DAVIS + GILBERT

Privacy + Data Security

Washington is First State to Pass Consumer Health Data Privacy Law

The Bottom Line

- With states passing comprehensive consumer privacy laws left and right, Washington is the first state to pass an aggressive privacy law focusing on consumer health data.
- With consent requirements to process health data and a private right of action, the Act is not one to be overlooked and will likely change the way marketers use and leverage health data for advertising purposes.
- The parade of new privacy laws will continue, as Indiana, Montana and Tennessee are poised to pass their own.

Washington is the first state to enact a comprehensive consumer privacy law focused on health data. House Bill 1155, also known as the My Health My Data Act, was signed into law by Gov. Jay Inslee on April 27, 2023. The Act will take effect on March 31, 2024, with certain small businesses granted an extension until June 30, 2024, and will add significant compliance obligations to the patchwork of state data privacy laws.

Unlike the existing patchwork, the Act focuses exclusively on consumer health data that is not regulated by the Health Insurance Portability and Accountability Act (HIPAA). While health care providers and similar HIPAA-covered entities are exempt, many advertisers, mobile app providers, wearable device manufacturers and health care companies and their data processors outside the scope of HIPAA may be materially impacted.

My Health My Data Threshold Requirements

The Act will apply to any entity, including nonprofits, that conducts business in Washington or provides products and services to consumers in Washington and, alone or jointly with others, determines the purpose and means of collecting, processing, sharing or selling consumer health data.

The Act broadly applies to any entity that does business in the state involving health data collection, regardless of revenue or size. Therefore, small businesses need to be aware of the law's reach. This is unlike other existing consumer data privacy laws, such as the California Consumer Privacy Act (CCPA) and Utah Consumer Privacy Act (UCPA), which have revenue thresholds, or the Virginia Consumer Data Protection Act (VCDPA), Colorado Privacy Act (CPA) and Connecticut Data Privacy Act (CTDPA), which have data processing thresholds.

Because the Act goes beyond Washington residents to cover any natural person whose data is collected in the state, the scope of who is a "consumer" has an extraterritorial application insofar as it applies to non-Washington residents who interact with regulated entities in the state.

In addition, the Act's broad definition of "health care services," which includes any service provided to a person to assess, measure, improve or learn about a person's mental or physical health, means that businesses providing services ancillary to clinical care that have contact with "consumer health data" (discussed below), could also have compliance obligations under the Act.

"Consumer Health Data"

The Act broadly defines "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. Consumer health data specifically includes:

- Individual health conditions, treatment, diseases or diagnoses
- Social, psychological, behavioral and medical interventions
- Health-related surgeries or procedures
- Use or purchase of prescribed medication
- Bodily functions, vital signs, symptoms or measurements of the information expressly identified in the definition of consumer health data
- Diagnoses or diagnostic testing, treatment or medication
- Gender-affirming care information
- Reproductive or sexual health 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
- Any information that a regulated entity, or its respective processor, processes to associate or identify a consumer with the data described above that is derived or extrapolated from non-health information (such as proxy, derivative, inferred or emergent data by any means, including algorithms or machine learning)

Within the definition of consumer health data, the Act defines "personal information" in a broad manner, similar to the CCPA. However, it clarifies that personal information "includes, but is not limited to, 'data associated with a persistent unique identifier, such as a cookie ID, an IP address, a device identifier, or any other form of persistent unique identifier.'" This definition is consistent with a recent FTC enforcement action regarding adtech practices by health care entities and digital health services.

Regulated Entities' Obligations

On top of the requirements under existing state privacy laws, the Act will add additional compliance obligations for regulated entities. Specifically, the Act will require regulated entities to do the following:

- Post a privacy policy that discloses the following with respect to consumer health data:
  1. the categories of consumer health data collected and the purposes of collection
  2. the categories of sources from which consumer health data is collected
  3. the categories of consumer health data that is shared and the categories of third parties and specific affiliates with whom the regulated entity shares consumer health data and
  4. how a consumer may exercise consumer rights regarding consumer health data
- Obtain the consumer's consent before collecting their health data, and obtain a consent that is "separate and distinct" from that collection consent, to share the health data with a third party
- Obtain an additional layer of consent, "separate and distinct" from the consent to collect or share data, to sell health data. "Sale" is defined broadly, similar to the CCPA, and includes any "exchange of consumer health data for monetary or other valuable consideration." A valid authorization to sell consumer health data must contain the following:

1. The specific consumer health data concerning the consumer that the regulated entity intends to sell
2. The name and contact information of the regulated entity collecting and selling the consumer health data
3. The name and contact information of the purchaser of the consumer health data
4. A description of the purpose for the sale, including how the consumer health data will be gathered and how it will be used by the purchaser when sold
5. A statement that the provision of goods or services may not be conditioned on the consumer signing the valid authorization
6. A statement that the consumer has a right to revoke their consent at any time, and a description on how to do so
7. A statement that the consumer health data may be subject to redisclosure by the purchaser and may no longer be protected by the Act
8. An expiration date for the authorization that is one year from when the consumer signs the valid authorization and
9. The signature of the consumer and the date

- Implement and maintain reasonable administrative, technical and physical data security controls surrounding consumer health data and limit access to consumer health data to only personnel who have a need-to-know
- Have a written contract with data processors related to their use of consumer health data detailing the processing instructions for the processor and limiting the actions that may be taken by the processor with respect to data processed on behalf of the regulated entity. Akin to the GDPR, processors must also use appropriate technical and organizational measures to assist regulated entities in fulfilling their obligations relating to consumer health data.

The Act also prohibits implementing a geofence around an entity that provides in-person health care services, if the geofence is used to

1. identify or track consumers seeking health care services
2. collect consumer health data from consumers or

3. send notifications, messages or advertisements to consumers related to their consumer health data or health care services

Geofence is defined as technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wi-Fi data and/or any other form of location detection to establish a virtual boundary of 2,000 feet or less from the perimeter of a specific physical location.

Consumer Rights

The Act provides consumers with the right to:

1. know whether a regulated entity is collecting, sharing or selling consumer health data
2. access their health data, including a list of all third parties and affiliates with whom the regulated entity has shared or sold the consumer health data
3. withdraw consent from the regulated entity's collection and sharing of consumer health data
4. request the deletion of consumer health data and
5. appeal a regulated entity's refusal to act on a consumer's rights

Regulated entities must respond to consumer requests within 45 days, with the option to obtain a 45-day extension from complicated requests. For deletion requests, regulated entities have six months to delete data on archived or backup systems and, unique to the Act (in contrast to other state privacy laws), there are no exceptions to the deletion requirement. Verified consumer requests must also flow down to all service providers, contractors, third parties and affiliates.

Enforcement and Private Right of Action

The Washington Attorney General is authorized to enforce the Act. However, businesses should be aware of the Act's private right of action, which gives Washington residents the right to bring a claim under Washington's Consumer Protection Act (CPA) for unfair or deceptive acts in trade or commerce and unfair methods of competition. Businesses that violate the CPA may face damages of up to $7,500 per violation, as well as additional damages, capped at $25,000. As such, the Act provides some of the stiffest penalties among any existing consumer data privacy law.

Privacy + Data Security

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Jeremy Merkel

Associate
212 468 4976
jmerkel@dglaw.com