Z-0302.1

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SENATE BILL 5351**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**State of Washington 68th Legislature 2023 Regular Session**

**By** Senators Dhingra, Billig, Boehnke, Hasegawa, Hunt, Keiser, Kuderer, Lovelett, Lovick, Nguyen, Nobles, Pedersen, Randall, Rivers, Rolfes, Salomon, Shewmake, Stanford, Trudeau, Valdez, C. Wilson, and J. Wilson; by request of Attorney General

AN ACT Relating to the collection, sharing, and selling of consumer health data; and adding a new chapter to Title 19 RCW.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. **Sec.**  This act may be known and cited as the Washington my health my data act.

NEW SECTION. **Sec.**  (1) The legislature finds that the people of Washington regard their privacy as a fundamental right and an essential element of their individual freedom. Washington's Constitution explicitly provides the right to privacy. Fundamental privacy rights have long been and continue to be integral to protecting Washingtonians and to safeguarding our democratic republic.

(2) Information related to an individual's health conditions or attempts to obtain health care services is among the most personal and sensitive categories of data collected. Washingtonians expect that their health data is protected under laws like the health information portability and accountability act (HIPAA). However, HIPAA only covers health data collected by specific health care entities, including most health care providers. Health data collected by noncovered entities, including certain apps and websites, are not afforded the same protections. This act works to close the gap between consumer knowledge and industry practice by providing stronger privacy protections for all Washington consumers' health data.

(3) With this act, the legislature intends to provide heightened protections for Washingtonian's health data by: Requiring additional disclosures and consumer consent regarding the collection, sharing, and use of such information; empowering consumers with the right to have their health data deleted; prohibiting the selling of consumer health data; and making it unlawful to utilize a geofence around a facility that provides health care services.

NEW SECTION. **Sec.**  The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Abortion" means the termination of a pregnancy for purposes other than producing a live birth.

(2) "Affiliate" means a legal entity that shares common branding with another legal entity and controls, is controlled by, or is under common control with another legal entity. For the purposes of this definition, "control" or "controlled" means:

(a) Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company;

(b) Control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(c) The power to exercise controlling influence over the management of a company.

(3) "Biometric data" means data generated from the measurement or technological processing of an individual's physiological, biological, or behavioral characteristics that can be used individually or in combination with other data to identify a consumer. Biometric data includes, but is not limited to:

(a) Imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted; or

(b) Keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(4) "Collect" means to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any manner.

(5)(a) "Consent" means a clear affirmative act by a consumer that openly communicates a consumer's freely given, informed, opt-in, voluntary, specific, and unambiguous written consent, which may include written consent provided by electronic means.

(b) "Consent" cannot be obtained by:

(i) A consumer's acceptance of a general or broad terms of use agreement or a similar document that contains descriptions of personal data processing along with other unrelated information;

(ii) A consumer hovering over, muting, pausing, or closing a given piece of content; or

(iii) A consumer's agreement obtained through the use of deceptive designs.

(6) "Consumer" means (a) a natural person who is a Washington resident; or (b) a natural person whose consumer health data is collected in Washington. "Consumer" means a natural person who acts only in an individual or household context, however identified, including by any unique identifier. "Consumer" does not include an individual acting in an employment context.

(7)(a) "Consumer health data" means personal information relating to the past, present, or future physical or mental health of a consumer including, but not limited to, any personal information relating to:

(i) Individual health conditions, treatment, status, diseases, or diagnoses;

(ii) Social, psychological, behavioral, and medical interventions;

(iii) Health-related surgeries or procedures;

(iv) Use or purchase of medication;

(v) Bodily functions, vital signs, symptoms, or measurements of the information described in this subsection;

(vi) Diagnoses or diagnostic testing, treatment, or medication;

(vii) Efforts to research or obtain health services or supplies;

(viii) Gender-affirming care information;

(ix) Reproductive or sexual health information;

(x) Biometric data related to information described in this subsection (7)(a);

(xi) Genetic data related to information described in this subsection (7)(a);

(xii) Location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies; or

(xiii) Any information described in (a)(i) through (xii) of this subsection that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).

