



**WA People's Privacy - Our Short list of Changes Requested**  
**Also tracked onto ESHB 1155 - Sent to AGO staff Friday, March 10, 2023**

**DEFINITIONS:**

**Page 2 Section 3.(3) Authenticate — WILL SEND VIA SEPARATE COVER**

**Page 3 Biometric Data:**

**ADD BACK IN** a (C) exercise, health, sleep data which is collected by wearable and/or “smart home” devices and their associated mobile apps or other software.

**Page 4 (8) Consumer Health Data (b) does not include.... WILL SEND VIA SEPARATE COVER - Key notes:** *Research — “reasonable”... etc.*

*Concerned about ensuring space for conscientious objection, also may need adjustment to deal with changes in de-identified data.*

**INSERT NEW DEFINITION: "Covered Location"**

“Covered Location” means any location where in-person health services, information, or health-related activities are performed, offered, received, purchased, sold or advertised.

**Page 4 Starting Line 26 (10) De-identified Data**

STRIKE “Deidentified” REPLACE with **Anonymized**

STRIKE “reasonably”

STRIKE “reasonable” and REPLACE with “the following”

After Individual, **INSERT new framework (I understand ACLU WA is working on this w/UW folks)**

STRIKE “deidentified fashion” and REPLACE with “**completely anonymized format**”

STRIKE “and” between (a) and (b) and INSERT “and (c)”

**Changes to (10) De-identified Data in textual context:**

(10) “Deidentified **Anonymized** 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 **the following** measures to ensure that such data cannot be associated with an individual

**(INSERT HERE a qualifying framework and an acceptable process or standard for anonymizing data, including stipulating that all data collected in connection with consumer health data shall be anonymized completely **before** it may be sold or shared with third parties, except in the case of M&A's where identifiable data is necessary to continue providing a service the consumer has requested or consented to.) ;**



(b) publicly commits to process such data only in a ~~deidentified fashion~~ **completely anonymized format** 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) **and (c)** of this subsection.

#### **Page. 5 Line 27 (14) "Geofence"**

INSERTIONS IN RED: means technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wifi data, and/or any other form of **spatial or** location detection to establish a virtual boundary around a specific physical location, **and/or to locate a consumer within a virtual boundary**. For purposes of this definition, "geofence" means a virtual boundary that is 2,000 feet or less from the perimeter of the physical location.

#### **ADD NEW DEFINITION: GEOFENCE TRACKING**

INSERT

"Geofence tracking" means the use of any technology to track a wearable or personal device or other personally owned item or vehicle, via device identifiers such as IP address, MAC address, Advertising identifiers, or other identifying data from any location that is geofenced (a) to or from any geofence-prohibited physical location where health services are rendered or performed, referred to in this bill as a **"covered location"**

EFFECT: LIMIT THE TRACKING OF PEOPLE FROM HOME/WORK/SCHOOL/PHARMACY/AIRPORT/OR OTHER GEOFENCED LOCATION TO A CLINIC OR OTHER PLACE WHERE HEALTH CARE SERVICES ARE PERFORMED *AND/OR FROM* SUCH LOCATION TO ANOTHER.

#### **Page 6 Line 25 (b) "Personal Information"**

STRIKE "knowledge" and INSERT "consent"

#### **Page 6 (19) "Precise location information" ~~Remove/Strike this definition.~~**

**Also ~~Remove/Strike "Precise" on~~**

**~~page 4 line 6 (8)(xi),~~**

**~~page 5 line 1 (11)(a),~~**

**~~page 7 line 18 (24)(a)~~**

#### **Page 6 Line 38 (21) "Processor"**

After 'on behalf of a regulated entity' INSERT/ADD NEW:

Including but not limited to

(a) software licensed to regulated entities that stores health data on networked servers, whether cloud-based, located in WA state or located outside of WA state (b) mobile apps on phones, tablets, and computers used by a consumer to input, collect or process health data while the consumer is in WA State (c) security and surveillance systems and their associated software that may collect or record consumer health data (d) services utilizing consumer health data to assist a regulated entity with scheduling, tracking, monitoring, communicating with, or serving consumers.



**Page 7 Line 2 (24) "Reproductive or sexual health information" (g)**

STRIKE "an abortion" INSERT in its place "an actual or possible pregnancy or abortion"  
EFFECT: this just disallows any loophole whatsoever for CPCs; makes the regulation "bulletproof" by including potential or actual pregnancies, given that CPCs will inevitably frame consumers showing up for help as needing help with a pregnancy, rather than needing help with an abortion.

