AN A.S. PRATT PUBLICATION
JULY-AUGUST 2023
VOL. 9 NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 6** **July - August 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2023–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Limit Your Health Data Sharing and Call Me in the Morning: Federal Trade Commission Prescribes Enforcement of the Health Breach Notification Rule

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

In this article, the authors discuss recent developments that indicate that health privacy is a priority focus area for federal regulators.

In a warning shot to businesses that collect personal health data online, the U.S. Department of Justice has filed a complaint[1] and proposed stipulated order[2] on behalf of the Federal Trade Commission (FTC), 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 authors, attorneys with Alston & Bird LLP, may be contacted at kathleen.benway@alston.com, david.keating@alston.com, sara.guercio@alston.com and hyunjai.oh@alston.com, respectively.

[1] https://www.ftc.gov/system/files/ftc_gov/pdf/goodrx_complaint_for_permanent_injunction_civil_penalties_and_other_relief.pdf.

[2] https://www.ftc.gov/system/files/ftc_gov/pdf/goodrx_stipulated_order_for_permanent_injunction_civil_penalty_judgment_and_other_relief.pdf.

THE FTC'S HEALTH BREACH NOTIFICATION RULE

The American Recovery and Reinvestment Act of 2009[3] 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,[4] 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[5] in September 2021 that warned businesses that collect personal health data online that they may qualify as applicable vendors. In a guidance document[6] 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]."

---

[3] https://www.congress.gov/111/plaws/publ5/PLAW-111publ5.pdf.

[4] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318.

[5] https://www.ftc.gov/legal-library/browse/statement-commission-breaches-health-apps-other-connected-devices.

[6] https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0.

FTC ENFORCEMENT ACTION

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[7] that applauds the FTC for its enforcement but expresses her

[7] https://www.ftc.gov/system/files/ftc_gov/pdf/2023090_goodrx_final_concurring_statement_wilson.pdf.

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."

ANOTHER FTC ENFORCEMENT ACTION

Just one month after the announcement of the GoodRx settlement, the FTC announced a proposed administrative settlement[8] with online counseling service BetterHelp Inc. that reiterates many of the FTC's positions in *GoodRx* – most importantly, its view on sharing consumers' health information with social media companies for third-party advertising. The commissioners voted 4–0 to issue the proposed administrative complaint and consent agreement, which is subject to a 30-day public comment period after which the FTC will decide whether to make the proposed order final.

In its proposed complaint,[9] the FTC alleged that BetterHelp transmitted millions of consumers' health data, including email address, address, IP address, and enrollment status in BetterHelp services, to third-party advertising platforms without obtaining affirmative express consent from consumers. According to the complaint, some of the disclosures occurred through BetterHelp's use of digital tracking technologies, including third-party cookies and pixels. The complaint alleges that these data-sharing practices were contrary to BetterHelp's privacy representations, which indicated consumers' health information would "stay private" and not be shared with third parties for advertising purposes.

In the FTC's view, BetterHelp engaged in unfair practices in violation of Section 5 of the FTC Act. The complaint asserts that consumers could not reasonably avoid the substantial privacy injury because BetterHelp's deceptive privacy promises made it impossible for consumers to know that the company was sharing consumers' health information with third parties for advertising purposes. The complaint also notes that, until October 2021, BetterHelp did not provide a conspicuous method for consumers to opt out of tracking technologies. While the FTC alleged that BetterHelp's false statements also constituted deceptive practices, the complaint does not address whether BetterHelp's disclosure was a security breach under the HBNR.

The proposed order provides a ban on BetterHelp's disclosure of consumers' mental or physical health conditions to third parties for advertising purposes. In addition, BetterHelp will need to obtain affirmative express consent before sharing with third parties "covered information," which the order defines broadly to include online contact information and persistent identifiers. Notably, the proposed order prohibits BetterHelp from sharing covered information to serve advertisements targeting consumers who had visited or used BetterHelp, regardless of consent. The order also requires BetterHelp

[8] https://www.ftc.gov/system/files/ftc_gov/pdf/202_3169-betterhelp-consent.pdf.
[9] https://www.ftc.gov/system/files/ftc_gov/pdf/2023169-betterhelp-complaint_.pdf.

to pay affected consumers $7.8 million to settle charges. This is the first FTC action returning funds to consumers whose health data was compromised. The proposed settlement will be open for public comment for 30 days, after which the FTC will finalize the settlement.

CONCLUSION

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[10] on the use of digital advertising and analytics technologies strongly suggests a level of cross-agency coordination in this area. The enforcement against BetterHelp also shows the FTC's expansive view of the scope of health information – even email or IP address can become health information when collected in the context of businesses providing health-related services.

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. These enforcement actions make clear that businesses that collect health-related personal data from

[10] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

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, what contractual protections are in place with relevant third-party vendors, and whether it is necessary to allow consumers to opt out of these tracking technologies. This is technical, time-consuming work – but it is critical in light of the current regulatory and enforcement environment.