

ESHB 1155 - S COMM AMD

By Committee on Law & Justice

NOT ADOPTED 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 a
16 consumer's past, present, or future physical or mental health
17 including, but not limited to:

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

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

22 (iii) Health-related surgeries or procedures;

23 (iv) Use or purchase of medication;

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

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

27 (vii) Gender-affirming care information;

28 (viii) Reproductive or sexual health information;

29 (ix) Biometric data related to information described in this
30 subsection (8)(a);

31 (x) Genetic data related to information described in this
32 subsection (8)(a);

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

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

38 (xiii) Any information described in (a)(i) through (xii) of this
39 subsection that is derived or extrapolated from nonhealth information

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

3 (b) "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 has
10 implemented reasonable safeguards to mitigate privacy risks
11 associated with research, including any risks associated with
12 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 that possesses such data (a) takes
20 reasonable measures to ensure that such data cannot be associated
21 with a consumer; (b) publicly commits to process such data only in a
22 deidentified fashion and not attempt to reidentify such data; and (c)
23 contractually obligates any recipients of such data to satisfy the
24 criteria set forth in this subsection (10).

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

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

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

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

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

1 services" includes, but is not limited to, treatments for gender
2 dysphoria, gender-affirming hormone therapy, and gender-affirming
3 surgical procedures.

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

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

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

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

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

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

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

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

28 (c) Health-related surgeries or procedures;

29 (d) Use or purchase of medication;

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

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

33 (g) Reproductive health care services; or

34 (h) Gender-affirming care services.

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

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

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

12 (b) "Personal information" does not include publicly available
13 information. Any biometric data collected about a consumer by a
14 business without the consumer's consent is not 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.

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 has a reasonable basis to believe a consumer has lawfully made
33 available to the general public.

34 (23) "Regulated entity" means any legal entity that: (a) Conducts
35 business in Washington, or produces or provides products or services
36 that are targeted to consumers in Washington; and (b) alone or
37 jointly with others, determines the purpose and means of collecting,
38 processing, sharing, or selling of consumer health data. "Regulated
39 entity" does not mean government agencies, tribal nations, or

1 contracted service providers when processing consumer health data on
2 behalf of the government agency.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 that complies with the requirements and obligations in this chapter;
2 or

3 (ii) By a regulated entity to a processor when such exchange is
4 consistent with the purpose for which the consumer health data was
5 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 to a third party or
10 affiliate.

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

12 (i) The disclosure of consumer health data by a regulated entity
13 to a processor when such sharing is to provide goods or services in a
14 manner consistent with the purpose for which the consumer health data
15 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 maintains control and ownership of
20 the data; and (C) the third party uses the consumer health data only
21 at direction from the regulated entity and consistent with the
22 purpose for which it was collected and consented to by the consumer;
23 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 assets and complies with the
28 requirements and obligations in this chapter.

29 (28) "Third party" means an entity other than a consumer,
30 regulated entity, processor, or affiliate of the regulated entity.

31 NEW SECTION. **Sec. 4.** (1) A regulated entity shall maintain a
32 consumer health data privacy policy that clearly and conspicuously
33 discloses:

34 (a) The categories of consumer health data collected and the
35 purpose for which the data is collected, including how the data will
36 be used;

37 (b) The categories of sources from which the consumer health data
38 is collected;

39 (c) The categories of consumer health data that is shared;

1 (d) A list of the categories of third parties and specific
2 affiliates with whom the regulated entity shares the consumer health
3 data; and

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

6 (2) A regulated entity shall prominently publish a link to its
7 consumer health data privacy policy on its homepage.

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

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

18 (5) It is a violation of this chapter for a regulated entity to
19 contract with a processor to process consumer health data in a manner
20 that is inconsistent with the regulated entity's consumer health data
21 privacy policy.

22 NEW SECTION. **Sec. 5.** (1) A regulated entity may not collect any
23 consumer health data except:

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

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

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

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

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

37 (3) Consent required under this section must be obtained prior to
38 the collection or sharing, as applicable, of any consumer health
39 data, and the request for consent must clearly and conspicuously

1 disclose: (a) The categories of consumer health data collected or
2 shared; (b) the purpose of the collection or sharing of the consumer
3 health data, including the specific ways in which it will be used;
4 (c) the categories of entities with whom the consumer health data is
5 shared; and (d) how the consumer can withdraw consent from future
6 collection or sharing of the consumer's health data.