**Page 7 (22) "Publicly available information":**

On line 5 after 'to the general public.' INSERT/ADD NEW:

and does not contain personally identifying information related to consumer's health.

(c) It shall be unlawful for any entity or person to consider to be publicly available information any personal health information that a consumer has posted on a consumer's own personal social media stream, wall or account, whether publicly viewable or restricted. All entities and persons to which such information is visible are prohibited from scraping (collecting) sharing, selling, or storing any such information that qualifies as or contains "consumer health data" without the consumer's consent (as consent is here defined).

*(the above might need a little more workshopping, but basically we need a way to protect when people post about their abortions, gender-affirming care, or other health details on their socials!)*

**Page 7 Line 6 (23) "Regulated entity"**

STRIKE WHOLE DEFINITION & REPLACE WITH:

means any legal entity that: (a) Conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington; and  
(b) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data; and may also  
(c) collect, process, share, or sell consumer health data;  
"Regulated entity" does not mean government agencies or tribal nations.

**Page 8 Line 32 (27)(b)(ii)**

STRIKE "~~disclosed to the consumer~~" INSERT "consented to by the consumer"

**Section 4: Privacy Policy**

**Page 9 Lines 1-12**

STRIKE all through (d) and replace with:

NEW SECTION. **Sec. 4.** (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 how the data will be used, how long it will be retained, and how the regulated entity carries out responsible data minimization and deletion practices;
- (b) The sources from which the consumer health data is collected;
- (c) A thorough list of the categories and types of consumer health data that are shared and the purpose for which the data is shared;



(d) A list of processors, third parties and specific affiliates the regulated entity shares data with, or sells data to.

(e) A brief list of any former names and ownership if the regulated entity has been acquired, merged and or renamed in the previous ten years.

#### **Page 9 Line 14/15**

##### **ADD:**

(g) at least three methods consumers may use to contact a regulated entity. One method must be a telephone number, another must be by postal mail, and the third of which must be an email. Regulated entities must guarantee that all methods of contact by consumers are checked at least once daily by a natural person, during operating business hours. Chats may be used as an optional fourth measure, but may not replace the three mandated methods of consumer contact, and must not utilize software or machine learning programs/AI that collects, shares, or sells personal information or health data.

#### **Page 12 Line 36 Section 8**

INSERT/ REPLACE "limit" with "strictly limits"

#### **Page 13 Line 15 Section 9: selling**

ADD "consent" and valid authorization

#### **Section 10: Geofencing**

STRIKE ALL and REPLACE WITH:

NEW SECTION. **Sec. 10.** It is unlawful for any person to implement a geofence around an entity that provides in-person health care services (a "covered location") where such geofence is used to: (1) Identify, track or collect data from consumers, including but not limited to consumer health data; or (2) send notifications, messages, or advertisements to a consumer that enters the virtual perimeter; or (3) collect identifying information to enable "geofence tracking" of a consumer from a "covered location" to another location.

#### **Section 11: Enforcement**

STRIKE ALL and REPLACE with:

NEW SECTION. **Sec. 11.** 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.



## WA People's Privacy - review of HOUSE FLOOR AMENDMENTS in ESHB 1155

**page 8 lines 4, 6, 13 BAKY 323** — Strikes “sale” inserts “exchange”  
OK with this.

### **page 13 BAKY 325**

On page 13, line 10, after "regulated entity" insert "with regard to such data"

On page 13, line 11, after "chapter" insert "with regard to such data"

### **NOT OK WITH THIS AMENDMENT — PLEASE REVERT TO Sub BILL LANGUAGE**

This subtly weakens the bill for purposes of enforcement, such that an entity is only really regulated if they are found to be collecting this data. Opens loophole for entities to claim they didn't know they were a regulated entity and kind of paired with Walen's failed right to cure amendment. That failed, so beyond being a bad amendment, now this weakening amendment doesn't even make *sense* to leave in.

### **page 14 line 21 – BAKY 320** - Hansen geofence changes - Removes Protections

This Costco & Grocery lobby carveout is selfish, myopic, and unfair to people seeking safety - **REJECT**.

