March 16, 2023

FTC Gets Serious About Healthcare Data Sharing—Brings First-of-Its Kind Enforcement Action for Violating the Health Breach Notification Rule

On February 1, the Federal Trade Commission (FTC) reached a settlement with digital health platform GoodRx for sharing users' personal health information (PHI) with third parties without properly disclosing its data practices or obtaining users' affirmative consent, as well as for failing to maintain adequate policies or procedures to protect users' PHI. This is the FTC's first-ever enforcement action under the Health Breach Notification Rule, which requires vendors of personal health records (PHRs) and certain PHR-related entities to notify consumers, the FTC and sometimes the media about discovery of certain data breaches.

The FTC's Complaint

GoodRx operates a telemedicine platform and a mobile app that track prescription drug prices in the United States and provide drug coupons for discounts on certain medications. In doing so, GoodRx collects personal information, including PHI, from users. The FTC's complaint charges GoodRx with violating Section 5 of the FTC Act and the Health Breach Notification Rule. Specifically, and among other things, the complaint alleges that GoodRx (1) deceived consumers by sharing their sensitive health information for targeted advertising purposes in violation of the representations it made in its privacy policy and other public statements, (2) did not limit third parties' use of the data, (3) used health information to target consumers with ads without first obtaining their consent, and (4) did not implement policies to protect personal information, including but not limited to PHI. As of the date of this article, GoodRx and the FTC have proposed to settle the allegations. The settlement would require GoodRx to agree to a consent order requiring numerous modifications to its data collection and use practices and would require a penalty payment of $1.5 million.

Focus on Deceptive Practices

The crux of the complaint focuses on the allegedly deceptive statements in GoodRx's privacy policy between 2017 and 2020 in which the company made the claim that it "never provide[s] advertisers any information that reveals a personal health condition." The FTC alleges that this statement was both false and deceptive because GoodRx, like so many other online applications and websites, used advertising tracking technologies such as cookies and pixels from popular services like Facebook. The FTC further alleges that these trackers transferred the Internet protocol addresses, names, browsing analytics, medications and health condition information of GoodRx users without their consent and in a manner inconsistent with the privacy policy. Using this transferred information, Facebook, Google and other advertisers obtained access to data that was allegedly sufficient to construct highly personal profiles of GoodRx users based on their health information, medical diagnoses and lifestyles. This allowed these advertisers to target users, such as through Instagram and Facebook, with ads related to their medications, health conditions or health profiles. The FTC also alleges that multiple statements GoodRx made to users were deceptive. Such alleged statements include a claim that the company was compliant with Digital Advertising Alliance principles and the use of a Health Insurance Portability and Accountability Act (HIPAA) compliance seal on its website. Since GoodRx is not subject to HIPAA, the FTC alleges that the seal created the misimpression that data was handled in accordance with HIPAA.

Expanding the Concept of a Data Breach

In the normal course, many individuals and companies think of a "data breach" as requiring involvement of a bad actor (e.g., for ransomware, a hack, phishing, theft) or an unfortunate, unintentional incident (such as a lost laptop). However, in this GoodRx matter, a novel application of the Health Breach Notification Rule, the FTC found that GoodRx's disclosures of personal information via advertising trackers were in fact "breaches" that GoodRx failed to report. This expanded interpretation of the Health Breach Notification Rule may indicate more FTC enforcement focused on the digital health industry, including health and fitness applications and activity and health status trackers.

Lessons for Healthcare Companies

This enforcement action and settlement are striking reminders to healthcare companies that words—including your privacy policy, your terms of use, your marketing materials and your compliance statements—matter. Companies should use this GoodRx issue as a reminder to:

- fully understand your company's data flows and how different departments at your organization (e.g., marketing) are collecting, using and disclosing personal data;
- ensure your website and application privacy policies and terms of use are current and accurate;
- avoid using "off the shelf" or stock privacy policies and terms of use without carefully customizing them and examining them for consistency with your actual data practices;
- examine and confirm the accuracy of your marketing statements and representations to customers; and
- reassess referencing compliance with HIPAA if you are not subject to HIPAA.

Day Pitney's Healthcare, Life Sciences and Technology practice group can assist you in all matters concerning HIPAA, FTC enforcement against healthcare companies and the development of accurate and compliant privacy policies and terms of use. Please reach out if you have any questions.

Would you like to receive our *Day Pitney C.H.A.T. Newsletter?* Sign up here.

Authors



William J. Roberts
Partner

Hartford, CT | (860) 275-0184

wroberts@daypitney.com



Colton J. Kopcik
Associate

Washington, D.C. | (203) 977-7362

ckopcik@daypitney.com