King & Spalding
Client Alert

FEBRUARY 21, 2023

FTC Announces First Enforcement of the Health Breach Notification Rule

For more information, contact:

Marisa Maleck
+1 202 626 9117
mmaleck@kslaw.com

Igor Gorlach
+1 713 276 7326
igorlach@kslaw.com

Sydney Teng
+1 404 572 4716
steng@kslaw.com

Kasey Ashford
+1 202 626 2906
kashford@kslaw.com

Rachel Brown
+1 202 626 9543
rbrown@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Suite 900
Washington, D.C. 20006
Tel: +1 202 737 0500

On February 1, the Federal Trade Commission ("FTC") announced its first enforcement action under the Health Breach Notification Rule ("HBNR" or "Rule") against GoodRx, a direct-to-consumer digital healthcare and prescription drug platform. GoodRx agreed to pay a $1.5 million penalty to settle claims stemming from the platform's undisclosed use of third-party tracking technologies.

FTC takes the position that "the Rule plays a vital role in holding companies accountable for how they disclose consumers' sensitive health information."[1] The HBNR is "one of only a handful of federal privacy laws protecting consumers' health information."[2] The GoodRx action makes good on the agency's promise to enforce the Rule "to keep pace with changing technology" as "consumers have turned to apps, wearables, and other technologies for health advice, information, and tracking."[3]

Background: The Health Breach Notification Rule

Last week's GoodRx announcement marks the first enforcement of the HBNR since it was promulgated over a decade ago.[4] The American Recovery and Reinvestment Act of 2009 ("Act") directed FTC to issue a rule regarding a "temporary breach notification requirement for vendors of personal health records ["PHR"] and other non-HIPAA covered entities."[5] FTC's HBNR became effective in August 2009 and requires PHR vendors and PHR related entities to, "following the discovery of a breach of security[,] . . . notify each individual . . . whose unsecured PHR identifiable health information was acquired by an unauthorized person . . . ." [6] Through subsequent business guidance, including a policy statement released in September 2021, FTC has described its broad interpretation of the Rule, including what qualifies as a breach triggering notification obligations.[7] Violations of the HBNR are unfair or deceptive acts or practices under the FTC Act, subject to civil penalties of up to $50,120 per violation.

The Rule Applies to PHR Vendors and Related Entities

The Rule applies to any entity that is not otherwise covered by the Health Insurance Portability and Accountability Act ("HIPAA") and (1) "offers or maintains a personal health record" (a "PHR vendor"), (2) "accesses information in a personal health record or sends information to a personal health record," (3) "offers products or services through the Web site of a vendor of personal health records," or (4) "offers products or services through the Web sites of HIPAA-covered entities that offer individuals personal health records" (each a "PHR related entity").[8]

FTC defines PHR as "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."[9]

FTC provides some non-exhaustive examples of PHR vendors and related entities, such as "online repositories of health information that individuals can create to track their medical visits, prescription information, etc." and "online applications through which individuals connect their blood pressure cuffs, blood glucose monitors, or other devices so that they can track the results through their PHRs."[10] Furthermore, FTC clarified that most fitness apps that "can sync with wearable fitness trackers" are "likely" vendors of PHR because they can draw information from multiple sources, which includes both users themselves and the Application Programming Interface ("API") that enables the app to connect with the wearable device.[11] FTC stresses that it is the technical capacity to pull any information, not just covered information, that satisfies the definitional requirement that PHRs "can be drawn from multiple sources."[12]

The Rule Requires Notice of Unauthorized Disclosures

The HBNR requires PHR vendors and PHR related entities to notify individuals when there has been (1) an unauthorized acquisition of (2) PHR-identifiable health information, thus allowing identification of individuals who have not authorized this acquisition, (3) that is unsecured and (4) in a personal health record.[13] If a HBNR-covered breach occurs, the entity must notify:

(1) each affected person who is a citizen or resident of the United States;

(2) FTC, using [a designated] form; and

(3) in some cases, the media.[14, 15]

On September 15, 2021, FTC, in a divided vote, issued *Policy Statement on Breaches by Health Apps and Other Connected Devices* ("Policy Statement").[16] In the Policy Statement, FTC announced a broad interpretation of a breach that would require notification under the Rule.[17] As described in later business guidance, "'breach' is not limited to cybersecurity intrusions or nefarious behavior by hackers or insiders. Incidents of unauthorized access, including a company's disclosure of covered information without a person's authorization, triggers notification obligations under the Rule."[18]

The GoodRx Complaint

GoodRx is a healthcare and prescription drug platform that offers discounted medications and specific telehealth services directly to consumers. The crux of FTC's action involves GoodRx's alleged disclosure of health-related data to advertising platforms, such as Facebook, Google, and Criteo, through tracking tools (often pixels). These tools allegedly recorded and transmitted to these third parties sensitive information through certain "events" (actions taken on GoodRx's websites).[19]

