akerman

Blog Post

FTC's Enforcement Action Against GoodRx Breathes New Life into Decade Old Regulation

February 27, 2023
By Jordan T. Cohen

The Federal Trade Commission (FTC) didn't mince words. On September 2021, it called out the health app industry for failing to understand the agency's Health Breach Notification Rule (HBNR) and for not disclosing its breaches. Apparently dissatisfied with the industry's response, the agency enforced the HBNR against GoodRx for the first time since the rule was released more than a decade ago.

GoodRx's platform enables users to compare prices at different pharmacies and receive discounted medications when using the company's coupons. GoodRx agreed to pay $1.5 million in connection with the action, but has not admitted to any wrongdoing.

When the FTC issued its warning in 2021, it likely had GoodRx in mind. According to its complaint, the agency began investigating GoodRx after Consumer Reports published an article in February 2020 about the company's data sharing practices. The publication used sophisticated traffic monitoring software to examine how the company used its app to collect, disclose, and use its customers' data, including data generated from searches for antidepressants, fertility treatments, and other sensitive medication.

Related People

Jordan T. Cohen

Related Work

Data Privacy and Security
Healthcare
Pharmacy, Drugs, and Medical Devices

Related Offices

New York

Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

Read blog posts

HBNR Background

The FTC's HBNR, released in 2009, was an attempt to provide a notification mechanism for breaches involving data that is not subject to HIPAA's breach notification rule. The rule requires vendors of personal health records (PHRs) to notify affected individuals and the FTC upon the discovery of a breach of security of its unsecured identifiable health information. 16 C.F.R. § 318.3(a). A "breach of security" includes the unauthorized acquisition of individually identifiable information in a PHR. 16 C.F.R. § 318.2(a). The specifics of the notification requirements are similar to HIPAA, including a general 60-day notice requirement to individuals, an obligation to notify the media for breaches involving 500 or more individuals in a state or jurisdiction, and expedited FTC notification for large breaches. The FTC has the authority to impose civil monetary penalties for violations of the HBNR. This is significant in the GoodRx case since the agency couldn't levy penalties against the company for deceptive trade practices under Section 5 of the FTC Act, which does not generally permit penalties against first-time offenders.

The Allegations

The FTC's complaint details GoodRx's pervasive sharing of user data with third parties, including vendors and social media companies. We learn in the complaint that GoodRx, like many healthcare organizations, used Meta's Pixel software to track its users. Meta Pixel works by adding a small amount of code to a website or web page. The code, which is invisible to the end user, collects data on the actions of users, such as page views, clicks, and conversions. According to the FTC, GoodRx used the software to capture information related to users' drug searches, and then shared the information with Facebook. This information included the drug name, the drug quantity, pharmacy name, and in certain cases the user's full name, email address, phone number, city, state, zip code, and IP address. After sharing the data with Facebook, GoodRx allegedly

used Facebook's advertising platform to serve its users targeted ads on Facebook and Instagram, including coupons for specific medications. Similar activities were also accomplished using tools offered by Google.

According to the FTC, this tracking and advertising violated the company's own representations to its users. In its privacy policy, GoodRx assured users that it would never disclose to advertisers or third parties any information that reveals a personal health condition or personal health information. The company also promised users that it would adhere to the Digital Advertising Alliance's principles, including the Alliance's prohibition on collecting and using pharmaceutical prescriptions or medical records for advertising purposes. The company doubled down on its privacy claims when its co-CEO Doug Hirsch tweeted that "any information that GoodRx receives is stored under the same guidelines as any health entity."

Seven of the eight counts in the FTC's complaint allege that the company's behavior violated the FTC Act's prohibition on unfair or deceptive acts or practices. And it's easy to see how that would be the case, given the alleged behavior. But for our purposes, the more relevant question is why the FTC believed that a prescription coupon company could violate a decade-old breach notification rule that applies to PHRs.

Does GoodRx's Platform Store PHR Identifiable Health Information?

The HBNR applies to "PHR identifiable health information," which the rules define to include individually identifiable health information (IIHI) that is provided by or on behalf of the individual and that identifies (or can be used to identify) the individual. 16 C.F.R. 318.2(e). The rule cross-references HIPAA's statutory definition of IIHI which defines the term to mean "any information, including demographic information collected from

an individual, that (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual...." 45 C.F.R. § 160.103. In the case of GoodRx, its platform pulls personally identifiable prescription-related information from its users' pharmacies and telehealth providers. Importing patient data created by such entities (which are health care providers under HIPAA) and storing it on behalf of its users puts GoodRx's data squarely within the HBNR's definition of PHR identifiable health information.

