

SENATE BILL REPORT

ESHB 1155

As Reported by Senate Committee On:
Law & Justice, March 22, 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, 3/22/23 [DPA, DNP, w/oRec].

Brief Summary of Amended 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.
- Provides an effective date of March 31, 2024, for sections of the bill

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.

related to consumer health data rights, regulated entity and processor obligations, and valid authorization.

SENATE COMMITTEE ON LAW & JUSTICE

Majority Report: Do pass as amended.

Signed by Senators Dhingra, Chair; Trudeau, Vice Chair; Kuderer, Pedersen, Salomon and Valdez.

Minority Report: Do not pass.

Signed by Senators Padden, Ranking Member; McCune, Torres and Wilson, L..

Minority Report: That it be referred without recommendation.

Signed by Senator Wagoner.

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 Amended 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. A regulated entity must take steps to authenticate a request but this must not extend the regulated entity's duty to comply with a request within 45 day. Information provided in response to a consumer request must be provided free of charge, up to twice annually per consumer.

Upon receipt of deletion request, a regulated entity must delete such data and notify all entities with whom the health data was shared 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. 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.

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 that are illegal under Washington state law or federal law. 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.

Effective Date. The sections of the bill related to consumer health data rights, regulated entity and processor obligations, and valid authorization take effect March 31, 2024.

EFFECT OF LAW & JUSTICE COMMITTEE AMENDMENT(S):

- Clarifies the definitions of consumer health data, deidentified data, geofence, personal information, and share.
- Removes the requirement for a regulated entity to respond to a request to delete health data without unreasonable delay and no more than 30 calendar days from authenticating the deletion request.
- Clarifies that authenticating a consumer's request to exercise a right does not extend the regulated entity's 45-day timeline for responding to a request.
- Removes the specification that the legislative declarations that make a violation of the bill a per se violation of the CPA apply in enforcement actions brought by the attorney general.
- Removes the requirement for any consumer injured by a violation of this chapter and bringing an action under the CPA to establish all required elements of an action under the CPA before relief may be granted.
- Adds exemptions for information processed by certain federally regulated medical device manufacturers and information that is part of a limited data set and is maintained in a manner required under HIPAA or identifiable data disclosed in the electronic sales tracking system implemented by the state pharmacy quality assurance commission and consistent with the federal combat meth act.
- Specifies that the exemption for responding to illegal activities and prosecuting those responsible for such actions applies to activities and actions that are illegal under Washington State law or federal law.
- Provides an effective date of March 31, 2024, for sections of the bill related to consumer health data rights, regulated entity and processor obligations, and valid authorization.

Appropriation: None.

Fiscal Note: Available.

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

Effective Date: The bill contains several effective dates. Please refer to the bill.

Staff Summary of Public Testimony on Engrossed Substitute House Bill: *The committee recommended a different version of the bill than what was heard.* PRO: This bill is about protecting the freedom and dignity to make private healthcare decisions and preventing vulnerabilities that can harm people. Not all health data is protected under federal laws like HIPAA. HIPAA protects data collected by covered entities and business associates. Data covered by apps, websites, and non-HIPAA covered entities are vulnerable. People are travelling to Washington for reproductive healthcare and gender affirming care. This bill would protect people from harassment and invasion of privacy and even prosecution for making their own healthcare decisions. The current bill creates potentially insurmountable barriers for people to hold companies that violate their rights accountable to protect Washingtonians.

OTHER: There is concern with the definition of consumer health data. As currently defined, the language goes beyond the most sensitive consumer health data. The protected data would include anything construed to be health data. Everyday activities would invoke opt in consent notifications. The unintended consequences of an expansive scope will water down the intent of the legislation, creating a deluge of opt in notifications which obscures the goal of the bill to provide opt in consent for truly sensitive healthcare data. There must be a workable and effective regulatory system that will produce predictable results for Washington consumers and businesses.

Persons Testifying: PRO: Representative Vandana Slatter, Prime Sponsor; Alicia Hupprich; Rachel Clavette; Danni Askini, Gender Justice League; Sally Richardson; Dr. Anuj Khattar, Cedar River Clinics; Nicole Kern, Planned Parenthood Alliance Advocates; Cher Scarlett; Jen Lee, ACLU of Washington; Joyce Bruce, WA State Attorney General's Office; Andrea Alegrett, WA State Attorney General's Office.

OTHER: Mark Johnson, Washington Retail Association; Ashley Sutton, TechNet; Kelly Fukai, Washington Technology Industry Association; Bob Battles, Association Washington Business; Andy Kingman, State Privacy and Security Coalition; Larry Shannon, WSAJ.

Persons Signed In To Testify But Not Testifying: PRO: Vera Cooley; Sasha Wasserstrom, WA Immigrant Solidarity Network; Yvette Maganya, Legal Voice; Sarah Dixit, Planned Parenthood Advocates of Greater WA and Idaho.

OTHER: Christine Kohnert, No organization - a group of individual women; Cynthia Spiess, No organization - a group of individual women; Karen Studders, No organization - a group of individual women; Maya Morales, WA People's Privacy (Other = Strengthen).