

ESHB 1155 - S AMD 270
By Senator Dhingra

ADOPTED AS AMENDED 04/05/2023

1 Strike everything after the enacting clause and insert the
2 following:

3 "NEW SECTION. **Sec. 1.** This act may be known and cited as the
4 Washington my health my data act.

5 NEW SECTION. **Sec. 2.** (1) The legislature finds that the people
6 of Washington regard their privacy as a fundamental right and an
7 essential element of their individual freedom. Washington's
8 Constitution explicitly provides the right to privacy. Fundamental
9 privacy rights have long been and continue to be integral to
10 protecting Washingtonians and to safeguarding our democratic
11 republic.

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

24 (3) With this act, the legislature intends to provide heightened
25 protections for Washingtonian's health data by: Requiring additional
26 disclosures and consumer consent regarding the collection, sharing,
27 and use of such information; empowering consumers with the right to
28 have their health data deleted; prohibiting the selling of consumer
29 health data without valid authorization signed by the consumer; and
30 making it unlawful to utilize a geofence around a facility that
31 provides health care services.

1 NEW SECTION. **Sec. 3.** The definitions in this section apply
2 throughout this chapter unless the context clearly requires
3 otherwise.

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

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

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

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

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

16 (3) "Authenticate" means to use reasonable means to determine
17 that a request to exercise any of the rights afforded in this chapter
18 is being made by, or on behalf of, the consumer who is entitled to
19 exercise such consumer rights with respect to the consumer health
20 data at issue.

21 (4) "Biometric data" means data that is generated from the
22 measurement or technological processing of an individual's
23 physiological, biological, or behavioral characteristics and that
24 identifies a consumer, whether individually or in combination with
25 other data. Biometric data includes, but is not limited to:

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

29 (b) Keystroke patterns or rhythms and gait patterns or rhythms
30 that contain identifying information.

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

34 (6) (a) "Consent" means a clear affirmative act that signifies a
35 consumer's freely given, specific, informed, opt-in, voluntary, and
36 unambiguous agreement, which may include written consent provided by
37 electronic means.

38 (b) "Consent" may not be obtained by:

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

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

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

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

14 (8) (a) "Consumer health data" means personal information that is
15 linked or reasonably linkable to a consumer and that identifies the
16 consumer's past, present, or future physical or mental health status.

17 (b) For the purposes of this definition, physical or mental
18 health status includes, but is not limited to:

19 (i) Individual health conditions, treatment, diseases, or
20 diagnosis;

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

23 (iii) Health-related surgeries or procedures;

24 (iv) Use or purchase of prescribed medication;

25 (v) Bodily functions, vital signs, symptoms, or measurements of
26 the information described in this subsection (8) (b);

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

28 (vii) Gender-affirming care information;

29 (viii) Reproductive or sexual health information;

30 (ix) Biometric data;

31 (x) Genetic data;

32 (xi) Precise location information that could reasonably indicate
33 a consumer's attempt to acquire or receive health services or
34 supplies;

35 (xii) Data that identifies a consumer seeking health care
36 services; or

37 (xiii) Any information that a regulated entity or a small
38 business, or their respective processor, processes to associate or
39 identify a consumer with the data described in (b) (i) through (xii)
40 of this subsection that is derived or extrapolated from nonhealth

1 information (such as proxy, derivative, inferred, or emergent data by
2 any means, including algorithms or machine learning).

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

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

16 (10) "Deidentified data" means data that cannot reasonably be
17 used to infer information about, or otherwise be linked to, an
18 identified or identifiable consumer, or a device linked to such
19 consumer, if the regulated entity or the small business that
20 possesses such data (a) takes reasonable measures to ensure that such
21 data cannot be associated with a consumer; (b) publicly commits to
22 process such data only in a deidentified fashion and not attempt to
23 reidentify such data; and (c) contractually obligates any recipients
24 of such data to satisfy the criteria set forth in this subsection
25 (10).

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

30 (a) Precise location information that could reasonably indicate a
31 consumer's attempt to acquire or receive gender-affirming care
32 services;

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

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

38 (12) "Gender-affirming care services" means health services or
39 products that support and affirm an individual's gender identity
40 including, but not limited to, social, psychological, behavioral,

1 cosmetic, medical, or surgical interventions. "Gender-affirming care
2 services" includes, but is not limited to, treatments for gender
3 dysphoria, gender-affirming hormone therapy, and gender-affirming
4 surgical procedures.

