Davis Polk

FTC brings first enforcement action under Health Breach Notification Rule against GoodRx

February 9, 2023 | Client Update | 4-minute read

In its first enforcement action under the Health Breach Notification Rule, the Federal Trade Commission (FTC) underscores its focus on sensitive health information and imposes a permanent ban on sharing such data for targeted advertising purposes.

Background

On February 1, 2023, the FTC filed an eight-count complaint against GoodRx Holdings Inc. (GoodRx), a digital healthcare company, for sharing its customers' health information with third-party advertisers without the customers' knowledge or consent. In addition to Section 5(a) of the FTC Act, the complaint invokes for the first time alleged violations of the Health Breach Notification Rule (HBNR). Promulgated in 2009, the HBNR requires any "vendor of personal health records" to notify individuals when the security of their individually identifiable health records has been breached. The allegations follow a September 2021 FTC policy statement warning health apps and "connected device companies" that they must comply with the HBNR. The proposed order resolving the enforcement action imposes a $1.5 million civil penalty and a first-of-its-kind ban on sharing health information with third parties for targeted advertising purposes. The FTC voted 4-0 in support of the action, with a concurring statement issued by Commissioner Christine S. Wilson.

GoodRx's alleged practices

GoodRx offers discounted prescriptions and telehealth services via its website and mobile app and collects a range of sensitive data from its customers, including information about health conditions and medications. According to the FTC, GoodRx violated Section 5(a) of the FTC Act by sharing this data with third-party advertising companies and platforms despite representations to the contrary. Among other things, the FTC also alleges that (i) GoodRx failed to restrict third-party use of customer data in accordance with its own policy; (ii) misrepresented that it adhered to the Digital Advertising Alliance's principles; (iii) misrepresented that it complied with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) by displaying a seal that stated, "HIPAA Secure. Patient Data Protected"; (iv) failed to implement sufficient policies and procedures governing its customers' health information; and (v) failed to notify its customers that identifiable health information had been shared with third parties in violation of the HBNR. Under the terms of the proposed order, GoodRx neither admits nor denies the allegations in the complaint.

Injunctive relief

The proposed order, which remains subject to court approval, requires GoodRx to pay a $1.5 million civil penalty and prohibits multiple use cases for sharing health information with third parties. As noted above, the order permanently bans GoodRx from sharing health information with third parties for targeted advertising purposes. The order also prohibits sharing of health information with third parties for any purpose without affirmative, express consent of the customer. The

requisite consent is defined as “any freely given, specific, informed and unambiguous indication of an individual’s wishes demonstrating agreement by the individual, such as by a clear affirmative action” following clear and conspicuous disclosure (defined separately).

The proposed order, which has a 20-year term, also imposes a series of compliance obligations and accountability mechanisms, including:

- **Mandated privacy program.** GoodRx must implement a comprehensive privacy program, including written safeguards that control for internal and external risks to protect the privacy and security of customer information, within 180 days of entry of the order. GoodRx must also designate a qualified employee to be responsible for the program and to report directly to the CEO.
- **Independent assessments.** GoodRx must obtain periodic evaluations of the privacy program from an independent, third-party assessor with a mandate to identify any gaps or weaknesses or material noncompliance with program requirements.
- **Executive certifications.** GoodRx must provide the FTC with annual statements from a senior corporate manager regarding the company’s implementation of and compliance with all terms of the order.

Key takeaways

The GoodRx enforcement action offers several key takeaways for companies that collect sensitive information, including health information.

- The FTC’s invocation of the HBNR – and its application of the HBNR’s “breach of security” provisions to intentional sharing of information – reflects the FTC’s focus on sensitive health information as an enforcement priority.
- The ban on sharing health information for targeted advertising purposes and the substantive limit imposed upon sharing of such information for other purposes indicates the FTC’s heightened expectations for companies operating in the health space, particularly companies that are not subject to HIPAA. This case follows a similar action against Flo Health, Inc. in 2021.
- A comprehensive privacy program and related compliance obligations are increasingly standard features in FTC enforcement actions involving consumer data. For example, many of the discrete elements of the mandated privacy program in the proposed order are similar to the privacy program Twitter was required to establish to resolve its FTC enforcement action in May 2022. As a result, this latest action provides valuable signal on the FTC’s views on sound privacy practices.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Martine M. Beamon
+1 212 450 4262
martine.beamon@davispolk.com

Angela T. Burgess
+1 212 450 4885
angela.burgess@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

James W. Haldin
+1 212 450 4059
james.haldin@davispolk.com

Paul J. Nathanson
+1 202 962 7055
+1 212 450 3133
paul.nathanson@davispolk.com

James P. Rouhandeh
+1 212 450 4835
rouhandeh@davispolk.com

Michael Scheinkman
+1 212 450 4754
michael.scheinkman@davispolk.com

Howard Shelanski
+1 202 962 7060
howard.shelanski@davispolk.com