(b) "Consumer health data" does not include personal information that is used to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity that determines that the regulated entity has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

(8) "Deceptive design" means a user interface designed or manipulated with the potential effect of subverting or impairing user autonomy, decision making, or choice.

(9) "Deidentified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the regulated entity that possesses such data (a) takes reasonable measures to ensure that such data cannot be associated with an individual; (b) publicly commits to process such data only in a deidentified fashion and not attempt to reidentify such data; and (c) contractually obligates any recipients of such data to satisfy the criteria set forth in (a) and (b) of this subsection.

(10) "Gender-affirming care information" means personal information relating to seeking or obtaining past, present, or future gender-affirming care services. "Gender-affirming care information" includes, but is not limited to:

(a) Location information that could reasonably indicate a consumer's attempt to acquire or receive gender-affirming care services;

(b) Efforts to research or obtain gender-affirming care services; or

(c) Any gender-affirming care information that is derived, extrapolated, or inferred, including from nonhealth information, such as proxy, derivative, inferred, emergent, or algorithmic data.

(11) "Gender-affirming care services" means health services or products that support and affirm an individual's gender identity including, but not limited to, social, psychological, behavioral, cosmetic, medical, or surgical interventions. "Gender-affirming care services" includes, but is not limited to, treatments for gender dysphoria, gender-affirming hormone therapy, and gender-affirming surgical procedures.

(12) "Genetic data" means any data, regardless of its format, that concerns a consumer's genetic characteristics. "Genetic data" includes, but is not limited to:

(a) Raw sequence data that result from the sequencing of a consumer's complete extracted deoxyribonucleic acid (DNA) or a portion of the extracted DNA;

(b) Genotypic and phenotypic information that results from analyzing the raw sequence data; and

(c) Self-reported health data that a consumer submits to a regulated entity and that is analyzed in connection with consumer's raw sequence data.

(13) "Geofence" means technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wifi data, and/or any other form of location detection to establish a virtual boundary around a specific physical location.

(14) "Health care services" means any service provided to a person to assess, measure, improve, or learn about a person's health, including but not limited to:

(a) Individual health conditions, status, diseases, or diagnoses;

(b) Social, psychological, behavioral, and medical interventions;

(c) Health-related surgeries or procedures;

(d) Use or purchase of medication;

(e) Bodily functions, vital signs, symptoms, or measurements of the information described in this subsection;

(f) Diagnoses or diagnostic testing, treatment, or medication;

(g) Reproductive health care services; or

(h) Gender-affirming care services.

(15) "Homepage" means the introductory page of an internet website and any internet webpage where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, and a link within the application, such as from the application configuration, "about," "information," or settings page.

(16) "Person" shall include, where applicable, natural persons, corporations, trusts, unincorporated associations, and partnerships.

(17)(a) "Personal information" means information that identifies, relates to, describes, or is reasonably capable of being associated or linked, directly or indirectly, with a particular consumer. "Personal information" includes, but is not limited to, data associated with a persistent unique identifier, such as a cookie ID, an IP address, a device identifier, or any other form of persistent unique identifier.

(b) "Personal information" does not include publicly available information. For purposes of this subsection, "publicly available" means information that is lawfully made available from federal, state, or local government records. Any biometric data collected about a consumer by a business without the consumer's knowledge is not publicly available information.

(c) "Personal information" does not include deidentified data.

(18) "Process" or "processing" means any operation or set of operations performed on consumer health data.

(19) "Regulated entity" means any legal entity that (a) conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington; (b) collects, shares, or sells consumer health data; and (c) determines the purpose and means of the processing of consumer health data. "Regulated entity" does not mean government agencies or tribal nations.

(20) "Reproductive or sexual health information" means personal information relating to seeking or obtaining past, present, or future reproductive or sexual health services. "Reproductive or sexual health information" includes, but is not limited to:

(a) Location information that could reasonably indicate a consumer's attempt to acquire or receive reproductive or sexual health services;

(b) Efforts to research or obtain reproductive or sexual health services; or

(c) Any reproductive or sexual health information that is derived, extrapolated, or inferred, including from nonhealth information (such as proxy, derivative, inferred, emergent, or algorithmic data).

