HOUSE BILL REPORT
HB 1155

As Reported by House Committee On:
Civil Rights & Judiciary

Title: An act relating to the collection, sharing, and selling of consumer health data.

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 History:
Committee Activity:
Civil Rights & Judiciary: 1/24/23, 2/3/23 [DPS].

Brief Summary of Substitute Bill

- Establishes consumer rights with regard to consumer health data and defines obligations of regulated entities that collect, process, share, and sell consumer health data.
- Exempts government agencies, tribal nations, and personal information subject to specified federal and state law.
- Prohibits selling consumer health data without a valid authorization.
- Prohibits implementing a geofence to track or collect data from consumers who enter certain health care entities.
- Makes violations enforceable under the Consumer Protection Act.

HOUSE COMMITTEE ON CIVIL RIGHTS & JUDICIARY

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 7 members: Representatives Hansen, Chair; Farivar, Vice Chair; Entenman,

---

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.

Goodman, Peterson, Thai and Walen.

Minority Report: Do not pass. Signed by 2 members: Representatives Walsh, Ranking Minority Member; Graham, Assistant Ranking Minority Member.

Minority Report: Without recommendation. Signed by 2 members: Representatives Cheney and Rude.

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," 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 health care 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 and 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 Substitute 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; and
- alone or jointly with others determines the purpose and means of collecting, processing, sharing, or selling of consumer health data.

"Regulated entity" does not include a government agency, a tribal nation, or a contracted service provider processing consumer health data on behalf of a government agency.

"Consumer health data" means 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. Consumer health data includes:

- 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;
- gender-affirming care information;
- reproductive or sexual health information;
- biometric and genetic data related to consumer health data;
- precise 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.

Privacy Policy Requirement.
A regulated entity must maintain and prominently 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 is shared and the categories 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.

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 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 categories of 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, 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 regulated entity's 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 and may request additional information from the consumer.

A regulated entity must respond to a consumer request within 45 days of receipt. This response period may be extended once by another 45 days when reasonably necessary. Information provided in response to a consumer request must be provided free of charge up to two times a year.

Within 30 calendar days of authenticating 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, processors, and other third parties with whom the regulated entity has shared the consumer health data of the consumer's deletion request. All notified affiliates, processors, and other third parties must honor the consumer's deletion request and delete the consumer health data from all records. If a consumer requests deletion of consumer health data stored on archived or backup systems, the deletion may be delayed for up to six months to enable restoration of the archived or backup systems.

A regulated entity must establish a process for a consumer to appeal the regulated entity's refusal to take action on a request. Within 45 days of receipt of an appeal, a regulated entity must inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the regulated entity must also provide the consumer with an online mechanism or other method through which the consumer may contact the Attorney General to submit a complaint.

Data Security Requirements.
A regulated entity must restrict access to consumer health data by the regulated entity's 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 establish and maintain administrative, technical, and physical 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 Processors.
A processor may process consumer health data only pursuant to a binding contract between the processor and the regulated entity. The contract must set forth the processing instructions and limit the actions a processor may take with respect to consumer health data. A processor may process consumer health data only in a manner that is consistent with the binding instructions set forth in the contract.

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

Prohibition on Sale of Consumer Health Data Without Valid Authorization.
It is unlawful for any person to sell consumer health data concerning a consumer without first obtaining a valid authorization from the consumer. A valid authorization must be written in plain language and must contain specified information, including:

- the specific consumer health data that the person intends to sell;
- the name and contact information of the seller and the purchaser;

- the purpose for the sale;
- a statement that the provision of goods or services may not be conditioned on the consumer's signing of the authorization; and
- an expiration date of one year from the date of signing.

A copy of the signed valid authorization must be provided to the consumer. The seller and purchaser of consumer health data must retain a copy of all valid authorizations for six years from the date of its signature or the date when it was last in effect, whichever is later.

Prohibition on Geofencing of Certain Health Care Entities.
It is unlawful for any person to implement a geofence to identify, track, collect data from, or send notifications or messages to a consumer who enters an entity that provides in-person health care services.

"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 of 2,000 feet or less from the perimeter of a specific physical location.

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

Exemptions.
The Washington My Health My Data Act does not apply to personal information that is collected, used, or disclosed pursuant to specified federal and state laws, including:

- protected health information for the purposes of the HIPAA;
- health care information collected, used, or disclosed in accordance with the state UHCIA;
- patient identifying information collected, used, or disclosed in accordance with federal law relating to confidentiality of substance use disorder records; and
- personal information governed by the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and statutes and regulations applicable to the Washington Health Benefit Exchange.