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

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

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

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

16 (14) "Geofence" means technology that uses global positioning
17 coordinates, cell tower connectivity, cellular data, radio frequency
18 identification, Wifi data, and/or any other form of spatial or
19 location detection to establish a virtual boundary around a specific
20 physical location, or to locate a consumer within a virtual boundary.
21 For purposes of this definition, "geofence" means a virtual boundary
22 that is 2,000 feet or less from the perimeter of the physical
23 location.

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

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

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

29 (c) Health-related surgeries or procedures;

30 (d) Use or purchase of medication;

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

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

34 (g) Reproductive health care services; or

35 (h) Gender-affirming care services.

36 (16) "Homepage" means the introductory page of an internet
37 website and any internet webpage where personal information is
38 collected. In the case of an online service, such as a mobile
39 application, homepage means the application's platform page or

1 download page, and a link within the application, such as from the
2 application configuration, "about," "information," or settings page.

3 (17) "Person" means, where applicable, natural persons,
4 corporations, trusts, unincorporated associations, and partnerships.
5 "Person" does not include government agencies, tribal nations, or
6 contracted service providers when processing consumer health data on
7 behalf of a government agency.

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

14 (b) "Personal information" does not include publicly available
15 information.

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

17 (19) "Precise location information" means information derived
18 from technology including, but not limited to, global positioning
19 system level latitude and longitude coordinates or other mechanisms,
20 that directly identifies the specific location of an individual with
21 precision and accuracy within a radius of 1,750 feet. "Precise
22 location information" does not include the content of communications,
23 or any data generated by or connected to advanced utility metering
24 infrastructure systems or equipment for use by a utility.

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

27 (21) "Processor" means a person that processes consumer health
28 data on behalf of a regulated entity or a small business.

29 (22) "Publicly available information" means information that (a)
30 is lawfully made available through federal, state, or municipal
31 government records or widely distributed media, and (b) a regulated
32 entity or a small business has a reasonable basis to believe a
33 consumer has lawfully made available to the general public. "Publicly
34 available information" does not include any biometric data collected
35 about a consumer by a business without the consumer's consent.

36 (23) "Regulated entity" means any legal entity that: (a) Conducts
37 business in Washington, or produces or provides products or services
38 that are targeted to consumers in Washington; and (b) alone or
39 jointly with others, determines the purpose and means of collecting,
40 processing, sharing, or selling of consumer health data. "Regulated

1 entity" does not mean government agencies, tribal nations, or
2 contracted service providers when processing consumer health data on
3 behalf of the government agency.

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

8 (a) Precise location information that could reasonably indicate a
9 consumer's attempt to acquire or receive reproductive or sexual
10 health services;

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

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

17 (25) "Reproductive or sexual health services" means health
18 services or products that support or relate to a consumer's
19 reproductive system or sexual well-being, including but not limited
20 to:

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

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

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

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

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

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

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

34 (26)(a) "Sell" or "sale" means the exchange of consumer health
35 data for monetary or other valuable consideration.

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

38 (i) To a third party as an asset that is part of a merger,
39 acquisition, bankruptcy, or other transaction in which the third
40 party assumes control of all or part of the regulated entity's or the

1 small business's assets that complies with the requirements and
2 obligations in this chapter; or

3 (ii) By a regulated entity or a small business to a processor
4 when such exchange is consistent with the purpose for which the
5 consumer health data was collected and disclosed to the consumer.

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

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

12 (i) The disclosure of consumer health data by a regulated entity
13 or a small business to a processor when such sharing is to provide
14 goods or services in a manner consistent with the purpose for which
15 the consumer health data was collected and disclosed to the consumer;

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

24 (iii) The disclosure or transfer of personal data to a third
25 party as an asset that is part of a merger, acquisition, bankruptcy,
26 or other transaction in which the third party assumes control of all
27 or part of the regulated entity's or the small business's assets and
28 complies with the requirements and obligations in this chapter.

29 (28) "Small business" means a regulated entity that satisfies one
30 or both of the following thresholds:

31 (a) Collects, processes, sells, or shares consumer health data of
32 fewer than 100,000 consumers during a calendar year; or

33 (b) Derives less than 50 percent of gross revenue from the
34 collection, processing, selling, or sharing of consumer health data,
35 and controls, processes, sells, or shares consumer health data of
36 fewer than 25,000 consumers.

