Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Technology, Economic Development, & Veterans Committee

HB 1671

Brief Description: Protecting personal data privacy.

Sponsors: Representatives Kloba, Fosse, Doglio, Parshley, Berry, Ramel, Scott, Taylor and Simmons.

Brief Summary of Bill

- Establishes consumer rights with regard to personal data and defines obligations of data controllers and processors.
- Requires controllers to conduct data protection assessments for processing activities that present a heightened risk of harm.
- Makes violations enforceable under the Consumer Protection Act.

Hearing Date: 2/4/25

Staff: Emily Poole (786-7106).

Background:

Privacy Regulation.
The collection, use, and transfer of personal information are subject to various provisions of state and federal law. At the federal level, regulated entities are governed by varying privacy frameworks based on the industry and types of data involved. For example, the Health Insurance Portability and Accountability Act (HIPAA) establishes standards for the use, disclosure, and transfer of "protected health information," and the Gramm-Leach-Bliley Act (GLBA) establishes a privacy framework for financial data.

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not part of the legislation nor does it constitute a statement of legislative intent.

In Washington, data privacy and security laws include data breach reporting requirements, privacy requirements placed on health care providers under the Uniform Health Care Information Act (UHCIA), and protections for consumer health data under the My Health My Data (MHMD) Act.

The My Health My Data Act.
The MHMD Act defines obligations of regulated entities that collect, use, or share consumer health data and specifies consumer rights with regard to consumer health data. "Consumer health data" is defined 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.

Privacy Policy Requirement
A regulated entity must publish a consumer health data privacy policy that discloses:
- the categories of consumer health data collected and the purposes of collection;
- the categories of sources from which consumer health data is collected;
- the categories of consumer health data that are shared and the categories of third parties with whom the regulated entity shares consumer health data; and
- how a consumer may exercise consumer rights with regard to consumer health data.

A regulated entity must make additional privacy policy disclosures and obtain consent before collecting or sharing categories of consumer health data not disclosed in the privacy policy, and before collecting or sharing consumer health data for additional purposes.

Consent Requirement
A regulated entity may not collect or share consumer health data except with the consumer's consent or to the extent necessary to provide a product or service that the consumer requested. Consent must be obtained prior to the collection or sharing of any consumer health data.

Consumer Rights Concerning Consumer Health Data
A consumer has rights with regard to consumer health data, including the right to:
- confirm whether a regulated entity is collecting, sharing, or selling consumer health data;
- access consumer health data, including a list of all third parties and affiliates with whom the regulated entity has shared or sold the consumer health data;
- withdraw consent from the collection and sharing of consumer health data; and
- have consumer health data deleted.

If a regulated entity is unable to authenticate a consumer request to exercise consumer rights using commercially reasonable efforts, the regulated entity is not required to comply with a request. A regulated entity must respond to a consumer request within 45 days. Information provided in response to a consumer request must be provided free of charge up to two times a year.

A regulated entity must establish a process for a consumer to appeal the regulated entity's refusal

to take action on a request.

It is unlawful for any person to sell consumer health data without first obtaining a valid authorization from the consumer, which must include certain specified information.

Data Security Requirements
A regulated entity must restrict access to consumer health data by employees, processors, and contractors to only as is necessary to further the purposes for which a consumer provided consent or to provide a product or service the consumer has requested. A regulated entity must maintain data security practices that, at a minimum, satisfy the reasonable standard of care.

Obligations of Processors
A processor may process consumer health data only pursuant to a binding contract between the processor and the regulated entity. The contract must include the processing instructions and limit the actions a processor may take with respect to consumer health data.

Enforcement
Violations are deemed to affect the public interest and are unfair or deceptive acts in trade or commerce for the purposes of applying the Consumer Protection Act (CPA).

Exemptions and Limitations
The MHMD Act does not apply to personal information that is collected, used, or disclosed pursuant to specified federal and state laws, including but not limited to protected health information for the purposes of the HIPAA and health care information collected, used, or disclosed in accordance with the UHCIA.

The obligations imposed on regulated entities and processors do not restrict their ability to collect, use, or disclose consumer health data in order to: prevent or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any activity that is illegal under state or federal law; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for such actions.

Summary of Bill:

Key Definitions and Scope
"Controller" means the natural or legal person who, alone or jointly with others, determines the purposes and means of collecting or processing of personal data.

"Personal data" means any information that identifies or is reasonably capable of being associated or linked, directly or indirectly, with a particular consumer. "Personal data" includes, but is not limited to, derived data and data associated with a persistent unique identifier, such as a cookie identifier, an internet protocol address, a device identifier, or any other form of persistent unique identifier. "Personal data" does not include publicly available information or deidentified data.

