ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy / Consumer Protection/FTC ADVISORY ■

FEBRUARY 10, 2023

Limit Your Health Data Sharing and Call Me in the Morning: FTC Prescribes Enforcement of the Health Breach Notification Rule for the First Time

By **Kathleen Benway**, **David C. Keating**, *and* **Sara Pullen Guercio**

In a warning shot to businesses that collect personal health data online, the U.S. Department of Justice filed a complaint and proposed stipulated order on behalf of the Federal Trade Commission (FTC) on February 1, 2023, alleging that GoodRx Holdings Inc., a telehealth and prescription drug discount provider, violated Section 5 of the FTC Act and the FTC's Health Breach Notification Rule (HBNR). According to the complaint, GoodRx shared personal data revealing health information about GoodRx users with third-party digital advertising and analytics providers in a manner that violated GoodRx's own privacy policy and resulted in a breach of security, as defined under the HBNR. The FTC also alleged that using and sharing personal health information without first obtaining consumers' express informed consent is unfair under Section 5.

The proposed order includes, among other things, a $1.5 million civil penalty; requirements to establish a comprehensive privacy program, undergo biennial third-party compliance assessments, and self-report violations for the next 20 years; and a permanent injunction against future disclosures of health information, subject to certain limited exceptions. Each of the four sitting commissioners voted in favor of filing the complaint and the order, but the order must still be approved by the court.

The FTC is making a clear statement to businesses that collect health-related personal data from individuals online or via mobile apps that they must carefully manage and limit the use and sharing of health data in connection with digital advertising, ensure their privacy policies align with those practices, and scrutinize the use of common digital advertising and analytics technologies embedded in their websites and apps to avoid potential liability under the FTC Act and HBNR.

The FTC's Health Breach Notification Rule

The American Recovery and Reinvestment Act of 2009 included the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was intended to strengthen privacy and security standards for health information. In part, the HITECH Act empowered the FTC to promulgate a rule requiring vendors of personal health records and related entities to notify affected persons and the FTC if there is a breach of security involving identifiable health information contained in personal health records.

The Health Breach Notification Rule, promulgated by the FTC in August 2009, applies to entities *that are not subject to HIPAA* and that are vendors of personal health records, related entities, or their third-party service providers. A "personal health record" is an electronic record containing individually identifiable health information "that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." The FTC has not made changes to the HBNR since it was originally promulgated. But in May 2020, as part of its regular rule review process, the FTC sought public comment on whether it should consider any changes to the HBNR. The FTC received 28 comments in response to its request, but it has not proposed any changes.

The HBNR requires applicable vendors to notify the FTC, impacted persons, and (when more than 500 individuals are impacted) the media of any breaches of security of identifiable health information contained in a personal health record. In most cases, notice must be provided within 60 days after discovery of the breach.

The FTC previously provided insight into applicability of the HBNR. The FTC published a Statement on Breaches by Health Apps and Other Connected Devices in September 2021 that warned businesses that collect personal health data online that they may qualify as applicable vendors. In a guidance document released in January 2022, the FTC further explained that "a 'breach' [under the HBNR] is not limited to cybersecurity intrusions or nefarious behavior by hackers or insiders. Incidents of unauthorized access, including a company's disclosure of covered information without a person's authorization, triggers notification obligations under the [HBNR]."

FTC Enforcement Against GoodRx

GoodRx provides a platform where users can compare drug prices at different pharmacies and obtain coupons for discounted pharmaceutical products. GoodRx's affiliate, HeyDoctor/GoodRx Care, also provides primary care telehealth services.

The FTC alleged that from 2017 to 2020, GoodRx and HeyDoctor used commonplace digital tracking technologies on their websites that captured identifiable health information such as name, email address, IP address, persistent identifiers, prescription purchases, and health conditions for millions of users and transmitted this information to third-party digital advertising and analytics providers. GoodRx did not prohibit these platforms from using that information for their own internal purposes, such as to build or enhance consumer profiles and optimize their analytics technologies for use on behalf of their other customers.

GoodRx also used the information to create consumer profiles, some of which overtly indicated a consumer's medications, health conditions, and location. The profiles were loaded into a social network's ad manager for GoodRx to use targeted ads to market its products and services to consumers. For example, the complaint notes that if a consumer visited an informational page on erectile dysfunction on GoodRx's website, the consumer might be shown an advertisement for a GoodRx coupon for Viagra on their feed.

The FTC alleged in the complaint that these practices were inconsistent with various representations GoodRx and its affiliates had made in their privacy policies, such as "we never provide advertisers or any other third parties any information that reveals a personal health condition or personal health information." The complaint alleges that GoodRx's practices violated these representations and that GoodRx therefore engaged in deceptive trade practices in violation of Section 5 of the FTC Act. The FTC also considered GoodRx's practices of collecting sensitive health information and sharing it with third parties *without notice or consent* from consumers to be a breach of security under the HBNR. GoodRx failed to provide notice of the breach of security to the individual consumers, the FTC, and the media, as required by the HBNR.

