Lawyer Insights

What To Know About State-Level Health Data Privacy Laws

By Michael La Marca, Jennie Cunningham and Marshall Mattera
Published in Law360 | March 28, 2024

The privacy of health data — in particular, health data that is not governed by the Health Insurance Portability and Accountability Act — has increasingly become a focus of federal and state regulators and legislators.

The Federal Trade Commission, for example, has released a number of recent public statements that provide both guidance on protecting the privacy of consumer health data and warnings that health privacy is a top priority for FTC enforcement efforts.

The FTC has also penalized companies, including X-Mode Social Inc. and its successor Outlogic LLC, in January, for allegedly selling and/or sharing geolocation data that could reveal sensitive locations such as healthcare and reproductive care facilities, failing to put appropriate safeguards in place with respect to third party data use, failing to provide appropriate notice to consumers or obtain their consent, and failing to put procedures in place to remove sensitive locations from raw data.[1]

Additionally, in July 2023, the FTC summarized key takeaways from "case after case involving consumers' sensitive health data," including that companies need to understand the breadth of health data, which may include location, app usage and other information that enables an inference about a consumer's health, and that companies' obligation to protect health data with appropriate policies and procedures is a "given".[2]

In September 2023, the FTC released additional guidance that outlines key requirements for companies under HIPAA, the FTC Act and the FTC's Health Breach Notification Rule and underscores that companies not subject to HIPAA are still responsible for practices, notices and procedures related to health data.[3]

We anticipate the focus on health and other sensitive personal data to continue at both the state and federal level in 2024, and certain recently enacted health privacy laws are poised to affect a number of companies that might otherwise have relatively low exposure to health privacy regulation.

In particular, in 2023, Washington, Nevada and Connecticut adopted health privacy legislation adding new state protections for consumer health data, including some that are currently in force and others that will become applicable in 2024.

Unlike HIPAA, which applies only to certain healthcare entities and insurers — and their business associates — these new state health privacy laws apply to a broad range of entities, including in the retail sector.

What To Know About State-Level Health Data Privacy Laws
By Michael La Marca, Jennie Cunningham and Marshall Mattera
Published in Law360 | March 28, 2024

Applicability

In April 2023, Washington enacted the My Health My Data Act, the first state comprehensive consumer health data privacy law in the U.S.

The My Health My Data Act applies to regulated entities and small businesses that (1) conduct business in Washington or offer products or services targeted at consumers in Washington and (2) determine the purpose and means of collecting, processing, sharing or selling of consumer health data.

The act's definition of "consumer health data" is extremely broad and the nonexclusive list of examples includes personal information that identifies a consumer's past, present or future "physical or mental health status."

Physical or mental health status includes individual health conditions, treatment, diseases or diagnosis and use or purchase of prescribed medications — but does not explicitly exclude nonprescription medications. It also includes precise location information "that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies."

Notably, and as explained in FAQs released by the Washington State Attorney General's Office, consumer health data may include inferences drawn from data that is not by itself consumer health data, such as a pregnancy prediction score calculated based on the purchase of certain products.[4]

In addition, certain requirements, such as the My Health My Data Act's geofencing prohibition, discussed below, and restrictions on selling or offering to sell consumer health data, apply to any person, i.e., not only regulated entities.

In June 2023, shortly following the passage of Washington's My Health My Data Act, Connecticut and Nevada enacted their own health privacy laws.

Nevada's health privacy law, S.B. 370, is similar to the My Health My Data Act in terms of applicability and structure. However, the Nevada law has a slightly narrower definition of "consumer health data" that applies only where the regulated entity uses the information to identify the consumer's health status. Nevada's definition is otherwise much like Washington's in that it includes a long list of examples.

Connecticut's health privacy law, S.B. 3, enacted as an amendment to the Connecticut Data Privacy Act, follows Nevada's approach in defining "consumer health data" more narrowly to mean any personal data that a controller "uses to identify" a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data.