The obligations imposed on regulated entities and processors do not restrict a regulated entity's or processor's ability for collection, use, or disclosure of consumer health data to: prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for such actions.

Substitute Bill Compared to Original Bill:

The substitute bill adds several definitions, including "precise location information" and "publicly available information," and modifies several existing definitions, such as

"consumer health data," "geofence," "person," and "regulated entity."

The substitute bill modifies the privacy policy requirements and provides that a regulated entity's privacy policy with respect to consumer health data must disclose:

- categories, rather than the specific types, of consumer health data collected;
- categories of sources from which the data is collected;
- categories of data, rather than specific data, that is shared; and
- a list of the categories of third parties and specific affiliates with whom the data is shared.

Additionally, the substitute bill makes several changes with regard to consumer rights and:

- allows a regulated entity to not comply with a consumer request or to request additional information if the regulated entity is unable to authenticate the request using commercially reasonable efforts;
- requires a regulated entity to provide requested information in response to a consumer free of charge, up to twice annually;
- requires a regulated entity to respond to consumer requests within 45 days of receiving the request and permits an additional 45-day extension when reasonably necessary;
- permits the regulated entity to decline to act on a request or to charge the consumer a reasonable fee to cover the administrative cost of manifestly unfounded, excessive, or repetitive requests; and
- requires a regulated entity to establish a process for a consumer to appeal the regulated entity's refusal to take action on a request.

With respect to the right of access, the substitute bill provides that a consumer's right to access consumer health data includes the right to access the list of all third parties and affiliates with whom the regulated entity has shared or sold the consumer health data and an email address or other online mechanism for contacting these third parties.

With respect to the right of deletion, the substitute bill:

- requires a regulated entity to delete consumer health data within 30 days from authenticating a consumer's deletion request, rather than within 30 days of receiving the request; and
- requires a regulated entity to delete consumer health data from archived and backup systems and allows the regulated entity up to six months from authenticating the deletion request to delete data from archived and backup systems.

The substitute bill removes the prohibition on the sale of consumer health data and instead prohibits selling or offering for sale consumer health data without a valid authorization that meets specified requirements. The substitute bill also modifies the geofencing prohibition to provide that it is unlawful to implement a geofence to identify, track, or collect data from a consumer that enters any entity that provides in-person health care services, rather than prohibiting geofencing around any entity that provides in-person health care services in

order to identify, track, or collect data from a consumer.

Lastly, the substitute bill adds several exemptions for health care information deidentified in accordance with the HIPAA standards and personal information collected, used, or disclosed pursuant to specified laws and regulations, including: the Gramm-Leach-Bliley Act; the Family Educational Rights and Privacy Act; state law governing Washington Health Benefits Exchange and Statewide Health Care Claims Database; privacy rules adopted by the Office of the Insurance Commissioner; and laws governing human subjects research, quality improvement and peer review committees, and reporting of health care-related infections and adverse events.

Appropriation: None.

Fiscal Note: Available.

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

Staff Summary of Public Testimony:

(In support) Health data is some of the most sensitive data collected from an individual, and most people expect this data to be protected or kept confidential by entities that collect it, but that is not always true. The HIPAA applies to covered entities and their business associates, which leaves data collected by applications, websites, and other non-HIPAA entities unregulated. Consumer health data is collected, shared, and sold with little to no oversight or transparency. Period-tracking applications may sell sensitive information about a woman's reproductive health. Pregnant individuals who visit crisis pregnancy centers seeking abortion care may unknowingly have their information shared with anti-abortion groups. Digital advertising firms can set up geofences around health care entities, and once a person crosses that invisible barrier, the person is bombarded with text messages and advertisements, urging the person not to seek reproductive or gender-affirming care. Recently, for just $160 a location data broker sold the aggregated location data of people who visited abortion clinics; the data showed where patients traveled from, how much time they spent at health care centers, and where they went afterwards.

The bill closes the gap between consumer expectations and current laws and gives Washingtonians more control over their data by requiring a distinct consumer health data privacy policy and prohibiting the collection or sharing of health data without consent. The bill also requires compliance with strict HIPAA authorization standards to sell consumer health data.