While Hansen's amendment did at least help clarify the muddled language that came out of his Sub bill from CR&J, it didn't strengthen, but *further* weakened and removed the geofence protections from the Original bill. **WE HAVE SUGGESTED CHANGES** - these have been suggested above to embrace *some* of Hansen's re-wording, while rectifying the strong protections the original bill intended, and further clarifying and strengthening that protection.

**To that end, we have suggested adding TWO NEW DEFINITIONS:**

**“Geofenced Tracking”**

**and**

**“Covered Location”**

### **page 14 line 24 and after line 31 — BAKY 335** - weakens enforcement

**REJECT** - revert to original HB 1155 language.

### **WA PEOPLE'S PRIVACY Unanswered Question:**

**Do we feel that the issue of pixels/trackers collecting personal and health data is addressed in this bill?**

This has been shown to be a way to gather information about who is seeking what types of healthcare, and collect their personal information from forms and websites they visit.



---

ENGROSSED SUBSTITUTE HOUSE BILL 1155

---

State of Washington

68th Legislature

2023 Regular Session

By House Civil Rights & Judiciary (originally sponsored by Representatives Slatter, Street, Reed, Ryu, Berg, Alvarado, Taylor, Bateman, Ramel, Senn, Goodman, Fitzgibbon, Macri, Simmons, Reeves, Lekanoff, Orwall, Duerr, Thai, Gregerson, Wylie, Ortiz-Self, Stonier, Pollet, Riccelli, Donaghy, Fosse, and Ormsby; by request of Attorney General)

READ FIRST TIME 02/07/23.



WA People's Privacy - list of Changes tracked onto ESHB 1155  
Sent to AGO staff Friday, March 10, 2023

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

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

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

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

13 (2) Information related to an individual's health conditions or  
14 attempts to obtain health care services is among the most personal  
15 and sensitive categories of data collected. Washingtonians expect  
16 that their health data is protected under laws like the health  
17 information portability and accountability act (HIPAA). However,  
18 HIPAA only covers health data collected by specific health care  
19 entities, including most health care providers. Health data collected  
20 by noncovered entities, including certain apps and websites, are not

1 afforded the same protections. This act works to close the gap  
2 between consumer knowledge and industry practice by providing  
3 stronger privacy protections for all Washington consumers' health  
4 data.

5 (3) With this act, the legislature intends to provide heightened  
6 protections for Washingtonian's health data by: Requiring additional  
7 disclosures and consumer consent regarding the collection, sharing,  
8 and use of such information; empowering consumers with the right to  
9 have their health data deleted; prohibiting the selling of consumer  
10 health data without valid authorization signed by the consumer; and  
11 making it unlawful to utilize a geofence around a facility that  
12 provides health care services.

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

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

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

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

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

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

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

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



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

4 (b) Keystroke patterns or rhythms and gait patterns or rhythms  
5 that contain identifying information.

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

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

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

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

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

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

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

27 (8)(a) "Consumer health data" means personal information that is  
28 linked or reasonably linkable to a consumer and that identifies a  
29 consumer's past, present, or future physical or mental health  
30 including, but not limited to:

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

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

35 (iii) Health-related surgeries or procedures;

36 (iv) Use or purchase of medication;

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

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

40 (vii) Gender-affirming care information;



1 (viii) Reproductive or sexual health information;

2 (ix) Biometric data related to information described in this  
3 subsection (8) (a);

4 (x) Genetic data related to information described in this  
5 subsection (8) (a);

6 (xi) Precise location information that could reasonably indicate  
7 a consumer's attempt to acquire or receive health services or  
8 supplies; or

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

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

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

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

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

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

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

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

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

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

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

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

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

27 (14) "Geofence" means technology that uses global positioning  
28 coordinates, cell tower connectivity, cellular data, radio frequency  
29 identification, Wifi data, and/or any other form of location  
30 detection to establish a virtual boundary around a specific physical  
31 location. For purposes of this definition, "geofence" means a virtual  
32 boundary that is 2,000 feet or less from the perimeter of the  
33 physical location.

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

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

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

39 (c) Health-related surgeries or procedures;

40 (d) Use or purchase of medication;

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

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

4 (g) Reproductive health care services; or

5 (h) Gender-affirming care services.

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

12 (17) "Person" means, where applicable, natural persons,  
13 corporations, trusts, unincorporated associations, and partnerships.  
14 "Person" does not include government agencies, tribal nations, or  
15 contracted service providers when processing consumer health data on  
16 behalf of a government agency.

