DORSEY
DORSEY+WHITNEY LLP

FTC Takes First Enforcement Action for Violation of the Health Breach Notification Rule – A Federal Health Privacy Rule Beyond HIPAA

March 21, 2023 – The TMCA
by Elise Brazelton and Ross C. D'Emanuele

On February 1, 2023, the Federal Trade Commission (FTC) filed a complaint in the U.S. District Court for the Northern District of California alleging that digital health platform GoodRx violated the FTC Act by repeatedly sharing personal health information with advertising companies and platforms, such as Facebook and Google, and failed to report the unauthorized disclosures pursuant to its Health Breach Notification Rule (16 C.F.R. § 318). Though GoodRx maintains that it shared all health information appropriately, according to the proposed stipulated order, the digital health platform has agreed to pay a $1.5 million civil penalty. Once the proposed order is approved by a federal court judge, the monetary penalty, as well as several non-monetary sanctions, will go into effect. This settlement may signal the beginning of a new era of health privacy enforcement, where the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is not the only federal health privacy law for which organizations must ensure compliance.

The FTC's Health Breach Notification Rule is not new—even though the GoodRx complaint marks its first enforcement action. The rule went into effect in September 2009 and was the subject of a 2021 FTC policy statement. Substantively, the Health Breach Notification Rule is very similar to HIPAA's Breach Notification Rule (45 C.F.R. §§ 164.400-414). Pursuant to both rules, a data holder must notify the subject of any unsecured "individually identifiable health information" and the agency responsible for enforcing the applicable rule in response to a breach of such information. Also pursuant to both rules, if a breach of unsecured personal health

Related People

- Elise Brazelton
- Ross C. D'Emanuele

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

information involves more than 500 individuals (and, in the case of the Health Breach Notification Rule, if a breach involves exactly 500 individuals), the data holder must notify the media.

The primary differentiating factor between the rules are the types of entities to which they apply. The HIPAA Breach Notification Rule is specific in scope and only applies to Covered Entities and their Business Associates. A Covered Entity is limited to a: (1) health plan, (2) health care clearinghouse, or (3) health care provider, who also electronically transmits health information in connection with transactions for which HHS has adopted standards. A Business Associate is a person or entity who, on behalf of a Covered Entity, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information.

The FTC's Health Breach Notification Rule is broader in scope and applies to all vendors that "offer or maintain a personal health record (PHR)." A PHR is an electronic record of "individually identifiable health information," as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual. The FTC has stated that an example PHR Vendor might be a health app that collects information from consumers and can sync with a consumer's fitness tracker.

The Health Breach Notification Rule also applies to "PHR related entities" and "third-party service providers." A PHR Related Entity interacts with a PHR Vendor by either offering products or services through the Vendor's website, offering products or services through a Covered Entity's website that offers individual's health records, or by accessing information in a PHR or sending information to a PHR. The FTC states that an example of a PHR Related Entity might be a company that offers a fitness tracker and sends information to health apps. A Third Party Service Provider is an entity that provides services to a PHR Vendor in connection with the offering or maintenance of a PHR or to a PHR Related Entity in connection with a product or service offered by that entity; and accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services. The FTC states that an example of a Third Party Service Provider might be a company that provides billing, debt collection, or data storage services relating to health information for a PHR.

In light of the GoodRx complaint and the FTC's enforcement of the Health Breach Notification Rule, all entities that utilize or maintain personal health information—and

especially those offering healthcare apps, connected devices, and wearables, that often do not fall under the definitions of Covered Entities and Business Associates—should evaluate the applicability of the Health Breach Notification Rule to their organization and its business practices. Entities that fall under the definitions of PHR Vendor, PHR Related Entity, and Third Party Service Provider, should be sure to have an effective privacy and security program in place, including procedures for conducting regular risk assessments and risk management trainings to ensure proper identification of and response to a breach of personal health information. Such entities should also review their privacy policies, both internally and externally-facing, to ensure they reflect current data-sharing practices, and should review their vendor contracts to take inventory of any permissions or restrictions on how personal health information is used and disclosed to ensure they are obtaining the necessary consent.

For more information on the Health Breach Notification Rule, the FTC's Health Privacy webpage offers a variety of resources—including a simplified explainer of the rule, compliance tips, and an interactive tool geared toward mobile health apps.