Published on *The National Law Review* https://natlawreview.com

FTC Brings Enforcement Action under FTC Act and Health Breach Notification Rule Based on GoodRx's Use of Advertising Tracking Technology on Its Websites and Mobile Application

Article By:

Brian G. Cesaratto

On February 1, 2023, the FTC announced a proposed $1.5 million settlement with GoodRx Holdings, based on alleged violations of the Federal Trade Commission Act ("FTC Act") and Health Breach Notification Rule ("HBNR") for using advertising technologies on its websites and mobile app that resulted in the unauthorized disclosure of consumers' personal and health information to advertisers and other third parties. On the same day, the U.S. Department of Justice, acting on behalf of the FTC, filed a Complaint and Proposed Stipulated Order detailing the FTC's allegations and the terms of the proposed settlement.

The HBNR was initially passed in 2009 but had never been enforced until now. In general, it requires that non–HIPAA-covered vendors of personal health records ("PHR") give notice in the event of a "breach of security," which is defined to include "unauthorized acquisition" of PHR. We have previously written about the FTC's guidance in 2021 that it intended to enforce the HBNR where health apps violated the rule. We have also previously written about the U.S. Health and Human Service's recent bulletin cautioning HIPAA-covered entities in their use of cookies, pixels, and other tracking technology to ensure that Protected Health Information (PHI) is not disclosed to third parties in violation of HIPAA. The GoodRx settlement shows that the FTC is also scrutinizing the use of advertising cookies and pixels on websites that collect personal health information. The FTC Act generally prohibits unfair or deceptive business practices, including misrepresentations or deceptive omissions concerning uses made of consumers' personal information.

Turning to the substance of the allegations, the FTC claims that GoodRx—a provider of services that allegedly allows individuals to compare prescription pricing at nearby pharmacies on its mobile application or on its website—"integrated third-party tracking tools from Facebook, Google, Criteo, and other third parties into its websites and Mobile App," which collected and sent personal data to third parties for "advertising, data analytics, or other business services." The information alleged to have been shared with third parties included contact information, persistent identifiers, location information, and "Events Data" (e.g., pages views that may have reflected the consumers' health concerns). Notably, GoodRx was also alleged to have tracked and shared "Custom Events" through the Facebook Pixel that conveyed health information about its website users, including medication

names and health conditions. And while GoodRx's privacy policy described the use of third-party tracking tools, it also stated: "we never provide advertisers or any other third parties any information that reveals a personal health condition or personal health information." The FTC also alleged that GoodRx monetized its violations by sharing the sensitive information with third parties so that it could target users with health related advertisements.

According to the FTC's Complaint, GoodRx violated the FTC Act by, among other things, disclosing personal and health information to third parties while representing in its privacy policies that it would "never" share such information with advertisers or other third parties. The FTC alleged that GoodRx also violated the FTC Act by deceptively stating in its privacy policies that disclosure to third party providers was limited to what was necessary to provide telehealth services, unless the consumer consented to other uses. The Complaint alleges that GoodRx failed to comply with the HBNR by failing to report these unauthorized disclosures.

The FTC's enforcement action against GoodRx and proposed settlement shows that non-HIPAA covered entities collecting health-related information should understand the technologies used on their websites and in their mobile applications and ensure that their privacy policies accurately reflect their collection, use and disclosure of such information using those technologies. The failure to properly disclose information sharing practices could be a violation of the FTC Act and in any event, lead to an investigation and/or enforcement action. The FTC's action also highlights the FTC's interpretation of "breach of security" under the HBNR, to potentially include the disclosure of health-related information through the use of third party advertising technology on a website or through a mobile application without appropriate consumer authorization. The FTC's action is, as we have previously discussed, part of a wider national and international privacy landscape that is increasingly focused on regulating the collection and use of personal information through web-based technologies and software that may not be readily apparent to the user.

National Law Review, Volume XIII, Number 38