharing practices with third parties.

- Monitor the third parties with which your company shares sensitive information to understand what information is disclosed, how that information is used (particularly for advertising purposes), and to ensure consistency with third parties' contractual obligations.

- If applicable, go through the FTC's basics about the HBNR and its application – HBNR compliance steps and its helpful web-based interactive tool page for health apps that can help you consider laws and rules that may apply to your business – and the FTC's comprehensive health privacy resource page.

* * *

If you have any questions concerning this Alert, please do not hesitate to contact one of the authors or your regular Ropes & Gray advisor.

1. Health Breach Notification Rule, 74 FR 42961 (finalized Aug. 25, 2009) (codified at 16 CFR Part 318).
2. American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).
3. "Breach of security" means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual. *See* 16 CFR 318.2(a)
4. "Unsecured" means PHR identifiable information that is not protected through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued under Section 13402(h)(2) of the Recovery Act. *See* 16 CFR 318.2(i).
5. *See* 16 CFR 318.2(d).
6. *See* 16 CFR 318.3.
7. *See* 16 CFR 318.3(h).
8. *See* 16 CFR 318.2(j).
9. *See* Complying with FTC's Health Breach Notification Rule Guidance.
10. *See* 16 CFR 318.2(f).
11. *See* Complying with FTC's Health Breach Notification Rule Guidance.
12. *See* 16 CFR 318.3(h).
13. *See* Complying with FTC's Health Breach Notification Rule Guidance.
14. *See* 42 U.S.C. § 1320d(3), d(6).
15. The FTC has said, for example, if a blood sugar monitoring app draws health information only from one source (e.g., a consumer's inputted blood sugar levels) but also takes non-health information from another source (e.g., dates from the consumer's phone's calendar), it is subject to the HBNR. *See* FTC Policy Statement.
16. Complaint for permanent injunction, civil penalties, and other relief, pg. 5, *United States of America vs. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (Dist. Ct. Nor. Dist. of Cali.).
17. *Id.* at pg. 2.
18. *Id.*
19. *Id.* at pgs. 2–3.
20. *Id.* at pgs. 8–9.