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

9 NEW SECTION. **Sec. 6.** (1) A consumer has the right to confirm
10 whether a regulated entity is collecting, sharing, or selling
11 consumer health data concerning the consumer and to access such data,
12 including a list of all third parties and affiliates with whom the
13 regulated entity has shared or sold the consumer health data and an
14 active email address or other online mechanism that the consumer may
15 use to contact these third parties.

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

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

23 (a) A regulated entity that receives a consumer's request to
24 delete any consumer health data concerning the consumer shall:

25 (i) Delete the consumer health data from its records, including
26 from all parts of the regulated entity's network, including archived
27 or backup systems pursuant to (c) of this subsection; and

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

31 (b) All affiliates, processors, contractors, and other third
32 parties that receive notice of a consumer's deletion request shall
33 honor the consumer's deletion request and delete the consumer health
34 data from its records, subject to the same requirements of this
35 chapter.

36 (c) If consumer health data that a consumer requests to be
37 deleted is stored on archived or backup systems, then the request for
38 deletion may be delayed to enable restoration of the archived or

1 backup systems and such delay may not exceed six months from
2 authenticating the deletion request.

3 (4) A consumer may exercise the rights set forth in this chapter
4 by submitting a request, at any time, to a regulated entity. Such a
5 request may be made by a secure and reliable means established by the
6 regulated entity and described in its consumer health data privacy
7 policy. The method must take into account the ways in which consumers
8 normally interact with the regulated entity, the need for secure and
9 reliable communication of such requests, and the ability of the
10 regulated entity to authenticate the identity of the consumer making
11 the request. A regulated entity may not require a consumer to create
12 a new account in order to exercise consumer rights pursuant to this
13 chapter but may require a consumer to use an existing account.

14 (5) If a regulated entity is unable to authenticate the request
15 using commercially reasonable efforts, the regulated entity is not
16 required to comply with a request to initiate an action under this
17 section and may request that the consumer provide additional
18 information reasonably necessary to authenticate the consumer and the
19 consumer's request.

20 (6) Information provided in response to a consumer request must
21 be provided by a regulated entity free of charge, up to twice
22 annually per consumer. If requests from a consumer are manifestly
23 unfounded, excessive, or repetitive, the regulated entity may charge
24 the consumer a reasonable fee to cover the administrative costs of
25 complying with the request or decline to act on the request. The
26 regulated entity bears the burden of demonstrating the manifestly
27 unfounded, excessive, or repetitive nature of the request.

28 (7) A regulated entity shall comply with the consumer's requests
29 under subsections (1) through (3) of this section without undue
30 delay, but in all cases within 45 days of receipt of the request
31 submitted pursuant to the methods described in this section. A
32 regulated entity must promptly take steps to authenticate a consumer
33 request but this does not extend the regulated entity's duty to
34 comply with the consumer's request within 45 days of receipt of the
35 consumer's request. The response period may be extended once by 45
36 additional days when reasonably necessary, taking into account the
37 complexity and number of the consumer's requests, so long as the
38 regulated entity informs the consumer of any such extension within
39 the initial 45-day response period, together with the reason for the
40 extension.

1 (8) A regulated entity shall establish a process for a consumer
2 to appeal the regulated entity's refusal to take action on a request
3 within a reasonable period of time after the consumer's receipt of
4 the decision. The appeal process must be conspicuously available and
5 similar to the process for submitting requests to initiate action
6 pursuant to this section. Within 45 days of receipt of an appeal, a
7 regulated entity shall inform the consumer in writing of any action
8 taken or not taken in response to the appeal, including a written
9 explanation of the reasons for the decisions. If the appeal is
10 denied, the regulated entity shall also provide the consumer with an
11 online mechanism, if available, or other method through which the
12 consumer may contact the attorney general to submit a complaint.

13 NEW SECTION. **Sec. 7.** (1) A regulated entity shall restrict
14 access to consumer health data by the employees, processors, and
15 contractors of such regulated entity to only those employees,
16 processors, and contractors for which access is necessary to further
17 the purposes for which the consumer provided consent or where
18 necessary to provide a product or service that the consumer to whom
19 such consumer health data relates has requested from such regulated
20 entity.

