FINAL BILL REPORT
ESHB 1155

C 191 L 23
Synopsis as Enacted

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

Sponsors: House Committee on Civil Rights & Judiciary (originally sponsored by 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).

House Committee on Civil Rights & Judiciary
Senate Committee on Law & Justice

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

---

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.

- 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:

The Washington My Health My Data Act (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.

"Small business" means a regulated entity that satisfies one or both of the following thresholds:
- collects, processes, sells, or shares consumer health data of fewer than 100,000 consumers during a calendar year; or
- controls, processes, sells, or shares consumer health data of fewer than 25,000 consumer and derives less than 50 percent of gross revenue from the collection, processing, selling, or sharing of consumer health data.

A regulated entity must comply with its obligations under the Act beginning on March 31,

2024. A small business must comply with its obligations under the Act beginning on June 30, 2024.

"Consumer health data" means 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. For the purposes of this definition, physical or mental health status includes includes:

- individual health conditions, treatment, diseases, or diagnoses;
- social, psychological, behavioral, and medical interventions;
- health-related surgeries or procedures, diagnostic testing, and treatment;
- use or purchase of prescribed medication;
- bodily functions, vital signs, symptoms, or related measurements;
- gender-affirming care information;
- reproductive or sexual health information;
- biometric and 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 a small business, or their respective processor, processes to associate or identify a consumer with the data 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 or small business 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 or small business shares consumer health data; and
- how a consumer may exercise consumer rights with regard to consumer health data.

A regulated entity or small business 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 or small business 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 or small business. 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 or small business 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 or small business 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 or small business is unable to authenticate a consumer request to exercise consumer rights using commercially reasonable efforts, the regulated entity or small business 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.

A regulated entity or small business that receives a deletion request must delete the consumer health data from its records and notify all affiliates, processors, and other third parties with whom the regulated entity or small business 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 or small business 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 or small business 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 or small business 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 or small business 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 or small business 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 or small business. 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 instructions or processes consumer health data in a manner that is outside the scope of the contract with the regulated entity or small business, the processor is considered a regulated entity or small business with regard to such data.

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 around an entity that provides in-

person health care services where such geofence is used to:

- identify or track consumers seeking health care services;
- collect consumer health data from consumers; or
- send notifications, messages, or advertisements to consumers related to their consumer health data or 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 spatial or location detection to establish a virtual boundary of 2,000 feet or less from the perimeter of a specific physical location or to locate a consumer within a virtual boundary.

Enforcement and Review of Enforcement Actions.
Violations are enforceable under the CPA.

The Joint Legislative Audit and Review Committee must review enforcement actions brought by the Attorney General and consumers to enforce the Act, and submit a report of its findings and recommendations to the Governor and the appropriate legislative committees by September 30, 2030.

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

Votes on Final Passage:

House	57	39	
Senate	27	21	(Senate amended)
House	57	40	(House concurred)

Effective: July 23, 2023