FTC Enforces Health Breach Notification Rule for the First Time

GoodRx, a prescription drug discount service provider, faces $1.5 million in civil penalties for disclosing individuals' health data to advertisers and advertising platforms such as Facebook and Google. User data, alleged to have included information about prescription medications and underlying health conditions, apparently was provided to companies like Facebook and Google through various web tracking tools and was then used to send targeted advertisements to those users. According to the Commission's press release, approximately 55 million consumers have visited or used GoodRx's website or mobile applications since 2017, either to access prescription drug discounts, or to make arrangements for telehealth visits and other health services.

This is the FTC's first ever action to enforce the 2009 Health Breach Notification Rule (the "Rule") (16 C.F.R. § 318). In addition to imposing a significant fine, the FTC permanently restrains GoodRx from disclosing health information to third parties for advertising purposes.

Following the FTC's announcement of the GoodRx enforcement action, the company now faces a class action lawsuit alleging that GoodRx breached state privacy laws by sharing end-user health data with advertisers. The lawsuit was filed in the Northern District of California on February 2, 2023.

What does this signal?

This enforcement effort, when viewed in combination with the OCR guidance issued in December 2022 regarding tracking technologies deployed by HIPAA Covered Entities and Business Associates, signals a significant shift on the part of the federal government to utilize its enforcement authority to limit otherwise ubiquitous web tracking tools, particularly where health information is involved. Both the OCR Guidance and the FTC's announcement of the Good Rx enforcement action also call out concerns on the part of the federal government that these tools might be used against women seeking reproductive health services that are being subjected to limitations, if not outright bans, by states after the *Dobbs* decision.

What is the rule and who is impacted?

The Rule prohibits the unauthorized disclosure of personal health data and imposes an obligation on companies to notify consumers if their data is exposed or shared without their permission. The FTC can enforce the rule when a company fails to notify consumers and others of unauthorized disclosures of consumers' personal health information. The Rule applies to foreign and domestic vendors of personal health records, personal health record related entities, and third party service providers (each defined at 16 C.F.R. § 318) that maintain information about U.S. citizens or residents. Types of companies subject to the Health Breach Notification Rule include, for example, mobile health applications that track medications, fertility, sleep, mental health, and diet.

The FTC previously offered guidance about the applicability of the Health Breach Notification Rule, but had yet to enforce it until the February 1, 2023 GoodRx filing.

What should companies do to avoid finding themselves in trouble with the FTC?

The GoodRx complaint does not just ban GoodRx from disclosing health information for advertising purposes. It lays out nearly a dozen specific orders. Companies subject to the Rule may want to reassess several points in light of this new enforcement effort.

- *Misrepresentations (Explicit or Inadvertent)* – Companies subject to the Rule must not misrepresent to whom they disclose and/or how they collect, maintain or use health data from end-users. Additionally, companies should be careful when publicizing on their websites that they are "HIPAA compliant" or otherwise sponsored by a standard-setting organization (e.g., Digital Advertising Alliance) if such a statement has not been evaluated and determined to be factually correct.

- *Affirmative Express Consent and Notice* – Companies that intend to disclose end-user health data to a third party must provide a clear notice that states the categories of health information that will be disclosed, the identities of the third parties that will receive the data, and the purposes for which the information is being disclosed. As a result, companies should review their Terms of Use, Privacy Policies, and any other end-user enrollment/sign-up procedures to ensure that this information is clearly and conspicuously made available to the end-user.

- *Health Breach Notifications* – Companies should evaluate their processes and procedures to ensure that any notifications required by the Rule are made in a timely manner following a breach of unsecured end-user health data, including notices to individuals, the FTC, and prominent media outlets, if applicable. The FTC provides information about these regulatory obligations, including a standard reporting form, on its website.

- *Evaluate Your Privacy Program* – Any business that collects, maintains, uses, discloses, or otherwise has access to health data implicated by the Rule is required to establish, implement, and maintain a comprehensive privacy program. This includes designing safeguards, such as policies, procedures, and technical measures that control internal and external risks to the privacy, security, availability, confidentiality, and integrity of health data.

- *Privacy Assessment by a Third Party* – Privacy policies and procedures should be reviewed and revised on an annual basis. Companies subject to the Rule may want to consider obtaining periodic assessments from a qualified, independent third party professional to review the company's privacy program. Findings from the third party assessor should then be reviewed and any deficiencies remediated by a designated individual within the company.

- *Covered Incident Reports* – Companies should maintain an incident log for each security incident. The log should record the date when the incident occurred, a description of facts relating to the incident, including causes and scope, the number of end-users or employees affected, and steps taken to remediate the incident.

In sum, the complaint filed against GoodRx signals the FTC's sharpened focus on direct-to-consumer health care mobile applications and websites that share data with third parties. Such businesses should carefully review their data privacy and security practices, and regularly evaluate whether their public-facing notices appropriately reflect how this data is being used.

If you have questions about these developments, please contact one of the following attorneys.

Adam J. Bookbinder
Co-Chair
617-248-4806 | abookbinder@choate.com

Julia R. Hesse
Co-Chair
617-248-5006 | jhesse@choate.com

Christine G. Savage
Co-Chair
617-248-4084 | csavage@choate.com

Sara E. Rau
Senior Associate
617-248-4720 | srau@choate.com