AN A.S. PRATT PUBLICATION
MAY 2024
VOL. 10 NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 **NUMBER 4** **May 2024**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@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*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (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

(2024–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.

So, What's "Consumer Health Data," Anyway?

By Peter A. Blenkinsop, Reed Abrahamson and Simonne Brousseau*

In this article, the authors explain how companies can meet their privacy obligations with respect to "consumer health data."

The U.S. privacy landscape has changed rapidly over the past few years. But the most significant recent changes relate to "consumer health data" – health information about identified or identifiable consumers that falls outside the scope of the Health Insurance Portability and Accountability Act (HIPAA). HIPAA regulates protected health information (PHI) collected by "covered entities" – health care providers, health plans and health care clearinghouses – and their business associates. It does not, however, regulate other health information that companies who are not covered entities or business associates collect.

That non-HIPAA-covered health information was subject to relatively light regulation before 2023. But multiple enforcement actions from the Federal Trade Commission (FTC), coupled with new state laws, have changed that significantly. These changes are best viewed as a response to increased scrutiny of online technologies that "track" consumers as well as federal and state concerns, post-*Dobbs v. Jackson*, over collection and disclosure of health information.

So, what does this all mean for industry? This article outlines the key changes from last year and discusses next steps for compliance.

FTC ENFORCEMENT ACTIONS

In February 2023, the FTC announced a settlement with GoodRx over claims that GoodRx was disclosing "health information" to third parties via cookies and other trackers.[1] The FTC alleged that GoodRx made these disclosures by sending information about its "users' prescription medications and personal health conditions," coupled with unique advertising IDs and other identifiable information to Google, Facebook and other third parties for their own marketing purposes.[2]

More specifically, the FTC was arguing that the fact that a person viewed a particular drug coupon on GoodRx's site, plus a unique identifier, constituted "health information," and that disclosures of such information allowed third parties to target consumers with

* The authors, attorneys with Faegre Drinker Biddle & Reath LLP, may be contacted at peter.blenkinsop@faegredrinker.com, reed.abrahamson@faegredrinker.com and simonne.brousseau@faegredrinker.com, respectively.

[1] https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising.

[2] See Compl., U.S. v. GoodRx Holdings, Inc., 3:23-cv-460 (N.D. Cal. Feb. 1, 2023), ¶ 4.

ads on other platforms. The FTC alleged that GoodRx's disclosure of such information without prior consent from consumers was substantively unfair under Section 5 of the FTC Act. And, for the first time ever, the FTC claimed the conduct also violated the FTC's never- before-enforced Health Breach Notification Rule. GoodRx settled with the FTC, agreeing to a $1.5 million monetary penalty and various substantive penalties, including a permanent prohibition on disclosure of health information to third parties for advertising purposes.

A month later, in March 2023, the FTC announced a settlement with online therapy provider BetterHelp over claims for unfair and deceptive practices under Section 5.[3]

Specifically, the FTC alleged that BetterHelp disclosed health information, again – unique online identifiers coupled with the fact that a consumer was interested in BetterHelp's therapy services, to Facebook and other third parties. To be clear – BetterHelp is not a HIPAA-covered entity and did not disclose mental health treatment records. But the FTC nonetheless took issue with BetterHelp's unconsented disclosures of identifiable information to third parties that allowed those entities to retarget consumers based on their interest in mental health services. The FTC also called out various privacy-related statements on BetterHelp's websites representing that BetterHelp did not sell personal information or disclose health information to third parties.

BetterHelp settled with the FTC, agreeing to pay $7.8 million in consumer refunds and accepting various substantive penalties, including (like GoodRx) a permanent prohibition on disclosure of health information to third parties for advertising purposes.

Subsequently, in May 2023, the FTC announced a settlement with fertility app Premom for violations of the Health Breach Notification Rule and Section 5.[4] Reminiscent of its 2021 enforcement action against Flo Health, the FTC alleged[5] that Premom allowed consumers to enter fertility information into its app, "falsely promised" that it would not disclose health information to third parties without consent, and then disclosed Custom App Events (such as a consumer's app sign up or ovulation test result, coupled with a unique advertising ID) to Google and other third parties via software development kits (SDKs) in its app.[6] Premom settled with the FTC and three state attorneys general, agreeing to pay $200,000 and accepting various substantive penalties, including (like GoodRx and BetterHelp) a permanent prohibition on disclosure of health information to third parties for advertising purposes.

