PAUL HASTINGS

Stay Current

April 2023

Follow @Paul_Hastings

Washington State is Set to Expand Protection of Consumer Health Data

By Jeremy Berkowitz, Aaron Charfoos & Jacqueline Cooney

Overview

Washington State ("Washington") is preparing to break new ground in the privacy law space, as its legislature finalizes the "My Health My Data Act" which will further regulate how health data of Washington residents should be processed and protected by private-sector entities. The bill, partially driven by restrictive new abortion laws in other states and the concern that reproductive health information could be improperly shared with legal authorities, provides further protections for "consumer health data" not currently covered by the Health Insurance Portability and Accountability Act ("HIPAA"). Both houses of the state legislature have passed the bill, and Governor Jay Inslee is expected to shortly sign it. Most provisions of the bill will take effect in March 2024.

The bill seeks to regulate more types of "consumer health data" and "legal entities" than are currently within HIPAA's purview. The number of entities that collect health data has grown in recent years, most prominently due to the proliferation of fitness apps and websites, which can track exercise, sleep patterns, and vitals/biometric data about individuals. Washington seeks to provide protection for this data, where it may not fall under HIPAA. Below are some main highlights of the legislation.

Scope

The bill applies to legal entities collecting "consumer health data," which is defined as "personal information that is linked or reasonably linkable to a consumer and that identifies a consumer's past, present, or future physical or mental health." The bill provides a long list of examples of consumer health data including but not limited to:

- Health-related surgeries or procedures;
- Gender affirming care information;
- Biometric data;
- Genetic data; and
- Reproductive or sexual health information.

Whereas HIPAA only applies to covered entities that explicitly provide healthcare services (e.g., doctors, hospitals, and insurance companies), this bill applies to any "legal entity that (a) conducts business in

Washington, or produces or provides products or services that are targeted to consumers in Washington; and (b) alone or jointly with others, determines the purposes and means of collecting, processing, sharing, or selling of consumer health data." This definition differs from recent state privacy laws that usually provide a threshold of applicability for entities (e.g., annual revenue, number of consumers in state). Any private-sector entity, including non-profits, must comply with the provisions of this bill if they have a presence within the state of Washington.

Consumer Rights

The bill requires legal entities to provide a privacy notice explaining how they process consumer health data. The bill says that the collection of consumer health data requires entities to receive consent for each specified purpose, and also says that a "separate and distinct" affirmative consent is required for the sharing of that data. The bill allows consumers to withdraw consent at any time. The bill defines sharing as releasing or disseminating consumer health to a third party. It excludes from this definition, sharing of data with processors to carry out activities for legal entities. The bill also allows for consumers to access their data and request deletion of their data. Legal entities must respond to authenticated deletion requests within 30 days, while other requests must be responded to within 45 days.

Selling of Data/Authorization

The bill has new requirements around "sale" of data, or providing for the "exchange of consumer health data for monetary or other valuable consideration." Legal entities will be required to obtain a written signed authorization from consumers that they approve of their data being sold. This authorization must include specific details of the sale, including the purchasers and how they plan to use it. Legal entities must permit consumers the right to revoke the authorization at any point with clear instructions on how to do so.

Geofencing

The bill also prohibits geofencing around legal entities for the purpose of tracking consumers, collecting consumer health data, or sending notifications. The bill defines geofencing as using technology (e.g., cellular data, GPS) to "establish a virtual boundary around a specific physical location." As an example, a legal entity could not collect data by targeting the mobile devices of individuals entering a reproductive health clinic and then send mobile ads to those individuals urging them to not get an abortion.

Private Right of Action

While the Washington Attorney General has the right to enforce violations of the bill, it also provides for a consumer private right of action. The only other state privacy laws that permit private right of action are the California Privacy Rights Act, and Illinois' Biometric Information Privacy Act. Companies can be fined up to $25,000 per violation.

Exemptions

Besides HIPAA-related data, the bill also provides exemptions for data covered under the Gramm Leach Bliley Act and the Federal Reporting Credit Act. The bill also exempts de-identified data that is "originating from, and intermingled to be indistinguishable with," data collected under HIPAA.

Effective Data

The provisions around geofencing will go into effect 90 days after they are signed. The remainder of the bill will go into effect on March 31, 2024.

Next Steps

- Determine if your business operates in Washington and/or has consumers there.
- Review whether your business collects health data from consumers in Washington and what steps must be taken to comply with the law, particularly provisions around consent and sharing or selling of data.
- Determine if your business currently engages in geofencing and take steps to deactivate it where needed.
- If your business does sell health consumer data as defined by the law, develop a process for obtaining authorizations that would permit sales by individual consumers.

Our Data Privacy and Cybersecurity practice regularly advises companies on how to meet the requirements of new laws and their regulations like this one. If you have any questions concerning this law or any other data privacy or cybersecurity laws, please do not hesitate to contact any member of our team.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings professionals:

Chicago

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

Washington, D.C.

Jeremy Berkowitz
1.202.551.1230
jeremyberkowitz@paulhastings.com

Jacqueline Cooney
1.202.551.1236
jacquelinecooney@paulhastings.com