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

23 (b) "Personal information" does not include publicly available  
24 information. Any biometric data collected about a consumer by a  
25 business without the consumer's knowledge is not publicly available  
26 information.

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

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

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

38 (21) "Processor" means a person that processes consumer health  
39 data on behalf of a regulated entity.

1 (22) "Publicly available information" means information that (a)  
2 is lawfully made available through federal, state, or municipal  
3 government records or widely distributed media, and (b) a regulated  
4 entity has a reasonable basis to believe a consumer has lawfully made  
5 available to the general public.

6 ~~(23) "Regulated entity" means any legal entity that: (a) Conducts~~  
7 ~~business in Washington, or produces or provides products or services~~  
8 ~~that are targeted to consumers in Washington; and (b) alone or~~  
9 ~~jointly with others, determines the purpose and means of collecting,~~  
10 ~~processing, sharing, or selling of consumer health data. "Regulated~~  
11 ~~entity" does not mean government agencies, tribal nations, or~~  
12 ~~contracted service providers when processing consumer health data on~~  
13 ~~behalf of the government agency.~~

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

18 (a) Precise location information that could reasonably indicate a  
19 consumer's attempt to acquire or receive reproductive or sexual  
20 health services;

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

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

27 (25) "Reproductive or sexual health services" means health  
28 services or products that support or relate to a consumer's  
29 reproductive system or sexual well-being, including but not limited  
30 to:

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

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

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

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

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

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

40 and

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

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

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

8 (i) To a third party as an asset that is part of a merger,  
9 acquisition, bankruptcy, or other transaction in which the third  
10 party assumes control of all or part of the regulated entity's assets  
11 that complies with the requirements and obligations in this chapter;  
12 or

13 (ii) By a regulated entity to a processor when such exchange is  
14 consistent with the purpose for which the consumer health data was  
15 collected and disclosed to the consumer.

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

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

22 (i) The disclosure of consumer health data by a regulated entity  
23 to a processor when such sharing is to provide goods or services in a  
24 manner consistent with the purpose for which the consumer health data  
25 was collected and disclosed to the consumer;

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

33 (iii) The disclosure or transfer of personal data to a third  
34 party as an asset that is part of a merger, acquisition, bankruptcy,  
35 or other transaction in which the third party assumes control of all  
36 or part of the regulated entity's assets and complies with the  
37 requirements and obligations in this chapter.

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

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

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

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

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

10 (d) A list of the categories of third parties and specific  
11 affiliates with whom the regulated entity shares the consumer health  
12 data; and

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

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

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

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

27 (5) It is a violation of this chapter for a regulated entity to  
28 contract with a processor to process consumer health data in a manner  
29 that is inconsistent with the regulated entity's consumer health data  
30 privacy policy.

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

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

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

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

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

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

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

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

18 NEW SECTION. **Sec. 6.** (1) A consumer has the right to confirm  
19 whether a regulated entity is collecting, sharing, or selling  
20 consumer health data concerning the consumer and to access such data,  
21 including a list of all third parties and affiliates with whom the  
22 regulated entity has shared or sold the consumer health data and an  
23 active email address or other online mechanism that the consumer may  
24 use to contact these third parties.

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

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

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

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



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

4 (b) All affiliates, processors, contractors, and other third  
5 parties that receive notice of a consumer's deletion request shall  
6 honor the consumer's deletion request and delete the consumer health  
7 data from its records, subject to the same requirements of this  
8 chapter.

9 (c) If consumer health data that a consumer requests to be  
10 deleted is stored on archived or backup systems, then the request for  
11 deletion may be delayed to enable restoration of the archived or  
12 backup systems and such delay may not exceed six months from  
13 authenticating the deletion request.

14 (4) A consumer may exercise the rights set forth in this chapter  
15 by submitting a request, at any time, to a regulated entity. Such a  
16 request may be made by a secure and reliable means established by the  
17 regulated entity and described in its consumer health data privacy  
18 policy. The method must take into account the ways in which consumers  
19 normally interact with the regulated entity, the need for secure and  
20 reliable communication of such requests, and the ability of the  
21 regulated entity to authenticate the identity of the consumer making  
22 the request. A regulated entity may not require a consumer to create  
23 a new account in order to exercise consumer rights pursuant to this  
24 chapter but may require a consumer to use an existing account.