37 (29) "Third party" means an entity other than a consumer,
38 regulated entity, processor, small business, or affiliate of the
39 regulated entity or the small business.

1 NEW SECTION. **Sec. 4.** (1)(a) Except as provided in subsection
2 (2) of this section, beginning March 31, 2024, a regulated entity and
3 a small business shall maintain a consumer health data privacy policy
4 that clearly and conspicuously discloses:

5 (i) The categories of consumer health data collected and the
6 purpose for which the data is collected, including how the data will
7 be used;

8 (ii) The categories of sources from which the consumer health
9 data is collected;

10 (iii) The categories of consumer health data that is shared;

11 (iv) A list of the categories of third parties and specific
12 affiliates with whom the regulated entity or the small business
13 shares the consumer health data; and

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

16 (b) A regulated entity and a small business shall prominently
17 publish a link to its consumer health data privacy policy on its
18 homepage.

19 (c) A regulated entity or a small business may not collect, use,
20 or share additional categories of consumer health data not disclosed
21 in the consumer health data privacy policy without first disclosing
22 the additional categories and obtaining the consumer's affirmative
23 consent prior to the collection, use, or sharing of such consumer
24 health data.

25 (d) A regulated entity or a small business may not collect, use,
26 or share consumer health data for additional purposes not disclosed
27 in the consumer health data privacy policy without first disclosing
28 the additional purposes and obtaining the consumer's affirmative
29 consent prior to the collection, use, or sharing of such consumer
30 health data.

31 (e) It is a violation of this chapter for a regulated entity or a
32 small business to contract with a processor to process consumer
33 health data in a manner that is inconsistent with the regulated
34 entity's or the small business's consumer health data privacy policy.

35 (2) A small business must comply with this section beginning June
36 30, 2024.

37 NEW SECTION. **Sec. 5.** (1)(a) Except as provided in subsection
38 (2) of this section, beginning March 31, 2024, a regulated entity or
39 a small business may not collect any consumer health data except:

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

3 (ii) To the extent necessary to provide a product or service that
4 the consumer to whom such consumer health data relates has requested
5 from such regulated entity or small business.

6 (b) A regulated entity or a small business may not share any
7 consumer health data except:

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

11 (ii) To the extent necessary to provide a product or service that
12 the consumer to whom such consumer health data relates has requested
13 from such regulated entity or small business.

14 (c) Consent required under this section must be obtained prior to
15 the collection or sharing, as applicable, of any consumer health
16 data, and the request for consent must clearly and conspicuously
17 disclose: (i) The categories of consumer health data collected or
18 shared; (ii) the purpose of the collection or sharing of the consumer
19 health data, including the specific ways in which it will be used;
20 (iii) the categories of entities with whom the consumer health data
21 is shared; and (iv) how the consumer can withdraw consent from future
22 collection or sharing of the consumer's health data.

23 (d) A regulated entity or a small business may not unlawfully
24 discriminate against a consumer for exercising any rights included in
25 this chapter.

26 (2) A small business must comply with this section beginning June
27 30, 2024.

28 NEW SECTION. **Sec. 6.** (1)(a) Except as provided in subsection
29 (2) of this section, beginning March 31, 2024, a consumer has the
30 right to confirm whether a regulated entity or a small business is
31 collecting, sharing, or selling consumer health data concerning the
32 consumer and to access such data, including a list of all third
33 parties and affiliates with whom the regulated entity or the small
34 business has shared or sold the consumer health data and an active
35 email address or other online mechanism that the consumer may use to
36 contact these third parties.

37 (b) A consumer has the right to withdraw consent from the
38 regulated entity's or the small business's collection and sharing of
39 consumer health data concerning the consumer.

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

5 (i) A regulated entity or a small business that receives a
6 consumer's request to delete any consumer health data concerning the
7 consumer shall:

8 (A) Delete the consumer health data from its records, including
9 from all parts of the regulated entity's or the small business's
10 network, including archived or backup systems pursuant to (c)(iii) of
11 this subsection; and

12 (B) Notify all affiliates, processors, contractors, and other
13 third parties with whom the regulated entity or the small business
14 has shared consumer health data of the deletion request.

15 (ii) All affiliates, processors, contractors, and other third
16 parties that receive notice of a consumer's deletion request shall
17 honor the consumer's deletion request and delete the consumer health
18 data from its records, subject to the same requirements of this
19 chapter.