(21) "Reproductive or sexual health services" means health services or products that support or relate to an individual's reproductive system or sexual well-being, including but not limited to:

(a) Individual health conditions, status, diseases, or diagnoses;

(b) Social, psychological, behavioral, and medical interventions;

(c) Health-related surgeries or procedures including, but not limited to, abortions;

(d) Use or purchase of medication including, but not limited to, medications for the purposes of abortion;

(e) Bodily functions, vital signs, symptoms, or measurements of the information described in this subsection;

(f) Diagnoses or diagnostic testing, treatment, or medication; and

(g) Medical or nonmedical services related to and provided in conjunction with an abortion, including but not limited to associated diagnostics, counseling, supplies, and follow-up services.

(22)(a) "Sell" or "sale" means the sharing of consumer health data for monetary or other valuable consideration.

(b) "Sell" or "sale" does not include the sharing of consumer health data for monetary or other valuable consideration:

(i) 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 that shall comply with the requirements and obligations in this chapter;

(ii) By a natural person selling their own consumer health data pursuant to a written contract of sale with a third party; or

(iii) By a regulated entity to a service provider when such sharing is consistent with the purpose for which the consumer health data was collected and disclosed to the consumer.

(23) "Service provider" means a person that processes consumer health data on behalf of a regulated entity.

(24)(a) "Share" or "sharing" means to release, disclose, disseminate, divulge, make available, provide access to, license, or otherwise communicate orally, in writing, or by electronic or other means, consumer health data by a regulated entity to a third party or affiliate.

(b) The term "share" or "sharing" does not include:

(i) The disclosure of consumer health data by a regulated entity to a service provider when such sharing is consistent with the purpose for which the consumer health data was collected and disclosed to the consumer;

(ii) The disclosure of consumer health data to a third party with whom the consumer has a direct relationship when: (A) The disclosure is for purposes of providing a product or service requested by the consumer; (B) the regulated entity maintains control and ownership of the data; and (C) the third party uses the consumer health data only at direction from the regulated entity and consistent with the purpose for which it was collected and disclosed to the consumer; or

(iii) The disclosure or transfer of personal data 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 and shall comply with the requirements and obligations in this chapter.

(25) "Third party" means an entity other than a consumer, regulated entity, service provider, or affiliate of the regulated entity.

NEW SECTION. **Sec.**  (1) A regulated entity shall maintain a consumer health data privacy policy that clearly and conspicuously discloses:

(a) The specific types of consumer health data collected and the purpose for which the data is collected, including the specific ways in which it will be used;

(b) The sources from which the consumer health data is collected;

(c) The specific consumer health data that is shared;

(d) A list of third parties and affiliates with whom the regulated entity shares the consumer health data, including an active email address or other online mechanism that the consumer may use to contact these third parties and affiliates; and

(e) How a consumer can exercise the rights provided in section 6 of this act.

(2) A regulated entity shall prominently publish its consumer health data privacy policy on its homepage.

(3) A regulated entity may not collect, use, or share additional categories of consumer health data not disclosed in the consumer health data privacy policy without first disclosing the additional categories and obtaining the consumer's affirmative consent prior to the collection, use, or sharing of such consumer health data.

(4) A regulated entity may not collect, use, or share consumer health data for additional purposes not disclosed in the consumer health data privacy policy without first disclosing the additional purposes and obtaining the consumer's affirmative consent prior to the collection, use, or sharing of such consumer health data.

(5) It is a violation of this chapter for a regulated entity to 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.

NEW SECTION. **Sec.**  (1) A regulated entity may not collect any consumer health data except:

(a) With consent from the consumer for such collection for a specified purpose; or

(b) To the extent strictly necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity.

(2) A regulated entity may not share any consumer health data except:

(a) With consent from the consumer for such sharing that is separate and distinct from the consent obtained to collect consumer health data; or

(b) To the extent strictly necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity.

(3) Consent required under this section must be obtained prior to the collection or sharing, as applicable, of any consumer health data, and the request for consent must clearly and conspicuously disclose: (a) The categories of consumer health data collected or shared; (b) the purpose of the collection or sharing of the consumer health data, including the specific ways in which it will be used; (c) the entities with whom the consumer health data is shared; and (d) how the consumer can withdraw consent from future collection or sharing of the consumer's health data.