The overturning of the *Roe v. Wade* decision highlighted and exacerbated gaps in the protection of health care data generally, and reproductive and gender-affirming care in

particular. As many states are moving rapidly to criminalize abortion care and gender-affirming care, Washington must take steps to bolster data privacy as part of its efforts to support access to abortion. Despite abortion remaining legal in Washington, patients traveling from other states are terrified of being criminally prosecuted for seeking legal health care in Washington. Patients are afraid to seek care because of privacy concerns and fear of surveillance. Women seeking reproductive services and transgender people seeking gender-affirming care are particularly at risk. Undocumented people seeking basic health care are concerned that their data will one day be shared with immigration authorities.

Crisis pregnancy centers are under no obligation to maintain patient-doctor confidentiality, which puts people's personal health information at risk. Currently available data management tools aggregate patient data to advance the anti-abortion agenda.

Some argue that this bill needs to be consistent with general data privacy bills enacted in other states. However, consumer health data is not the same as other data collected, and it should be afforded added protections, which is exactly what this bill does. The upcoming revised draft of the bill has undergone robust stakeholder process, and the input from the technology and health care industry has made the bill stronger. The amended version addresses concerns about the overly broad definitions.

The legislators should ignore claims that this bill will cause the sky to fall and resist any attempts to weaken the bill, for example, by narrowing the definition of "consumer health data." Good definitions are important, and companies should have no problem complying with this straightforward law and its requirements for opt-in consent before collecting or sharing health data. The bill could be strengthened by removing the exemption for deidentified data.

(Opposed) The bill should apply equally to all medical facilities, including not only pregnancy resource centers, but also abortion facilities, gender-affirming care hospitals, specialized outpatient clinics, and other medical facilities. The bill should not be used by bureaucratic agencies to protect abortion and gender-care facilities.

(Other) The overly broad definitions would negatively alter the consumer experience and fail to accomplish the legislative intent of the bill. Without changes to key definitions, virtually all data would be included, including the purchase of everyday consumer products like toilet paper, deodorant, and even shoes. The definition of geofencing should be clarified that it refers to a precise location rather than a broad unbounded area. The operational provisions would be impossible to comply with because of the definitions, such as "sale" and "share," which are used differently throughout the bill.

The definition of "consumer health data" should be focused on uses because otherwise it would apply to a wide range of consumer data, even when that data is not used to facilitate the inference of health information. More precise definitions focused on reproductive or gender-affirming care would better accomplish the intended goals of this legislation. The

bill is essentially an omnibus privacy legislation that is entirely unaligned with other states' privacy laws and requires opt-in consent for consumers' normal everyday purchases.

The bill should provide regulated entities with the right to cure. If the bill is going to be enforced under the CPA, a consumer bringing a claim should be required to prove all five elements of a claim.

Today's passenger vehicles contain many complex safety features, including sensors that rely on facial detection technology, which is not the same as facial recognition technology, but the bill does not distinguish between these two different things. Additionally, the bill seems to require consent for auto companies to process data for the vehicle safety features.

The health care industry supports the goal of the bill to extend HIPAA-like protections to health care data that is not covered by the HIPAA. As currently drafted, there is a lack of clarity about what data is exempt. In addition to the HIPAA, there are other laws that protect health care data, and the bill should not duplicate that well-established regulatory framework.

Persons Testifying: (In support) Representative Vandana Slatter, prime sponsor; Stanley Shikuma, Japanese American Citizens League and La Resistencia; Andrea Alegrett, Washington State Attorney General's Office; Nicole Kern, Planned Parenthood Alliance Advocates; Danni Askini, Gender Justice League; Jon Pincus, Indivisible; Anuj Khattar, Cedar River Clinics; Sasha Wasserstrom, Washington Immigrant Solidarity Network; Alicia Hupprich, Pro-Choice Washington; Yvette Maganya, Legal Voice; and Jen Lee, American Civil Liberties Union of Washington.

(Opposed) Brad Payne, Family Policy Institute of Washington.

(Other) Andrew Kingman, State Privacy and Security Coalition; Mark Johnson, Washington Retail Association; Bob Battles, Association of Washington Business; Kelly Fukai, Washington Technology Industry Association; Ashley Sutton, TechNet; Felicity Slater, Future of Privacy Forum; Cara Helmer, Washington State Hospital Association; Ryan Spiller, Alliance for Automotive Innovation; Darbi Gottlieb; and Brian Warren, Biotechnology Innovation Organization.

Persons Signed In To Testify But Not Testifying: Maya Morales, Washington People's Privacy; Cher Scarlett; Irene Knapp; Uma Raghavan; and Mary Lynne Courtney, League of Women Voters of Washington.