21 (2) A regulated entity shall establish, implement, and maintain
22 administrative, technical, and physical data security practices that,
23 at a minimum, satisfy reasonable standard of care within the
24 regulated entity's industry to protect the confidentiality,
25 integrity, and accessibility of consumer health data appropriate to
26 the volume and nature of the consumer health data at issue.

27 NEW SECTION. **Sec. 8.** (1)(a) A processor may process consumer
28 health data only pursuant to a binding contract between the processor
29 and the regulated entity that sets forth the processing instructions
30 and limit the actions the processor may take with respect to the
31 consumer health data it processes on behalf of the regulated entity.

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

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

1 (3) If a processor fails to adhere to the regulated entity's
2 instructions or processes consumer health data in a manner that is
3 outside the scope of the processor's contract with the regulated
4 entity, the processor is considered a regulated entity with regard to
5 such data and is subject to all the requirements of this chapter with
6 regard to such data.

7 NEW SECTION. **Sec. 9.** (1) It is unlawful for any person to sell
8 or offer to sell consumer health data concerning a consumer without
9 first obtaining valid authorization from the consumer. The sale of
10 consumer health data must be consistent with the valid authorization
11 signed by the consumer. This authorization must be separate and
12 distinct from the consent obtained to collect or share consumer
13 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 NEW SECTION. **Sec. 10.** It is unlawful for any person to
18 implement a geofence around an entity that provides in-person health
19 care services where such geofence is used to: (1) Identify or track
20 consumers seeking health care services; (2) collect consumer health
21 data from consumers; or (3) send notifications, messages, or
22 advertisements to consumers related to their consumer health data or
23 health care services.

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

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

33 (a) Information that meets the definition of:

34 (i) Protected health information for purposes of the federal
35 health insurance portability and accountability act of 1996 and
36 related regulations;

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

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

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

15 (v) Information and documents created specifically for, and
16 collected and maintained by:

17 (A) A quality improvement committee for purposes of RCW
18 43.70.510, 70.230.080, or 70.41.200;

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

20 (C) A quality assurance committee for purposes of RCW 74.42.640
21 or 18.20.390;

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

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

30 (vi) Information and documents created for purposes of the
31 federal health care quality improvement act of 1986, and related
32 regulations;

33 (vii) Patient safety work product for purposes of 42 C.F.R. Part
34 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26;

35 (viii) Information that is (A) deidentified in accordance with
36 the requirements for deidentification set forth in 45 C.F.R. Part
37 164, and (B) derived from any of the health care-related information
38 listed in this subsection (1)(a)(viii);

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

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

7 (ii) A health care facility or health care provider as defined in
8 RCW 70.02.010; or

9 (iii) A program or a qualified service organization as defined by
10 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

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

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

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

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

38 (4) If a regulated entity or processor processes consumer health
39 data pursuant to subsection (3) of this section, such entity bears

1 the burden of demonstrating that such processing qualifies for the
2 exemption and complies with the requirements of this section.

3 NEW SECTION. **Sec. 13.** If any provision of this act or its
4 application to any person or circumstance is held invalid, the
5 remainder of the act or the application of the provision to other
6 persons or circumstances is not affected.

7 NEW SECTION. **Sec. 14.** Sections 1 through 12 of this act
8 constitute a new chapter in Title 19 RCW.

9 NEW SECTION. **Sec. 15.** Sections 4 through 9 of this act take
10 effect March 31, 2024."

ESHB 1155 - S COMM AMD

By Committee on Law & Justice

NOT ADOPTED 04/05/2023

11 On page 1, line 2 of the title, after "data;" strike the
12 remainder of the title and insert "adding a new chapter to Title 19
13 RCW; and providing an effective date."

EFFECT: • Specifies consumer health data includes data that identifies a consumer seeking health care services.

• 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.

• 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.

• 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.

• 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.

• 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.

• 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.

- Clarifies authorization to sell consumer health data must be obtained separate and distinct from the consent obtained to collect or share consumer health data.
- 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.
- 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.
- 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.
- 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.
- 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.
- Makes technical corrections.
- Provides an effective date of March 31, 2024, for sections of the bill that relate to the consumer health data rights, a consumer health data privacy policy, consent for the collection or sharing of data, regulated entity and processor obligations, restriction of access and data security practices, and valid authorization.

--- END ---