20 (iii) If consumer health data that a consumer requests to be
21 deleted is stored on archived or backup systems, then the request for
22 deletion may be delayed to enable restoration of the archived or
23 backup systems and such delay may not exceed six months from
24 authenticating the deletion request.

25 (d) A consumer may exercise the rights set forth in this chapter
26 by submitting a request, at any time, to a regulated entity or a
27 small business. Such a request may be made by a secure and reliable
28 means established by the regulated entity or the small business and
29 described in its consumer health data privacy policy. The method must
30 take into account the ways in which consumers normally interact with
31 the regulated entity or the small business, the need for secure and
32 reliable communication of such requests, and the ability of the
33 regulated entity or the small business to authenticate the identity
34 of the consumer making the request. A regulated entity or a small
35 business may not require a consumer to create a new account in order
36 to exercise consumer rights pursuant to this chapter but may require
37 a consumer to use an existing account.

38 (e) If a regulated entity or a small business is unable to
39 authenticate the request using commercially reasonable efforts, the
40 regulated entity or the small business is not required to comply with

1 a request to initiate an action under this section and may request
2 that the consumer provide additional information reasonably necessary
3 to authenticate the consumer and the consumer's request.

4 (f) Information provided in response to a consumer request must
5 be provided by a regulated entity and a small business free of
6 charge, up to twice annually per consumer. If requests from a
7 consumer are manifestly unfounded, excessive, or repetitive, the
8 regulated entity or the small business may charge the consumer a
9 reasonable fee to cover the administrative costs of complying with
10 the request or decline to act on the request. The regulated entity
11 and the small business bear the burden of demonstrating the
12 manifestly unfounded, excessive, or repetitive nature of the request.

13 (g) A regulated entity and a small business shall comply with the
14 consumer's requests under subsection (1)(a) through (c) of this
15 section without undue delay, but in all cases within 45 days of
16 receipt of the request submitted pursuant to the methods described in
17 this section. A regulated entity and a small business must promptly
18 take steps to authenticate a consumer request but this does not
19 extend the regulated entity's and the small business's duty to comply
20 with the consumer's request within 45 days of receipt of the
21 consumer's request. The response period may be extended once by 45
22 additional days when reasonably necessary, taking into account the
23 complexity and number of the consumer's requests, so long as the
24 regulated entity or the small business informs the consumer of any
25 such extension within the initial 45-day response period, together
26 with the reason for the extension.

27 (h) A regulated entity and a small business shall establish a
28 process for a consumer to appeal the regulated entity's or the small
29 business's refusal to take action on a request within a reasonable
30 period of time after the consumer's receipt of the decision. The
31 appeal process must be conspicuously available and similar to the
32 process for submitting requests to initiate action pursuant to this
33 section. Within 45 days of receipt of an appeal, a regulated entity
34 or a small business shall inform the consumer in writing of any
35 action taken or not taken in response to the appeal, including a
36 written explanation of the reasons for the decisions. If the appeal
37 is denied, the regulated entity or the small business shall also
38 provide the consumer with an online mechanism, if available, or other
39 method through which the consumer may contact the attorney general to
40 submit a complaint.

1 (2) A small business must comply with this section beginning June
2 30, 2024.

3 NEW SECTION. **Sec. 7.** (1) Except as provided in subsection (2)
4 of this section, beginning March 31, 2024, a regulated entity and a
5 small business shall:

6 (a) Restrict access to consumer health data by the employees,
7 processors, and contractors of such regulated entity or small
8 business to only those employees, processors, and contractors for
9 which access is necessary to further the purposes for which the
10 consumer provided consent or where necessary to provide a product or
11 service that the consumer to whom such consumer health data relates
12 has requested from such regulated entity or small business; and

13 (b) Establish, implement, and maintain administrative, technical,
14 and physical data security practices that, at a minimum, satisfy
15 reasonable standard of care within the regulated entity's or the
16 small business's industry to protect the confidentiality, integrity,
17 and accessibility of consumer health data appropriate to the volume
18 and nature of the consumer health data at issue.

19 (2) A small business must comply with this section beginning June
20 30, 2024.