(4) A regulated entity may not discriminate against a consumer for exercising any rights included in this chapter.

NEW SECTION. **Sec.**  (1) A consumer has the right to confirm whether a regulated entity is collecting or sharing consumer health data concerning the consumer and to access such data.

(2) A consumer has the right to confirm that a regulated entity has not sold consumer health data concerning the consumer.

(3) A consumer has the right to withdraw consent from the regulated entity's collection and sharing of consumer health data concerning the consumer.

(4) A consumer has the right to have consumer health data concerning the consumer deleted and may exercise that right by informing the regulated entity of the consumer's request for deletion.

(a) A regulated entity that receives a consumer's request to delete any consumer health data concerning the consumer shall without unreasonable delay and no more than 30 calendar days from receiving the deletion request:

(i) Delete the consumer health data from its records, including from all parts of the regulated entity's network or backup systems; and

(ii) Notify all affiliates, service providers, contractors, and other third parties with whom the regulated entity has shared consumer health data of the deletion request.

(b) All affiliates, service providers, contractors, and other third parties that receive notice of a consumer's deletion request shall honor the consumer's deletion request and delete the consumer health data from its records, including from all parts of its network or backup systems.

(5) A consumer may exercise the rights set forth in this chapter by submitting a request, at any time, to a regulated entity. Such a request may be made by contacting the regulated entity through the manner included in its consumer health data privacy policy.

NEW SECTION. **Sec.**  (1) A regulated entity shall restrict access to consumer health data by the employees, service providers, and contractors of such regulated entity to only those employees, service providers, and contractors for which access is necessary to further the purposes for which the consumer provided consent or where strictly necessary to provide a product or service that the consumer to whom such data and information relates has requested from such regulated entity.

(2) A regulated entity shall establish, implement, 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 the confidentiality, integrity, and accessibility of consumer health data appropriate to the volume and nature of the personal data at issue.

NEW SECTION. **Sec.**  (1)(a) A service provider may process consumer health data only pursuant to a binding contract between the service provider and the regulated entity that sets forth the processing instructions and limit the actions the service provider may take with respect to the consumer health data it processes on behalf of the regulated entity.

(b) A service provider may process consumer health data only in a manner that is consistent with the binding instructions set forth in the contract with the regulated entity.

(2) A service provider shall assist the regulated entity by appropriate technical and organizational measures, insofar as this is possible, in fulfilling the regulated entity's obligations under this chapter.

(3) 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 and is subject to all the requirements of this chapter.

NEW SECTION. **Sec.**  It is unlawful for any person including, but not limited to, regulated entities or service providers, to sell consumer health data.

NEW SECTION. **Sec.**  It is unlawful for any person to implement a geofence around any entity that provides in-person health care services where such geofence is used to identify, track, collect data from, or send notifications or messages to a consumer that enters the virtual perimeter.

NEW SECTION. **Sec.**  The legislature finds that the practices covered by this chapter are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. A violation of this chapter 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 purpose of applying the consumer protection act, chapter 19.86 RCW.

NEW SECTION. **Sec.**  (1) This chapter does not apply to:

(a) Protected health information, or information treated like protected health information, collected, used, or disclosed by covered entities and business associates when: (i) The protected health information is collected, used, or disclosed in accordance with the federal health insurance portability and accountability act of 1996 and the health information technology for economic and clinical health act, 45 C.F.R. Parts 160 and 164, and its implementing regulations; and (ii) the protected health information is afforded all the privacy protections and security safeguards of those federal laws and their implementing regulations. For the purpose of this subsection (1), "protected health information," "covered entity," and "business associate" have the same meaning as in the federal health insurance portability and accountability act of 1996 and its implementing regulations;

(b) Patient identifying information collected, used, or disclosed in accordance with 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2; or

(c) Health care information collected, used, or disclosed in accordance with chapter 70.02 RCW.

(2) Nothing in this chapter shall be construed to prohibit disclosure as required under chapters 26.44 and 74.34 RCW.

NEW SECTION. **Sec.**  If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected.

NEW SECTION. **Sec.**  Sections 1 through 12 of this act constitute a new chapter in Title 19 RCW.

**--- END ---**