According to the complaint, GoodRx further represented in the marketing and delivery of its services that it was HIPAA-compliant and that it adhered to the self-regulatory principles of the Digital Advertising Alliance. But, according to the complaint, these representations were false and constituted deceptive acts or practices in violation of Section 5 of the FTC Act.

The FTC voted 4–0 to refer the complaint and order to the Department of Justice for filing. Commissioner Christine S. Wilson also released a concurring statement that applauds the FTC for its enforcement but expresses her disappointment that the civil penalty was not larger and also notes the order "does not hold senior executives liable, and does not modify the core GoodRx business model."

Takeaways

Health privacy is a priority focus area for regulators. The FTC's first enforcement of the HBNR signals a focus on safeguarding sensitive health information, regardless of whether an entity is subject to HIPAA. The FTC's position in the 2021 statement also highlights the FTC's desire to apply the HBNR to all entities collecting health information that are not subject to HIPAA. The December publication by the U.S. Department of Health and Human Services of a guidance document on the use of digital advertising and analytics technologies strongly suggests a level of cross-agency coordination in this area.

The use of health-related information for digital advertising is subject to significant conditions and restrictions. The use of sensitive health-related data for digital advertising requires careful review and evaluation to determine what disclosures are necessary and whether affirmative express consent is required. The failure to ensure transparency and secure such consent in an effective manner, where required, can expose health care and other businesses to significant liability risks. In addition, like all businesses handling consumers' personal information, companies that collect, use, and share health data must be sure that their privacy policies and public-facing statements about their use of that data are accurate.

The use of digital advertising and analytics technologies online and in mobile apps by businesses that collect personal health data is subject to heightened scrutiny. Many businesses deploy sophisticated digital tracking technologies online through digital marketing teams, with limited or no input from internal privacy and legal teams. A scan of the typical website will reveal multiple advertising and analytics cookies, pixels, and other trackers. Mobile apps routinely embed third-party software development kits (SDKs) that send data about app operations to third-party vendors. This enforcement action makes clear that businesses that collect health-related personal data from individuals online or via mobile apps need to understand what cookies, pixels, and other tracking scripts and code are implemented on those sites and apps, what data these tools collect and transmit, and what contractual protections are in place with relevant third-party vendors. This is technical, time-consuming work – but it is critical in light of the current regulatory and enforcement environment.

You can subscribe to future ***Privacy, Cyber & Data Strategy*** and ***Consumer Protection/FTC*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Privacy, Cyber & Data Strategy Team

David C. Keating
+1 404 881 7355
+1 202 239 3921
david.keating@alston.com

Kimberly Kiefer Peretti
+1 202 239 3720
kimberly.peretti@alston.com

Angie Burnette
+1 404 881 7665
angie.burnette@alston.com

Maki DePalo
+1 404 881 4280
maki.depalo@alston.com

Kellen Dwyer
+1 202 239 3240
+1 212 905 9340
kellen.dwyer@alston.com

Daniel J. Felz
+1 404 881 7694
daniel.felz@alston.com

Katherine Doty Hanniford
+1 202 239 3725
kate.hanniford@alston.com

Amy Mushahwar
+1 202 239 3791
amy.mushahwar@alston.com

Karen M. Sanzaro
+1 202 239 3719
karen.sanzaro@alston.com

Sara Pullen Guercio
+1 404 881 4726
sara.guercio@alston.com

Consumer Protection/FTC Team

Kathleen Benway
+1 202 239 3034
kathleen.benway@alston.com

Kelly Connolly Barnaby
+1 202 239 3687
kelly.barnaby@alston.com

Alexander G. Brown
+1 404 881 7943
alex.brown@alston.com

Kristine McAlister Brown
+1 404 881 7584
kristy.brown@alston.com

Joseph H. Hunt
+1 202 239 3278
+1 404 881 7811
jody.hunt@alston.com

T.C. Spencer Pryor
+1 404 881 7978
spence.pryor@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ +1 404 881 7000 ■ Fax: +1 404 881 7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ +1 704 444 1000 ■ Fax: +1 704 444 1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ +1 214.922.3400 ■ Fax: +1 214.922.3899
FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ +1 214 922 3400 ■ Fax: +1 214 922 3899
LONDON: 4th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44 0 20 3823 2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ +1 213 576 1000 ■ Fax: +1 213 576 1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ +1 212 210 9400 ■ Fax: +1 212 210 9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ +1 919 862 2200 ■ Fax: +1 919 862 2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ +1 415 243 1000 ■ Fax: +1 415 243 1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ +1 650 838 2000 ■ Fax: +1 650 838 2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ +1 202 239 3300 ■ Fax: +1 202 239 3333