The complaint alleges that, when a user accessed a GoodRx coupon for a medication, a Facebook pixel recorded the medication name and related health condition associated with the coupon under the event names "Drug Name" and "Drug Category."[20] In some instances, FTC alleged, the Facebook pixel also shared information that overtly identified the user, including full name, email address, phone number, and zip code. In others, the pixel allegedly conveyed the user's IP address. The complaint details several such examples of pixels sharing drug information, including data points like the user's pharmacy, dosage amount, form of medication, and drug quantity. Throughout these examples, the complaint stresses that GoodRx shared specific user activities under customized and descriptive titles, as distinguished from standard events that occur on websites, such as when a website is first launched, or through anonymous names for custom events, such as "Event_1."[21]

In addition to pixels that conveyed drug information, the complaint also describes another pixel on GoodRx's telehealth website. This pixel transmitted the specific URL that a user visited within GoodRx's treatment pages prior to beginning a telehealth consultation. The treatment page URLs directly referenced a health condition, such as "www.heydoctor/goodrx.com/services/hyperlipidemia," which linked to GoodRx's treatment services for high cholesterol.[22]

Ultimately, this information sharing enabled GoodRx, through digital advertisers and their platforms, to target users with advertisements based on health conditions and drug purchases associated with the user. For many advertising campaigns, GoodRx used a health condition (e.g., "HIV") or drug name (e.g., "atorvastatin claims") to label the specific campaign and corresponding targeted audience within the digital advertiser's management account.

Furthermore, GoodRx did not seek specific contractual assurances from digital advertisers to protect the health information. Rather, GoodRx agreed to their standard terms of use and/or entered into agreements that permitted digital advertisers to use the health information for their own internal business purposes.[23]

Because GoodRx did not report these unauthorized disclosures, FTC took the position that the company shared health information in violation of the HBNR.[24] Apart from the HBNR violation, FTC alleges seven other counts of unfair or deceptive acts or practices, including five "privacy misrepresentations" and two counts of "unfairness" related to failure to maintain appropriate measures to obtain consent and prevent unauthorized disclosures.

The complaint extensively cites GoodRx's privacy policy to support its five counts of privacy misrepresentations, including statements such as "[GoodRx] never provide[s] advertisers or any other third parties any information that reveals a personal health condition or personal health information."[25] The privacy policy also promised users that when GoodRx shared health information, it "takes steps such that these third parties are subject to confidentiality obligations", despite the fact that GoodRx lacked any internal policies governing data sharing or contractual or technical protections with respect to its relationships with digital advertisers. Lastly, GoodRx's telehealth website displayed a "HIPAA Secure. Patient Data Protected." seal, even though GoodRx is not a HIPAA-covered entity, and its information practices did not comply with HIPAA.[26]

The GoodRx Stipulated Consent Order

GoodRx agreed to a stipulated consent order with FTC to settle the eight FTC Act violations.[27] In doing so, GoodRx did not admit or deny any of the FTC's allegations. Assuming the proposed order is approved, GoodRx will pay a $1.5 million penalty and will be permanently prohibited from disclosing health information to third parties for advertising purposes.

The order also prohibits GoodRx from disclosing health information to third parties for non-advertising purposes without first obtaining affirmative express consent from the individual. An individual can provide affirmative express consent only after the company makes a clear and conspicuous disclosure of the type of health information that would be disclosed to a third party, the identity or category of the third party, and the purposes and uses of the health information. The order considers a disclosure to be clear and conspicuous when it is easily noticeable and understandable, and not located in a privacy policy, terms of service, or terms of use.

GoodRx must also implement a comprehensive privacy program that includes an annual reporting requirement to the company's board of directors and chief executive officer. Other selected highlights from the mandated privacy program include: annual internal privacy risk assessments; systematic data inventorying; audits and reviews of any contracts, privacy policies, or terms of service associated with third parties that receive information from GoodRx; internal access controls and annual employee privacy training; a data retention schedule; and audits of any pixels or Software Development Kits, and any third parties associated with these technologies.

The stipulated order also requires GoodRx to identify all third parties that received health information from GoodRx and to direct them to delete all such data. GoodRx must obtain written confirmation of the deletion. Further, GoodRx must inform individual users of the order, including a brief summary of some of the above mandated information practices, by posting a notice on its websites and mobile application and also emailing all impacted individuals.

Similar to other FTC consent orders, GoodRx must also submit to a third-party privacy assessment every two years for twenty years following the order and satisfy recordkeeping and compliance reporting requirements for twenty years as well.

Conclusion

FTC's first HBNR enforcement action focuses on the sharing of prescription drug information with third-party digital advertisers, a group that FTC has separately described as contributors to a "murky marketplace."[28] The examples of information sharing here included data fields and descriptions that, on their face, revealed health information, such as "Lipitor" under the event title "Drug Name." Furthermore, this health information was linked to an individual either through their full name and contact information or their IP address.

The GoodRx enforcement action also highlights the breadth of FTC's application of the HBNR, particularly with respect to "breaches" that, perhaps contrary to conventional understanding, include certain intentional disclosures to third-party vendors.