25 (5) If a regulated entity is unable to authenticate the request  
26 using commercially reasonable efforts, the regulated entity is not  
27 required to comply with a request to initiate an action under this  
28 section and may request that the consumer provide additional  
29 information reasonably necessary to authenticate the consumer and the  
30 consumer's request.

31 (6) Information provided in response to a consumer request must  
32 be provided by a regulated entity free of charge, up to twice  
33 annually per consumer. If requests from a consumer are manifestly  
34 unfounded, excessive, or repetitive, the regulated entity may charge  
35 the consumer a reasonable fee to cover the administrative costs of  
36 complying with the request or decline to act on the request. The  
37 regulated entity bears the burden of demonstrating the manifestly  
38 unfounded, excessive, or repetitive nature of the request.

39 (7) A regulated entity shall respond to the consumer without  
40 undue delay, but in all cases within 45 days of receipt of the

1 request submitted pursuant to the methods described in this section.  
2 The response period may be extended once by 45 additional days when  
3 reasonably necessary, taking into account the complexity and number  
4 of the consumer's requests, so long as the regulated entity informs  
5 the consumer of any such extension within the initial 45-day response  
6 period, together with the reason for the extension.

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

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

27 (2) A regulated entity shall establish, implement, and maintain  
28 administrative, technical, and physical data security practices that,  
29 at a minimum, satisfy reasonable standard of care within the  
30 regulated entity's industry to protect the confidentiality,  
31 integrity, and accessibility of consumer health data appropriate to  
32 the volume and nature of the personal data at issue.

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

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

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

7 (3) If a processor fails to adhere to the regulated entity's  
8 instructions or processes consumer health data in a manner that is  
9 outside the scope of the processor's contract with the regulated  
10 entity, the processor is considered a regulated entity with regard to  
11 such data and is subject to all the requirements of this chapter with  
12 regard to such data.

13 NEW SECTION. **Sec. 9.** (1) It is unlawful for any person to sell  
14 or offer to sell consumer health data concerning a consumer without  
15 first obtaining valid authorization from the consumer. The sale of  
16 consumer health data must be consistent with the valid authorization  
17 signed by the consumer.

18 (2) A valid authorization to sell consumer health data is a  
19 document consistent with this section and must be written in plain  
20 language. The valid authorization to sell consumer health data must  
21 contain the following:

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

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

26 (c) The name and contact information of the person purchasing the  
27 consumer health data from the seller identified in (b) of this  
28 subsection;

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

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

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

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

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

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

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

6 (a) The expiration date has passed;

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

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

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

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

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

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

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

27 NEW SECTION. Sec. 11. (1) For actions brought by the attorney  
28 general to enforce this chapter, the legislature finds that the  
29 practices covered by this chapter are matters vitally affecting the  
30 public interest for the purpose of applying the consumer protection  
31 act, chapter 19.86 RCW. A violation of this chapter is not reasonable  
32 in relation to the development and preservation of business, and is  
33 an unfair or deceptive act in trade or commerce and an unfair method  
34 of competition for the purpose of applying the consumer protection  
35 act, chapter 19.86 RCW.

36 (2) Any consumer injured by a violation of this chapter may bring  
37 an action under chapter 19.86 RCW, but must establish all required

1 elements of an action under chapter 19.86 RCW before relief may be  
2 granted.

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

4 (a) Information that meets the definition of:

5 (i) Protected health information for purposes of the federal  
6 health insurance portability and accountability act of 1996 and  
7 related regulations;

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

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

13 (iv) Identifiable private information for purposes of the federal  
14 policy for the protection of human subjects, 45 C.F.R. Part 46;  
15 identifiable private information that is otherwise information  
16 collected as part of human subjects research pursuant to the good  
17 clinical practice guidelines issued by the international council for  
18 harmonization; the protection of human subjects under 21 C.F.R. Parts  
19 50 and 56; or personal data used or shared in research conducted in  
20 accordance with one or more of the requirements set forth in this  
21 subsection;

22 (v) Information and documents created specifically for, and  
23 collected and maintained by:

24 (A) A quality improvement committee for purposes of RCW  
25 43.70.510, 70.230.080, or 70.41.200;

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

27 (C) A quality assurance committee for purposes of RCW 74.42.640  
28 or 18.20.390; or

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

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

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

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 illegal activity; preserve the integrity  
34 or security of systems; or investigate, report, or prosecute those  
35 responsible for any such action.

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

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

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

--- END ---