Unlike Washington and Nevada, Connecticut's definition does not otherwise include a long list of examples. The law applies to entities that process the consumer health data of Connecticut residents.

General Requirements

Both the Washington and Nevada laws impose a number of obligations on regulated entities, including to develop and maintain a consumer health data privacy policy, comply with certain consumer rights requests, maintain administrative, technical and physical data security practices, and enter into contracts that meet specific requirements with processors that process consumer health data.

What To Know About State-Level Health Data Privacy Laws
By Michael La Marca, Jennie Cunningham and Marshall Mattera
Published in Law360 | March 28, 2024

All three new state laws require entities to obtain consent prior to certain disclosures —e.g., selling — of consumer health data and restrict access to consumer health data by employees, processors and other entities. In addition, in many cases, separate consent is required for the collection of consumer health data.

With respect to the type of consent, the Nevada law notes only that consent must be affirmative and voluntary. In contrast, the Washington law is far more specific, requiring the consent to be a "clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement" and prohibiting certain means of obtaining consent, e.g., "acceptance of a general or broad terms of use agreement or a similar document"; "hovering over, muting, pausing, or closing a given piece of content"; or through the use of "deceptive designs."

The Connecticut law defines consent almost identically to Washington. The Washington and Connecticut version of consent appears to underscore the importance of specific and separate consent that should not be grouped in with other types of processing activities or notices and consents.

Geofencing Ban

In Washington and Nevada, any person — i.e., not only regulated entities — is prohibited from establishing a geofence around an entity that provides in-person health care services, where the geofence is used to (1) identify or track consumers seeking healthcare services; (2) collect consumer health data from consumers; or (3) send notifications, messages or advertisements to consumers related to their consumer health data or healthcare services.

Notably, "health care services" is broadly defined to include any service "provided to a person to assess, measure, improve, or learn about" a person's mental or physical health, and specifically includes use or purchase of medication, i.e., not just prescription medication.

Retail companies may be subject to this prohibition, if, for example, they sell over-the-counter medications or other health-related products.

Connecticut's geofencing provision is a bit narrower, prohibiting the use of a geofence around "any mental health facility or reproductive or sexual health facility for the purpose of identifying, tracking, collecting data from or sending any notification to a consumer" regarding their health data.

Exemptions

Each law contains significant exemptions and exclusions, which should be reviewed carefully by entities before assuming a particular processing activity is or is not subject to the laws. Several are described here, but this is not an exhaustive list.

On balance, the Nevada and Connecticut laws appear to have broader exclusions, particularly in combination with the narrower definition of "consumer health data." The Washington law, for example, exempts data covered by HIPAA or the Gramm-Leach-Bliley Act, while the Nevada law has entity-level exemptions under HIPAA and the GLBA.

What To Know About State-Level Health Data Privacy Laws
By Michael La Marca, Jennie Cunningham and Marshall Mattera
Published in Law360 | March 28, 2024

The Connecticut law exempts both entities and data under HIPAA and the GLBA. The My Health My Data Act also exempts healthcare data covered by Washington's medical records act, and all three states provide for various other data-level exemptions.

The Washington, Nevada and Connecticut laws exempt data collected as part of human subjects research that is covered by Title 45 of the Code of Federal Regulations, Part 46 — Part A of which is usually referred to as the Common Rule — and Title 21 of the Code of Federal Regulations, Parts 50 and 56.

All three also exempt data subject to the Fair Credit Reporting Act, Family Educational Rights and Privacy Act, and a number of other federal and state laws.

The Connecticut law extends entity-level exemptions for various other types of entities, including state and tribal nation government bodies, contractors that process consumer health data for state government, nonprofits, higher education institutions, certain national securities associations and air carriers all — as defined under the relevant laws.

The Nevada law extends entity-level exemptions to law enforcement agencies and their contractors, and to holders of certain gaming licenses and their affiliates.