21 NEW SECTION. **Sec. 8.** (1)(a)(i) Except as provided in subsection
22 (2) of this section, beginning March 31, 2024, a processor may
23 process consumer health data only pursuant to a binding contract
24 between the processor and the regulated entity or the small business
25 that sets forth the processing instructions and limit the actions the
26 processor may take with respect to the consumer health data it
27 processes on behalf of the regulated entity or the small business.

28 (ii) A processor may process consumer health data only in a
29 manner that is consistent with the binding instructions set forth in
30 the contract with the regulated entity or the small business.

31 (b) A processor shall assist the regulated entity or the small
32 business by appropriate technical and organizational measures,
33 insofar as this is possible, in fulfilling the regulated entity's and
34 the small business's obligations under this chapter.

35 (c) If a processor fails to adhere to the regulated entity's or
36 the small business's instructions or processes consumer health data
37 in a manner that is outside the scope of the processor's contract
38 with the regulated entity or the small business, the processor is

1 considered a regulated entity or a small business with regard to such
2 data and is subject to all the requirements of this chapter with
3 regard to such data.

4 (2) A small business must comply with this section beginning June
5 30, 2024.

6 NEW SECTION. **Sec. 9.** (1) Except as provided in subsection (6)
7 of this section, beginning March 31, 2024, it is unlawful for any
8 person to sell or offer to sell consumer health data concerning a
9 consumer without first obtaining valid authorization from the
10 consumer. The sale of consumer health data must be consistent with
11 the valid authorization signed by the consumer. This authorization
12 must be separate and distinct from the consent obtained to collect or
13 share consumer health data, as required under section 5 of this act.

14 (2) A valid authorization to sell consumer health data is a
15 document consistent with this section and must be written in plain
16 language. The valid authorization to sell consumer health data must
17 contain the following:

18 (a) The specific consumer health data concerning the consumer
19 that the person intends to sell;

20 (b) The name and contact information of the person collecting and
21 selling the consumer health data;

22 (c) The name and contact information of the person purchasing the
23 consumer health data from the seller identified in (b) of this
24 subsection;

25 (d) A description of the purpose for the sale, including how the
26 consumer health data will be gathered and how it will be used by the
27 purchaser identified in (c) of this subsection when sold;

28 (e) A statement that the provision of goods or services may not
29 be conditioned on the consumer signing the valid authorization;

30 (f) A statement that the consumer has a right to revoke the valid
31 authorization at any time and a description on how to submit a
32 revocation of the valid authorization;

33 (g) A statement that the consumer health data sold pursuant to
34 the valid authorization may be subject to redisclosure by the
35 purchaser and may no longer be protected by this section;

36 (h) An expiration date for the valid authorization that expires
37 one year from when the consumer signs the valid authorization; and

38 (i) The signature of the consumer and date.

1 (3) An authorization is not valid if the document has any of the
2 following defects:

3 (a) The expiration date has passed;

4 (b) The authorization does not contain all the information
5 required under this section;

6 (c) The authorization has been revoked by the consumer;

7 (d) The authorization has been combined with other documents to
8 create a compound authorization; or

9 (e) The provision of goods or services is conditioned on the
10 consumer signing the authorization.

11 (4) A copy of the signed valid authorization must be provided to
12 the consumer.

13 (5) The seller and purchaser of consumer health data must retain
14 a copy of all valid authorizations for sale of consumer health data
15 for six years from the date of its signature or the date when it was
16 last in effect, whichever is later.

17 (6) A small business must comply with this section beginning June
18 30, 2024.

19 NEW SECTION. **Sec. 10.** It is unlawful for any person to
20 implement a geofence around an entity that provides in-person health
21 care services where such geofence is used to: (1) Identify or track
22 consumers seeking health care services; (2) collect consumer health
23 data from consumers; or (3) send notifications, messages, or
24 advertisements to consumers related to their consumer health data or
25 health care services.

26 NEW SECTION. **Sec. 11.** The legislature finds that the practices
27 covered by this chapter are matters vitally affecting the public
28 interest for the purpose of applying the consumer protection act,
29 chapter 19.86 RCW. A violation of this chapter is not reasonable in
30 relation to the development and preservation of business, and is an
31 unfair or deceptive act in trade or commerce and an unfair method of
32 competition for the purpose of applying the consumer protection act,
33 chapter 19.86 RCW.