---

[3] https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook.

[4] https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc.

[5] https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.

[6] See Compl., U.S. v. Easy Healthcare Corp., 1:23-cv-3107 (N.D. Ill. May 17, 2023), ¶¶ 2–3, 25–29.

More recently, the FTC announced settlements with data brokers X-Mode Social/Outlogic[7] (X-Mode) and InMarket Media (InMarket) in January 2024 for alleged violations of Section 5.[8]

In both cases, the FTC alleged that the data broker collected location information about consumers en masse via SDKs in mobile apps, sold that information to third parties, and failed to remove from its datasets information that facilitated inferences about consumers' visits to sensitive locations, such as health care providers and reproductive health clinics. The FTC called out the data brokers' failure to confirm that the apps using their SDKs obtained consent from consumers prior to collecting and disclosing their location data back to the data brokers. It also highlighted the data brokers' failure to enforce contractual restrictions on its customers that purport to prohibit them from using purchased location data to infer sensitive characteristics.

X-Mode and InMarket both settled with the FTC, agreeing, among other things, to delete all historic location data collected without consent, subject to a few caveats.

In early February 2024, the FTC also survived a motion to dismiss its complaint against data broker Kochava, where it has raised very similar allegations.[9]

CONSUMER HEALTH DATA LAWS

New "consumer health data" laws have also begun to pop up across the U.S. In April 2023, Washington adopted the Washington My Health My Data Act (WA MHMD Act), and in June 2023, Nevada adopted very similar legislation (collectively, the MHMD Acts). Most provisions of the MHMD Acts will go into effect on March 31, 2024, and they effectively codify the FTC's enforcement actions against GoodRx, BetterHelp and Premom. The WA MHMD Act has a private right of action, while Nevada's statute does not.

The MHMD Acts were adopted with the explicit intent to regulate health information that is not covered by HIPAA. And they sweep very broadly, defining "consumer health data" as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status," including health conditions, treatment, diagnoses, use of medication, reproductive information, biometric data, genetic data, precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies, data that identifies a consumer seeking health care services and more.[10] Importantly, "consumer health data" also includes any information processed to identify a consumer

---

[7] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

[8] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data.

[9] See Mem. Decision & Order, FTC v. Kochava, Inc., 2:22-cv-377 (D. Idaho Feb. 3, 2024).

[10] See Wash. Rev. Code § 19.373.010(8); see also Nev. Rev. Stat. § 603A(8) (similar).

with other consumer health data that is derived or extrapolated from non-health information.[11]

Practically speaking, that likely includes any information about consumers collected via apps and websites that discuss medical conditions, treatment, weight loss, fertility, etc., including via cookies and other trackers used on those apps/websites. It is also likely to include any health information collected by social media companies, software-as-a-service providers and data brokers that operate outside of the traditional "health" space, but nonetheless collect information that relates to consumers' health, fitness, location, treatment, etc. for business purposes. As the Washington Attorney General has noted in its guidance[12] on the WA MHMD Act, a retailer "assigning shoppers a 'pregnancy prediction score' based on the purchase of certain products is protected consumer health data even though it was inferred from nonhealth data."

The MHMD Acts require companies to obtain consent for collection, disclosure and sale of consumer health data; publish a consumer health data privacy policy; maintain controller/processor contract terms with their data processors; and give consumers certain data subject rights. The MHMD Acts' consent requirements are particularly onerous. They require companies to obtain separate consents to collect and disclose consumer health data, and to further obtain a separate authorization, similar to a HIPAA authorization in form and content, before selling consumer health data. That means that in contexts where companies previously used only a single checkbox to obtain consent – or just did not obtain consent at all – companies must now use layered consents and obtain more than one signature from consumers prior to collecting and disclosing consumer health data. It also poses substantial logistical challenges. In the cookie context, for example, companies that have apps or webpages relating to medications, health conditions, symptoms, etc. must now consider how to obtain two to three consents from Washington and Nevada consumers before any tracking technologies collect information about them.

Other states have also taken similar steps. Connecticut adopted consumer health data provisions into the Connecticut Data Privacy Act in June 2023, and other states have proposed consumer health data laws that are still pending in state legislatures. To add further complexity, new regulations interpreting the Colorado Privacy Act have detailed consent requirements for collection of "sensitive data," which must be incorporated when drafting consent forms for collection of consumer health data.