FTC also asserts an expansive reading of the definition of PHR. Despite multiple health information inputs in GoodRx, the Policy Statement stresses that health information only needs to originate from one source, which could be the user themselves, so long as the PHR is "capable of drawing information from multiple sources." The complaint against GoodRx cited a third-party tech provider that approximated geolocation from IP address and the Policy Statement cites "dates from your phone's calendar", which suggests that even the most basic platforms that collect some health information will likely be covered by the Rule.

Finally, the GoodRx enforcement is yet another indication of FTC's heightened scrutiny of information practices related to health information. Indeed, the agency's recently released *Health Products Compliance Guidance* mimics similar high expectations with respect to health claims, including those made in the digital health space.[29] FTC's guidance and enforcement activity signal the agency's intent to fill any perceived regulatory gaps with respect to health information, as made clear in its business guidance: "[M]any companies that collect people's health information . . . aren't covered by HIPAA. Does that mean this sensitive health information

doesn't have any legal protections? Not at all." Put differently, FTC's consumer protection director, Samuel Levine, stated, "The FTC is serving notice that it will use all of its legal authority to protect American consumers' sensitive data from misuse and illegal exploitation."[30]

ABOUT KING & SPALDING'S DATA, PRIVACY AND SECURITY PRACTICE

King & Spalding has substantial experience with the technology at the heart of the HBNR. The firm is unique in its ability to employ forensic tools to easily determine whether and where this technology resides on websites and has substantial experience in advising legal departments, IT specialists, and marketing departments about how to use this technology within the bounds of the HBNR. The firm also has substantial experience handling inquiries from state Attorneys General and the Federal Trade Commission about the use of this technology.

[1] Fed. Trade Comm'n, Complying with the FTC's Health Breach Notification Rule (Jan. 2022) ("Complying with FTC's HBNR"), https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.

[2] *Id*.

[3] *Id*.

[4] *See* Press Release, Fed. Trade Comm'n, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising (Feb. 1, 2023) ("Press Release"), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising.

[5] 42 U.S.C. § 17937.

[6] *See* Health Breach Notification Rule; Final Rule, 74 Fed. Reg. 42,962 (Aug. 25, 2009) (codified at 16 C.F.R. Part 318).

> "Breach of security" means acquisition of [PHR identifiable health information] without the authorization of the individual." Information that is acquired by someone else without the affected person's approval constitutes an unauthorized acquisition under the HBNR. Generally, FTC presumes that unauthorized acquisition is the same as unauthorized access. 16 C.F.R. § 318.2(a).
>
> "PHR identifiable health information" means (a) "individually identifiable health information," as defined in the Social Security Act, (b) "that is provided by or on behalf of the individual" and (c) "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." *Id.* at § 318.2(e).
>
> "Unsecured" has the same meaning as that term is defined by the U.S. Department of Health and Human Services and includes any information that is not encrypted or destroyed. *Id.* at § 318.2(i); 45 C.F.R. § 164.304.

[7] *See* Fed. Trade Comm'n, Statement of the Commission on Breaches by Health Apps and Other Connected Devices (Sept. 15, 2021) ("Policy Statement"), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.; *Complying with FTC's HBNR*.

[8] 16 C.F.R. § 318.2(f), (j).

[9] *Id.* at § 318.2(d).

[10] 74 Fed. Reg. 42962 n.2, n.78.

[11] *See Policy Statement* at 2, *Complying with FTC's HBNR* ("Answers to Questions About the [HBNR]").

[12] *See Policy Statement* at 2 ("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 your phone's calendar), it is covered under the Rule.").

[13] *See* 16 C.F.R. § 318.2(a).

[14] *Complying with FTC's HBNR*.

[15] Media notification is necessary if more than 500 residents of a particular state, the District of Columbia, or a U.S. territory or possession were affected or where the entity doesn't have contact information for at least 10 affected users. *See* 74 Fed. Reg. at 42974.

[16] *See Policy Statement*.

[17] *Id*. at 1–2 (citing 16 C.F.R. § 318.2(a)).

[18] *Complying with FTC's HBNR*.

[19] Complaint for Permanent Injunction, Civil Penalties, and Other Relief at 10, U.S. v. GoodRx Holdings, No. 23-CV-460, (N.D. Cal. Feb. 1, 2023) ("Complaint").

[20] *Id.* at 10–11.

[21] *Id.* at 10.

[22] *Id.* at 11-12.
[23] *Id.* at 14–15.
[24] Complaint at 13, 20.
[25] *Id.* at 7.
[26] *Id.* at 9–10.
[27] Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, U.S. v. GoodRx Holdings, No. 23-CV-460, (N.D. Cal. Feb. 1, 2023).
[28] *See FTC Publishes Blog Post Announcing Focus on "Murky Marketplace"* available at https://kslawemail.com/84/9346/pages/ftc.asp.
[29] *It's Not Just for Dietary Supplements Anymore: FTC Revises and Expands Guidance for Health Claims* available at https://www.kslaw.com/news-and-insights/its-not-just-for-dietary-supplements-anymore-ftc-revises-and-expands-guidance-for-health-claims.
[30] *See Press Release*.