STRATEGIC MANAGEMENT SERVICES

FTC Enforcement of the Health Breach Notification Rule

Lisa Shuman | May 2023

The Federal Trade Commission (FTC) for the first time has taken enforcement action under its Health Breach Notification Rule against GoodRX Holdings Inc., the telehealth and prescription drug discount provider. The FTC action, announced February 2023, included a $1.5 million civil penalty, along with requirements that GoodRx (a) Permanently be banned from disclosing health information to third parties for advertising; (b) Be prohibited from misrepresentations; (c) Require affirmative express consent and notice for sharing health information for other non-advertising purposes; (d) Comply with the FTC's Health Breach Notification requirements; (e) Post a notice to users; (f) Direct third parties to delete consumer health data that was shared; (g) Implement and maintain a comprehensive privacy program; and (h) Obtain initial and biennial privacy assessments by a third-party assessor for 20 years.

The FTC stated GoodRX violated the Health Breach Notification Rule by (a) Failing to notify consumers, FTC and media of unauthorized disclosures of individually identifiable health information; (b) Sharing its users' personal health information with third party advertising companies (Facebook, Google, Criteo, Branch and Twilio); (c) Using its users' personal health information to target its users with health related advertisements on Facebook and Instagram; (d) Allowing third parties to use personal health information for their own internal purposes, including to improve advertising; (e) Falsely representing to consumers that GoodRX complied with HIPAA; and (e) Failing to maintain policies and procedures to protect its users' personal health information.

This action was under the authority provided by Section 5 of the FTC Act, which "prohibits companies from misleading consumers or engaging in unfair practices that harm consumers," and the Health Breach Notification Rule issued in 2009, which requires certain organizations not covered by HIPAA to notify their customers, the FTC, and in some cases the media, if there is a breach of unsecured individually identifiable health information. This applies to vendors of

personal health records (PHRs), a PHR-related entity, or a third-party service provider for a vendor of PHRS or PHR related entity.

More recently, in March 2023 the FTC fined BetterHelp, an online therapy company, for sharing consumer data, including sensitive mental health information, to Facebook and Shapchat for advertising purposes. The $7.8 million fine will be used to provide partial refunds to consumers who signed up for and paid for BetterHelp's services between August 1, 2017, and December 31, 2020.

In September 2021, FTC issued a policy statement clarifying that health apps and connected devices that collect or use consumers' health information must comply with the FTC's Health Breach Notification Rule. In December 2022, the HHS Office for Civil Rights (OCR) issued a bulletin summarizing the obligations of covered entities and business associates when using online tracking technologies. Further, a February 2023 press release from the DOJ states they are "committed to enforcing protections against deceptive practices and unauthorized disclosure of personal health information.".

Organizations that are subject to FTC regulations should ensure that they comply with the regulations and have implemented a privacy program with adequate policies and procedures to protect individually identifiable health information. Companies that violate the FTC's Health Breach Notification Rule could be subject to a civil penalty of up to $50,120 per violation. Each violation of the Rule will be treated by the FTC as an unfair or deceptive act or practice in violation of an FTC regulation.

For more information on other privacy related topics, contact Lisa Shuman (lshuman@strategicm.com).

Keep up-to-date with Strategic Management Services by following us on LinkedIn

About the Author

Ms. Shuman assists health care organizations to develop, implement and evaluate their compliance programs and HIPAA privacy programs. Ms. Shuman specializes in our firm's HIPAA Privacy services, including leading privacy investigations, breach risk assessments, breach notification letters, breach reporting to the Office for Civil Rights and corrective actions plans. She specializes in serving as Interim Privacy Officer for large health care systems, managed care organizations, comprehensive cancer center and health care business associate.