The FTC hasn't always had such an easy time. The prime example is the agency's action in 2021 against fertility tracker Flo Health. The agency's complaint did not allege a violation of the HBNR, presumably because the user data was limited to what the user entered, and did not include data from health care providers, health plans, etc. Two commissioners dissented from the decision, arguing that Flo Health was, itself, a "health care provider" under the cross-referenced definition, thus making the user data subject to the HBNR. Later in 2021, the agency released its HBNR guidance, repeating its developer-as-a-healthcare provider argument. That tortured logic wasn't needed in the case of GoodRx.

Is the GoodRx Platform a "PHR"?

For the regulation to apply, the information must exist in a PHR, which is defined 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." 16 C.F.R. 318.2(d). According to the complaint, GoodRx's platform satisfies the multi-source requirement:

GoodRx's website and mobile applications "...are capable of drawing information from multiple sources, including inputs from users; Medication

Purchase Data, pricing, and refill information from Pharmacy Benefit Managers; pharmacy information from pharmacies; information about prescribed medications from healthcare professionals (such as the name of a medication prescribed during a telehealth session); and users' geographic location information from a third-party vendor that approximates geolocation based on IP address. FTC Complaint ¶ 111.

The FTC then spends only one sentence on the patient-centered requirement of the definition, explaining that "GoodRx lets users keep track of their personal health information, including to save, track, and receive alerts about their prescriptions, refills, pricing, and medication purchase history.

Is GoodRx a PHR Vendor?

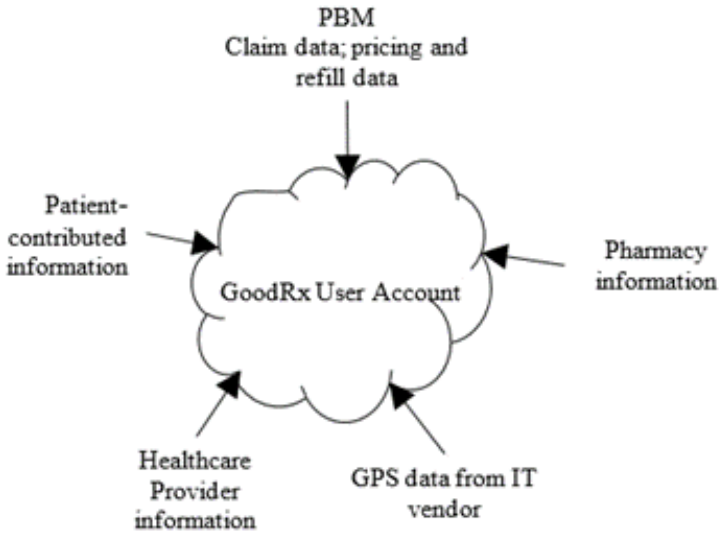
Even if the platform is a PHR, GoodRx must be considered a "PHR vendor" for the rule to apply. "PHR vendor" is defined in the rule as an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that offers or maintains a personal health record. 16 C.F.R. 318.2(j).

As a general matter, a developer of a consumer-facing health application is not regulated by HIPAA if it makes the app directly available to, and on behalf of, the end user, without the direction or involvement of a covered entity (i.e., a health care provider, health plan, or clearinghouse) or a business associate of a covered entity. This appears to be the case for GoodRx, which enables users to independently sign up to use the platform without involving a HIPAA-regulated entity that has an existing relationship with the user. The sourcing of information from pharmacies and telehealth providers (typically covered entities) and PBMs (typically business associates) is done on behalf of the user, not the pharmacy or PBM.

The above analysis holds true even though GoodRx facilitates telehealth services through a subsidiary, HeyDoctor, that it acquired in 2019 and rebranded as GoodRx Care. The fact that GoodRx Care presumably acts as a business associate of telehealth providers does not change the fact that GoodRx's core prescription coupon service is maintained on behalf of the customer. (Readers looking for additional discussion of this topic can review OCR's Health App Scenarios & HIPAA Guidance document which it released in 2016.)

Lessons Learned

The GoodRx saga demonstrates the FTC willingness to make good on its earlier warning to the developer industry and its comfort with broadly interpreting the HBNR to cover patient-centric platforms that are sector-specific and more limited than traditional notions of a PHR. And the complaint makes clear that even a more limited platform like GoodRx involves a sprawling data collection effort that ingests and synthesizes information from various sources throughout the healthcare and IT industries.



Developers creating similar apps that are offered directly to users and that consume IIHI from other sources should carefully review the HBNR to determine its applicability. Such developers should also consider implementing targeted policies and

procedures to ensure alignment between the company's data-sharing practices, its user consent process, and the company's representations in privacy policies and elsewhere.

Only time will tell if the GoodRx enforcement action signals an era of increased FTC enforcement of the HBNR. But there are reasons to think that may be the case. In an effort to empower individuals to interact with their health information, including through mobile apps, the 21st Century Cures Act introduced information blocking rules and API requirements. While this may usher in a golden age of consumer-focused health apps, developers should expect increased scrutiny by enterprising investigators. And as the Consumer Reports investigation makes clear, not all press is good press, especially when the FTC is watching.