KEY TAKEAWAYS

Collectively, all of these changes have significant impacts for industry. In addition to new compliance obligations, companies should be aware that the WA MHMD Act contains a private right of action, which increases the potential risk of non-compliance. Some other key takeaways include:

---

[11] Id.

[12] https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy.

- *"Consumer Health Data" Has a Broad Scope.* The FTC, state attorneys general and state legislators are trying to regulate any health information that is not covered by HIPAA. They're concerned that companies are collecting health information without consent and using that information to target ads and profile consumers based on interests and sensitive locations visited. Accordingly, companies need to understand that consumer health data is regulated even when it is not directly identifiable on its face and even when it does not include specific medical records – like treatment or diagnosis. Regulators and legislators are increasingly arguing that the mere fact that a consumer visits a website/app relating to a medication, condition, etc., plus a unique identifier like an IP address or mobile ad ID, constitutes consumer health data.

- *Consumer Health Data Flows.* To comply with new consumer health data requirements, companies will need to know what consumer health data they are collecting, where they get it from and where they send it. That means that companies' legal and compliance teams will need to work with business personnel to identify data streams, understand use cases, and implement appropriate consents for collection, disclosure and sale of consumer health data, as appropriate. It also means that companies will need to carefully consider whether they sell consumer health data, including via cookies and other tracking technologies, and implement robust consent language to do so compliantly.

- *Consumer Health Data Privacy Policies.* The MHMD Acts require companies to maintain a consumer health data privacy policy. Per new guidance from the Washington AG,[13] companies' consumer health data privacy policies must be separate from their "main" privacy policies, accessible via a dedicated link on their websites, and "may not contain additional information not required under the [Washington] My Health My Data Act." That means that companies need to be taking steps now to implement a new "Consumer Health Data Privacy Policy" on their websites, and that they'll need to separately address privacy policy disclosures required by Nevada's consumer health data law, which are more extensive than those required by the WA MHMD Act.

- *Consent Language Updates.* The MHMD Acts, Colorado Privacy Act regulations and FTC enforcement actions collectively require detailed and layered consent language for collection, disclosure and sale of consumer health data. Companies will need to update consent forms to reflect

[13] https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy.

these changes before the end of March and will likely need to implement consent forms in places where they have not collected detailed consent before, such as the cookie context. Companies should also be aware that consent requirements are likely to keep changing over the next few years as further enforcement actions and new state laws further inform the consent requirements in this space.

- *Penalty Calculations.* GoodRx settled for $1.5 million, Premom paid $200,000, and X-Mode and InMarket both settled without monetary penalties. BetterHelp paid the most, but still settled for only $7.8 million. So does all of this really matter? Well, yes. Penalties were low because the FTC's authority to impose monetary penalties for violations of the FTC Act is limited. But the FTC can seek monetary penalties for violations of its Health Breach Notification Rule, and now that the FTC has set precedents for enforcing the Rule in GoodRx and Premom, it's likely to seek higher penalties in future cases. Moreover, the real penalties in all of these cases were substantive. *GoodRx*, BetterHelp and *Premom* are all permanently prohibited from disclosing health information to third parties for advertising purposes. Similarly, X-Mode and InMarket must delete all historic location data they collected about consumers without prior express consent, subject to a few caveats. For data brokers whose business it is to buy and sell data, deleting historic location data and complying with the FTC's other robust substantive penalties is a considerable blow.

- *More (Not Less) Complexity Is Coming*. 2023 brought a lot of changes in the consumer health data space. But it is probably only the tip of the iceberg. The message from regulators and legislators is clear: Consumers do not want to be tracked, especially when it comes to sensitive information about their health. More enforcement and consumer health data statutes are likely, as are private suits under the WA MHMD Act.

These new requirements do not prevent companies from collecting, disclosing, and selling consumer health data altogether, but they do – intentionally – make all of those things a lot harder to do. Business practice that were relatively standard six to twelve months ago will now require much more scrutiny and impose heightened risk. Companies will need to be aware of these changes, understand their implications and adjust business practices to manage risk.

IN SUMMARY

- Consumer health data – health information that falls outside the scope of HIPAA – was subject to relatively light regulation before 2023.

- Enforcement actions from the FTC, along with a wave of new state laws and regulations, have created new compliance obligations and substantially increased risk for industry stakeholders.