People that conduct business in Washington or produce products or services that are targeted to residents of Washington, and that collect or process the personal data of consumers, are subject to certain requirements relating to the collection, use, and sharing of personal data. Such requirements do not apply to government entities and do not apply to certain specified types of exempted information, including information collected and processed in accordance with the HIPAA, the UHCIA, the GLBA, the Fair Credit Reporting Act, the Family Educational Rights and Privacy Act, and other state and federal laws.

Consumer Rights
A consumer has the right to:

- confirm whether a controller is collecting or processing the consumer's personal data, access such data, and confirm whether the data is used to profile the consumer for the purpose of automated decision making;
- obtain a list of specific third parties to which the controller has transferred personal data;
- correct inaccuracies in the consumer's personal data;
- delete personal data concerning the consumer;
- obtain a copy of the consumer's personal data collected or processed by a controller; and
- opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

A consumer may exercise these rights by a means established by the controller and described in the controller's privacy notice.

Responding to Consumer Requests
A controller is required to comply with a consumer request to exercise their rights, subject to certain requirements and exceptions. A controller must respond within 45 days of receiving a request, but the controller may extend that period when reasonably necessary. Information provided in response to a consumer request must be provided free of charge up to two times a year. Except for opt-out requests, a controller is not required to comply with a request if the controller is unable to authenticate the request using commercially reasonable efforts. A controller must establish a process for a consumer to appeal a controller's refusal to take action on a request.

A controller may not condition the exercise of consumer rights through the use of dark patterns or any false or materially misleading statement or representation.

A controller must describe in their privacy notice a means for consumers to submit requests to exercise their rights. Among other requirements, the means must include a link on the controller's website that enables a consumer to opt out of targeted advertising, the sale of personal data, and profiling in furtherance of certain automated decisions. By December 31, 2025, a controller must also allow opt-outs through a preference signal that is consumer friendly and enables a controller to reasonably determine residency.

Responsibilities of Controllers
A controller must limit the collection, processing, and transfer of personal data to what is strictly necessary to provide or maintain a specific product or service requested by the consumer or certain consumer communications. A controller may only collect and transfer consumer health data in accordance with the MHMD Act.

Except with respect to sensitive data, a controller may process or transfer personal data to provide first-party advertising or targeted advertising, unless a consumer has opted out. Except as specified in the MHMD Act, a controller may not transfer sensitive data concerning a consumer without obtaining the consumer's affirmative consent. A controller may not sell sensitive data unless allowed by the MHMD Act. Controllers must establish a mechanism for consumers to revoke affirmative consent.

Controllers must maintain data security practices that satisfy the reasonable standard of care, and controllers may not discriminate or retaliate against consumers for exercising their rights.

Controllers must provide consumers with a reasonably accessible, clear, meaningful privacy notice that includes certain required contents, including: the categories of personal data collected and processed by the controller; the purpose for the collection and processing; the length of time the controller intends to retain each category of personal data; and other information. If a controller makes a material change to the notice, the controller must notify affected consumers before implementing the change and provide a reasonable opportunity for each consumer to withdraw consent.

If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must disclose such activities, as well as the manner in which a consumer may exercise the right to opt out.

Responsibilities of Processors
Processors must adhere to the instructions of controllers, pursuant to a binding contract, and must assist controllers in meeting their privacy obligations. Processors may only process and transfer data received from a controller to the extent necessary to provide a service requested by the controller, as set out in the contract. Contracts between controllers and processors must contain certain specified provisions, such as requirements regarding confidentiality, processes for deleting personal data, subcontractor contracts, the combining of personal data, and controller assessments. Processors must maintain data security practices that satisfy the reasonable standard of care.

Data Protection Assessments
A controller may not conduct processing that presents a heightened risk of harm to a consumer without conducting a data protection assessment for each of the controller's processing activities that presents the heightened risk of harm. The assessment must include certain specified contents, and a controller must make a summary of the assessment publicly available. A

controller must make the data protection assessment available to the Attorney General upon request.

Deidentified Data
A controller in possession of deidentified data must: take technical measures to ensure that the data cannot be associated with an individual; publicly commit to maintaining deidentified data without attempting to reidentify the data; and require any recipients of the deidentified data to comply with relevant data privacy requirements.

Limitations
The data privacy obligations imposed on controllers and processors do not restrict a controller's or processor's ability to conduct certain specified activities, including complying with other laws, cooperating with law enforcement agencies, providing requested consumer products, protecting against fraud, engaging in scientific research, and other activities.

Enforcement
Violations of privacy requirements are deemed to affect the public interest and are unfair or deceptive acts in trade or commerce for the purposes of applying the CPA.

Additional Requirements
Controllers and processors that collect or process consumer health data may be subject to additional data privacy requirements under the MHMD Act.

Appropriation: None.

Fiscal Note: Requested on January 30, 2025.

Effective Date: The bill contains multiple effective dates. Please see the bill.