Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Civil Rights & Judiciary Committee

HB 1155

Brief Description: Addressing the collection, sharing, and selling of consumer health data.

Sponsors: Representatives Slatter, Street, Reed, Ryu, Berg, Alvarado, Taylor, Bateman, Ramel, Senn, Goodman, Fitzgibbon, Macri, Simmons, Reeves, Lekanoff, Orwall, Duerr, Thai, Gregerson, Wylie, Ortiz-Self, Stonier, Pollet, Riccelli, Donaghy, Fosse and Ormsby; by request of Attorney General.

Brief Summary of Bill

- Establishes consumer rights with regard to consumer health data and defines obligations of regulated entities that collect, use, and share consumer health data.
- Exempts government agencies, tribal nations, and health care information subject to federal and state law related to confidentiality of health care information.
- Prohibits selling consumer health data and implementing a geofence around certain health care entities.
- Makes violations enforceable under the Consumer Protection Act.

Hearing Date: 1/24/23

Staff: Yelena Baker (786-7301).

Background:

Confidentiality of Health Care Information.
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes nationwide standards for the use, disclosure, and transfer of "protected health information,"

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.

defined as individually identifiable health information that relates to an individual's past, present, or future physical or mental health or condition, or to the provision of health care to the individual. The HIPAA applies to "covered entities," which are health care providers, health plans, and health care clearinghouses, and "business associates," which are entities that perform certain functions or activities that involve the use or disclosure of protected health information on behalf of a covered entity.

Covered entities and business associates must have an individual's authorization to use or disclose protected health care information. The HIPAA permits use and disclosure of protected health information without an individual's authorization for specified purposes, including:

- treatment, payment, and healthcare operations;
- research and public health activities, or health oversight activities;
- to prevent or lessen a serious and imminent threat to a person or the public;
- law enforcement purposes, judicial and administrative proceedings; and
- as required by law, including by statute, regulation, or court orders.

In Washington, the Uniform Health Care Information Act (UHCIA) governs the disclosure of health care information by health care providers and their agents or employees. The UHCIA provides that a health care provider may not disclose health care information about a patient unless there is a statutory exception or written authorization by the patient. Statutory exceptions under the UHCIA are similar to those under HIPAA and include disclosures made for: the provision of health care; quality improvement; legal and administrative services; research purposes; public health and law enforcement activities; and judicial proceedings.

Washington Consumer Protection Act.
The Consumer Protection Act (CPA) prohibits unfair methods of competition or unfair or deceptive practices in the conduct of any trade or commerce. The Attorney General is authorized to investigate and prosecute claims under the CPA on behalf of the state or individuals in the state. A person injured by a violation of the CPA may bring a civil action for injunctive relief, recovery of actual damages, and reasonable attorneys' fees. The courts may increase awarded damages up to three times the actual damages sustained.

Summary of Bill:

The Washington My Health My Data Act is adopted to define obligations of regulated entities that collect, use, or share consumer health data and to specify consumer rights with regard to consumer health data.

Key Definitions and Scope.
"Regulated entity" means any legal entity that:

- conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington;
- collects, shares, or sells consumer health data; and
- determines the purpose and means of the processing of consumer health data.

"Regulated entity" does not include a government agency or a tribal nation.

"Consumer health data" means personal information relating to the past, present, or future physical or mental health of a consumer including any personal information relating to:

- individual health conditions, treatment, status, diseases, or diagnoses;
- social, psychological, behavioral, and medical interventions;
- health-related surgeries or procedures, diagnostic testing, and treatment;
- use or purchase of medication;
- bodily functions, vital signs, symptoms, or related measurements;
- efforts to research or obtain health services or supplies;
- gender-affirming care information;
- reproductive or sexual health information;
- biometric and genetic data related to consumer health data;
- location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies; and
- any consumer health data information that is derived or extrapolated from non-health information, such as proxy, derivative, inferred, or emergent data.

"Consumer health data" does not include personal information that is used to engage in public or peer-reviewed scientific, historical, or statistical research that adheres to all other applicable ethics and privacy laws and is monitored or governed by an independent oversight entity.

The Washington My Health My Data Act does not apply to:

- health care information collected, used, or disclosed in accordance with the state Uniform Health Care Information Act;
- protected health information, or information treated like protected health information, that is collected, used, or disclosed by covered entities and businesses associates subject to and in accordance with the federal Health Insurance Portability and Accountability Act; and
- patient identifying information collected, used, or disclosed in accordance with federal law relating to confidentiality of substance use disorder records.

Privacy Policy Requirement.
A regulated entity must maintain and prominently publish on its homepage a consumer health data privacy policy that discloses:

- the specific types of consumer health data collected and the purposes of collection;
- the sources from which consumer health data is collected;
- the specific consumer health data that is shared and the list of third parties and affiliates 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 consumer 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. A

regulated entity may not contract with a service provider to process consumer health data in a manner that is inconsistent with the regulated entity's consumer health data privacy policy.

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

- the categories of consumer health data collected or shared;
- the purpose of the collection or sharing;
- the entities with whom the consumer health data is shared; and
- how the consumer can withdraw consent.

A consumer's consent for the sharing of consumer health data must be separate and distinct from the consumer's consent for the collection of consumer health data.

Consumer Rights Concerning Consumer Health Data.
A consumer has rights with regard to consumer health data concerning the consumer, including the right to:

- confirm whether a regulated entity is collecting or sharing consumer health data;
- access consumer health data;
- confirm that a regulated entity has not sold consumer health data;
- withdraw consent from the regulated entity's collection and sharing of consumer health data; and
- have consumer health data deleted.

Within 30 calendar days of receiving a consumer's request to delete consumer health data concerning the consumer, a regulated entity must delete the consumer health data from its records and notify all affiliates, service providers, and other third parties with whom the regulated entity has shared the consumer health data of the consumer's deletion request. All notified affiliates, service providers, and other third parties must honor the consumer's deletion request and delete the consumer health data from all records.

Data Security Requirements.
A regulated entity must restrict access to consumer health data by the regulated entity's employees, service providers, 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 establish and maintain administrative, technical, and psychical data security practices that, at a minimum, satisfy reasonable standard of care within the regulated entity's industry to protect confidentiality, integrity, and accessibility of consumer health data.

Obligations of Service Providers.
A service provider may process consumer health data only pursuant to a binding contract

between the service provider and the regulated entity. The contract must set forth the processing instructions and limit the actions a service provider may take with respect to consumer health data. A service provider may process consumer health data only in a manner that is consistent with the binding instructions set forth in the contract.

If a service provider fails to adhere to the regulated entity's instructions or processes consumer health data in a manner that is outside the scope of the service provider's contract with the regulated entity, the service provider is considered a regulated entity.

Prohibition on Sale of Consumer Health Data.
It is unlawful for any person to sell consumer health data. To "sell" means to share consumer health data for monetary or other valuable consideration. "Selling" does not include sharing:

- to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the regulated entity's assets;
- by a natural person selling their own consumer health data pursuant to a written contract with a third party; or
- by a regulated entity to a service provider when the sharing is consistent with the purpose for which the consumer health data was collected.

Prohibition on Geofencing of Certain Health Care Entities.
It is unlawful for any person to implement a geofence around any entity that provides in-person health care services where the geofence is used to identify, track, collect data from, or send notifications or messages to a consumer that enters the virtual perimeter. "Geofence" means technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wi-Fi data, and any other form of location detection to establish a virtual boundary around a specific physical location.

Enforcement.
Violations of the Washington My Health My Data Act are enforceable under the Consumer Protection Act.

Appropriation: None.

Fiscal Note: Requested on January 18, 2023.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.