SENATE BILL REPORT
ESHB 1155

As of March 13, 2023

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: 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).

Brief History: Passed House: 3/4/23, 57-39.
Committee Activity: Law & Justice: 3/14/23.

Brief Summary of Bill

- Establishes consumer rights of access, withdraw consent, and deletion regarding consumer health data.
- Requires regulated entities to obtain consent in order to collect, share, or sell consumer health data.
- Specifies regulated entity obligations regarding consumer health data privacy notice, access, and security requirements.
- Prohibits implementing a geofence around an entity that provides in-person health care services to collect or track data from consumers or to send advertisements related to consumer health data.
- Exempts government agencies, tribal nations, and personal information governed by certain federal or state laws.
- Makes violations enforceable under the Consumer Protection Act.

SENATE COMMITTEE ON LAW & JUSTICE

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.

Staff: Angela Kleis (786-7469)

Background: Regulation of Health Care Information. *Federal Law.* The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established nationwide standards for using, disclosing, storing, and transferring protected health information (PHI). Covered entities and business associates subject to HIPAA must have an individual's authorization to use or disclose PHI unless a specified exception applies. Some exceptions pertain to disclosures for treatment, payment, and health care operations, research purposes, law enforcement purposes, and public health activities.

State Law. The Uniform Health Care Information Act governs the disclosure of health care information. A health care provider or an agent and employee of a health care provider may not disclose a patient's health care information without written authorization unless a statutory exceptions applies. Statutory exceptions include disclosures made for the provision of health care, research purposes, law enforcement activities, and protection of public health.

Washington Consumer Protections. 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 (AG) 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 private 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.

In 1986, the state Supreme Court issued a decision that established a test for all private actions under the CPA, which requires a plaintiff to prove five elements: an unfair or deception act or practice, occurs in trade or commerce, public interest impact, injury to plaintiff's business or property, and causation.

Summary of Bill: Short Title. This act may be known as the Washington My Health My Data Act (act).

Consumer Health Data Rights. A consumer has the right to access, delete, and withdraw consent from the collection, sharing, or selling of their consumer health data (health data). A consumer may exercise these rights by submitting a request to a regulated entity at any time.

Regulated Entity Obligations. A regulated entity must establish a secure, reliable means for a consumer to submit a request to exercise any health data rights and may not unlawfully discriminate against a consumer for exercising any of these rights.

Responding to Requests. If a regulated entity is unable to authenticate a request, the regulated entity is not required to comply with a consumer's request and may request the

consumer to provide additional information reasonably necessary for authentication.

A regulated entity must respond to the consumer within 45 days of receipt of the request, which may be extended once by 45 additional days under specified circumstances. Information provided in response to a consumer request must be provided free of charge, up to twice annually per consumer.

Within 30 days from authenticating a request to delete health data, a regulated entity must delete such data and notify all entities with whom the health data was shared of the deletion request and such entities must honor the consumer's deletion request. If health data subject to a deletion request is stored on archived or backup systems, then the deletion request may be delayed up to six months to enable restoration of such systems.

Appeals Process. 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. If the appeal is denied, the regulated entity must also provide the consumer with a method to contact the AG to submit a complaint.

Consent. A regulated entity may not collect or share any health data except with consumer consent for such collection for a specified purpose, with consumer consent for such sharing that is separate from the consent obtained to collect health data, or to the extent necessary to provide a product or service requested by the consumer. Consent must be obtained prior to the collection or sharing of any health data. The request for consent must clearly disclose specified information.

Privacy Policy. A regulated entity must maintain a health data privacy policy that discloses specified information such as the categories of health data collected and shared, the purpose for which health data is collected, and how a consumer can exercise the rights provided in this act. A regulated entity must publish a link to its health data privacy policy on its homepage.

Restriction of Access and Security. A regulated entity must restrict access to health data to only those employees, processors, and contractors for which access is necessary to further the purposes for which the consumer provided consent or where necessary to provide a product or service requested by a consumer.

A regulated entity must establish, implement, and maintain data security practices that, at a minimum, satisfy reasonable standard of care within the regulated entity's industry to protect the confidentiality, integrity, and accessibility of health data, as appropriate.

Processor Obligations. A processor may process health data only pursuant to a binding contract between the processor and the regulated entity. If a processor fails to adhere to the regulated entity's instructions or processes health data in a manner that is outside the scope

of the processor's contract with the regulated entity, the processor is considered a regulated entity with regard to such data and is subject to all the requirements of this act.

Valid Authorization. It is unlawful for any person to sell or offer to sell health data without first obtaining valid authorization from a consumer. An authorization to sell health data must be written in plain language, expires one year from when the consumer signs it, and is a document that contains specified information such as the contact information of persons collecting, selling, and purchasing the health data. A copy of the authorization must be provided to the consumer. The seller and purchaser of health data must retain a copy of all authorizations for six years.

Geofencing. 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 health data from consumers, or send notifications, messages, or advertisements to consumers related to their health data or health care services.

Enforcement. In actions brought by the AG, the Legislature finds that the practices covered by this act are matters vitally affecting the public interest for the purposes of applying the CPA. A violation of this act is not reasonable in relation to the development and preservation of business, and is an unfair or deceptive act in trade or commerce, and an unfair method of competition for the purposes of applying the CPA. Any consumer injured by a violation of this act may bring an action under the CPA, but must establish all required elements of an action under the CPA before relief may be granted.

Exemptions. This act does not apply to government agencies, tribal nations, or personal information governed by certain federal or state laws. The obligations of this act imposed on regulated entities and processors does not restrict their ability for collection, use, or disclosure of health data for specified purposes such as to prevent or respond to security incidents. If a regulated entity or processor processes health data for a specified exemption, such entity bears the burden of demonstrating that such processing qualifies for the exemption.

Miscellaneous. The bill includes a severability clause.

Appropriation: None.

Fiscal Note: Available.

Creates Committee/Commission/Task Force that includes Legislative members: No.

Effective Date: Ninety days after adjournment of session in which bill is passed.