34 NEW SECTION. **Sec. 12.** (1) This chapter does not apply to:

35 (a) Information that meets the definition of:

1 (i) Protected health information for purposes of the federal
2 health insurance portability and accountability act of 1996 and
3 related regulations;

4 (ii) Health care information collected, used, or disclosed in
5 accordance with chapter 70.02 RCW;

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

9 (iv) Identifiable private information for purposes of the federal
10 policy for the protection of human subjects, 45 C.F.R. Part 46;
11 identifiable private information that is otherwise information
12 collected as part of human subjects research pursuant to the good
13 clinical practice guidelines issued by the international council for
14 harmonization; the protection of human subjects under 21 C.F.R. Parts
15 50 and 56; or personal data used or shared in research conducted in
16 accordance with one or more of the requirements set forth in this
17 subsection;

18 (v) Information and documents created specifically for, and
19 collected and maintained by:

20 (A) A quality improvement committee for purposes of RCW
21 43.70.510, 70.230.080, or 70.41.200;

22 (B) A peer review committee for purposes of RCW 4.24.250;

23 (C) A quality assurance committee for purposes of RCW 74.42.640
24 or 18.20.390;

25 (D) A hospital, as defined in RCW 43.70.056, for reporting of
26 health care-associated infections for purposes of RCW 43.70.056, a
27 notification of an incident for purposes of RCW 70.56.040(5), or
28 reports regarding adverse events for purposes of RCW 70.56.020(2)(b);
29 or

30 (E) A manufacturer, as defined in 21 C.F.R. Sec. 820.3(o), when
31 collected, used, or disclosed for purposes specified in chapter 70.02
32 RCW;

33 (vi) Information and documents created for purposes of the
34 federal health care quality improvement act of 1986, and related
35 regulations;

36 (vii) Patient safety work product for purposes of 42 C.F.R. Part
37 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26;

38 (viii) Information that is (A) deidentified in accordance with
39 the requirements for deidentification set forth in 45 C.F.R. Part

1 164, and (B) derived from any of the health care-related information
2 listed in this subsection (1)(a)(viii);

3 (b) Information originating from, and intermingled to be
4 indistinguishable with, information under (a) of this subsection that
5 is maintained by:

6 (i) A covered entity or business associate as defined by the
7 health insurance portability and accountability act of 1996 and
8 related regulations;

9 (ii) A health care facility or health care provider as defined in
10 RCW 70.02.010; or

11 (iii) A program or a qualified service organization as defined by
12 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

13 (c) Information used only for public health activities and
14 purposes as described in 45 C.F.R. Sec. 164.512 or that is part of a
15 limited data set, as defined, and is used, disclosed, and maintained
16 in the manner required, by 45 C.F.R. Sec. 164.514; or

17 (d) Identifiable data collected, used, or disclosed in accordance
18 with chapter 43.371 RCW or RCW 69.43.165.

19 (2) Personal information that is governed by and collected, used,
20 or disclosed pursuant to the following regulations, parts, titles, or
21 acts, is exempt from this chapter: (a) The Gramm-Leach-Bliley act (15
22 U.S.C. 6801 et seq.) and implementing regulations; (b) part C of
23 Title XI of the social security act (42 U.S.C. 1320d et seq.); (c)
24 the fair credit reporting act (15 U.S.C. 1681 et seq.); (d) the
25 family educational rights and privacy act (20 U.S.C. 1232g; Part 99
26 of Title 34, C.F.R.); (e) the Washington health benefit exchange and
27 applicable statutes and regulations, including 45 C.F.R. Sec. 155.260
28 and chapter 43.71 RCW; or (f) privacy rules adopted by the office of
29 the insurance commissioner pursuant to chapter 48.02 or 48.43 RCW.

30 (3) The obligations imposed on regulated entities, small
31 businesses, and processors under this chapter does not restrict a
32 regulated entity's, small business's, or processor's ability for
33 collection, use, or disclosure of consumer health data to prevent,
34 detect, protect against, or respond to security incidents, identity
35 theft, fraud, harassment, malicious or deceptive activities, or any
36 activity that is illegal under Washington state law or federal law;
37 preserve the integrity or security of systems; or investigate,
38 report, or prosecute those responsible for any such action that is
39 illegal under Washington state law or federal law.

1 (4) If a regulated entity, small business, or processor processes
2 consumer health data pursuant to subsection (3) of this section, such
3 entity bears the burden of demonstrating that such processing
4 qualifies for the exemption and complies with the requirements of
5 this section.