Enforcement

All three laws provide for government enforcement, but the My Health My Data Act also provides for a private right of action. Most of the act's substantive provisions will not apply to regulated entities that are not small businesses, as defined in the act, until March 31, and will not apply to small businesses until June 30.

Notably, the law's geofencing prohibition is already in force. Certain provisions of Connecticut's health privacy law are in force, but others, such as those relating to the protection of minors, will not apply until Oct. 1. Nevada's law will take effect on March 31.

While companies await enforcement by the states, the FTC has been especially active in enforcing violations related to health data, particularly for companies not otherwise subject to HIPAA.

Recent FTC actions include penalties for 1Health.io, for allegedly deceiving consumers about their ability to delete data, changing its privacy policy retroactively, and exposing health and genetic data;[5] BetterHelp, for allegedly sharing sensitive mental health information for targeted advertising;[6] Easy Healthcare Corporation, for allegedly violating the Health Breach Notification Rule by sharing sensitive information from its Premom fertility tracker app;[7] and GoodRx, for alleged violations of the Health Breach Notification Rule by disclosing consumer health information to third party advertisers and other companies.[8]

Next Steps in 2024

Retail companies should take a conservative approach when interpreting the scope of these new laws. This will help to mitigate risk of liability, particularly as we anticipate regulatory and enforcement efforts to focus on this area and in light of the private right of action under Washington's law.

Companies should assess the applicability of these laws to their businesses to determine next steps to take for compliance, which may include development of privacy notices, consent procedures, rights request response processes and processor contracts, among others.

Companies should also be aware that similar bills are being considered by state legislatures, such as the Vermont My Health My Data Act, which would take effect on Jan. 1, 2025.

Notes

1. See Press Release, FTC, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data (last visited Jan. 22, 2024); Press Release, FTC, FTC Order Will Ban InMarket from Selling Precise Consumer Location Data (Jan. 18, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data (last visited Jan. 22, 2024).

2. FTC, Protecting the privacy of health information: A baker's dozen takeaways from FTC cases (July 25, 2023), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited March 7, 2024). The FTC also described takeaways regarding the importance of proper notices; use of pixels, software development kits and other tracking practices; sharing and receiving of health data; and internal practices for data handling, among others.

3. FTC, Updated FTC-HHS publication outlines privacy and security laws and rules that impact consumer health data (September 15, 2023), https://www.ftc.gov/business-guidance/blog/2023/09/updated-ftc-hhs-publication-outlines-privacy-security-laws-rules-impact-consumer-health-data (last visited March 7, 2024); FTC, Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule (September 2023), https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach (last visited March 7, 2024).

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

5. Press Release, FTC, FTC Says Genetic Testing Company 1Health Failed to Protect Privacy and Security of DNA Data and Unfairly Changed its Privacy Policy (June 16, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-says-genetic-testing-company-1health-failed-protect-privacy-security-dna-data-unfairly-changed (last visited Feb. 12, 2024).

6. Press Release, FTC, FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising (Mar. 2, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook (last visited Mar. 5, 2023).

7. Press Release, FTC, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order (May 17, 2023), 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 (last visited Feb. 4, 2024).

8. Press Release, FTC, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising (last visited Feb. 3, 2023).

Michael La Marca *is a partner in the firm's Global Technology, Outsourcing & Privacy practice in the firm's New York office. Michael can be reached at 212-309-1116 or mlamarca@HuntonAK.com.*

Jennie Cunningham *is an associate in the firm's Global Technology, Outsourcing & Privacy practice in the firm's New York office. She can be reached at +1 (212) 309-1095 or jcunningham@HuntonAK.com.*

Marshall Mattera *is a an associate in the firm's Global Technology, Outsourcing & Privacy practice in the firm's New York office. He can be reached at +1 (212) 309-1270 or mmattera@HuntonAK.com.*