6 NEW SECTION. **Sec. 13.** A new section is added to chapter 44.28
7 RCW to read as follows:

8 (1) The joint committee must review enforcement actions, as
9 authorized in section 6 of this act, brought by the attorney general
10 and consumers to enforce violations of this act.

11 (2) The report must include, at a minimum:

12 (a) The number of enforcement actions reported by the attorney
13 general, a consumer, a regulated entity, or a small business that
14 resulted in a settlement, including the average settlement amount;

15 (b) The number of complaints reported, including categories of
16 complaints and the number of complaints for each category, reported
17 by the attorney general, a consumer, a regulated entity, or a small
18 business;

19 (c) The number of enforcement actions brought by the attorney
20 general and consumers, including the categories of violations and the
21 number of violations per category;

22 (e) The number of civil actions where a judge determined the
23 position of the nonprevailing party was frivolous, if any;

24 (f) The types of resources, including associated costs, expended
25 by the attorney general, a consumer, a regulated entity, or a small
26 business for enforcement actions; and

27 (g) Recommendations for potential changes to enforcement
28 provisions of this act.

29 (3) The office of the attorney general shall provide the joint
30 committee any data within their purview that the joint committee
31 considers necessary to conduct the review.

32 (4) The joint committee shall submit a report of its findings and
33 recommendations to the governor and the appropriate committees of the
34 legislature by September 30, 2030.

35 (5) This section expires June 30, 2031.

36 NEW SECTION. **Sec. 14.** If any provision of this act or its
37 application to any person or circumstance is held invalid, the

1 remainder of the act or the application of the provision to other
2 persons or circumstances is not affected.

3 NEW SECTION. **Sec. 15.** Sections 1 through 12 of this act
4 constitute a new chapter in Title 19 RCW."

ESHB 1155 - S AMD 270
By Senator Dhingra

ADOPTED AS AMENDED 04/05/2023

5 On page 1, line 2 of the title, after "data;" strike the
6 remainder of the title and insert "adding a new section to chapter
7 44.28 RCW; adding a new chapter to Title 19 RCW; providing an
8 effective date; and providing an expiration date."

EFFECT: (1) Specifies "consumer health data" includes any information that a regulated entity or small business processes to identify a consumer's physical or mental health status that is derived from nonhealth information and includes data that identifies a consumer seeking health care services.

(2) Revises the definition of "deidentified data" by clarifying a regulated entity that possesses such data must contractually obligate any recipients of such data to satisfy all defined criteria.

(3) Revises the definition of "geofence" by including spatial detection as a form of detection to establish a virtual boundary and specifies detection also includes the purpose to locate a consumer within a virtual boundary.

(4) Revises the exemption in the definition of "personal information" so that biometric data collected about a consumer by a business without a consumer's consent, rather than knowledge, is not publicly available information.

(5) Clarifies the definition of "share" does not include disclosures to a third party with whom the consumer has a direct relationship when the third party uses the consumer health data only at the direction from the regulated entity and consistent with the purpose for which it was collected and consented to, rather than disclosed to.

(6) Provides a definition for "small business."

(7) Removes the requirement for a regulated entity to respond to a request to delete consumer health data without unreasonable delay and no more than 30 calendar days from authenticating the deletion request.

(8) 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.

(9) Clarifies authorization to sell consumer health data must be obtained separate and distinct from the consent obtained to collect or share consumer health data.

(10) Removes the specification that the legislative declarations that make a violation of the bill a per se violation of the Consumer

Protection Act (CPA) apply in enforcement actions brought by the Attorney General.

(11) 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.

(12) Provides that this act does not apply to information and documents created specifically for, and collected and maintained by, a federally regulated medical device manufacturer when collected, used, or disclosed for use in medical records.

(13) Specifies this act also does not apply to information that is part of a limited data set and is used, disclosed, and maintained in a manner required under HIPAA or identifiable data collected, used, or disclosed in the electronic sales tracking system implemented by the state pharmacy quality assurance commission and consistent with the federal combat meth act.

(14) 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.

(15) Provides an effective date of March 31, 2024, for regulated entities and an effective date of June 30, 2024, for small businesses.

(16) Requires the Joint Legislative Audit and Review Committee to review enforcement actions, as authorized under the act, and submit a report of its findings by September 30, 2030.

(17) Makes technical corrections.

--- END ---