

JAN 19 2024

A BILL FOR AN ACT

RELATING TO CONSUMER HEALTH DATA.

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

1 SECTION 1. The Hawaii Revised Statutes is amended by
2 adding a new chapter to be appropriately designated and to read
3 as follows:

4 **"CHAPTER**

5 **PRIVACY OF CONSUMER HEALTH DATA**

6 § -1 **Definitions.** As used in this chapter:

7 "Abortion" means the termination of a pregnancy for
8 purposes other than producing a live birth.

9 "Affiliate" means a legal entity that shares common
10 branding with another legal entity and controls, is controlled
11 by, or is under common control with another legal entity. For
12 the purposes of this definition, "control" or "controlled"
13 means:

14 (1) Ownership of, or the power to vote, more than fifty
15 per cent of the outstanding shares of any class of
16 voting security of a company;



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

4 (3) The power to exercise controlling influence over the
5 management of a company.

6 "Authenticate" means to use reasonable means to determine
7 that a request to exercise any of the rights afforded in this
8 chapter is being made by, or on behalf of, the consumer who is
9 entitled to exercise consumer rights with respect to the
10 consumer health data at issue.

11 "Biometric data" means data that is generated from the
12 measurement or technological processing of an individual's
13 physiological, biological, or behavioral characteristics and
14 that identifies a consumer, whether individually or in
15 combination with other data. Biometric data includes but is not
16 limited to:

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

20 (2) Keystroke patterns or rhythms and gait patterns or
21 rhythms that contain identifying information.



1 "Collect" means to buy, rent, access, retain, receive,
2 acquire, infer, derive, or otherwise process consumer health
3 data in any manner.

4 "Consent" means a clear affirmative act that signifies a
5 consumer's freely given, specific, informed, opt-in, voluntary,
6 and unambiguous agreement, which may include written consent
7 provided by electronic means. "Consent" may not be obtained by:

- 8 (1) A consumer's acceptance of a general or broad terms of
9 use agreement or a similar document that contains
10 descriptions of personal data processing along with
11 other unrelated information;
- 12 (2) A consumer hovering over, muting, pausing, or closing
13 a given piece of content; or
- 14 (3) A consumer's agreement obtained using deceptive
15 designs.

16 "Consumer" means a natural person who is a resident of the
17 State or a natural person whose consumer health data is
18 collected in the State. "Consumer" means a natural person who
19 acts only in an individual or household context, however
20 identified, including by any unique identifier. "Consumer" does
21 not include an individual acting in an employment context.



1 "Consumer health data" means personal information that is
2 linked or reasonably linkable to a consumer and that identifies
3 the consumer's past, present, or future physical or mental
4 health status. Physical or mental health status includes but is
5 not limited to:

- 6 (1) Individual health conditions, treatment, diseases, or
7 diagnosis;
- 8 (2) Social, psychological, behavioral, and medical
9 interventions;
- 10 (3) Health-related surgeries or procedures;
- 11 (4) Use or purchase of prescribed medication;
- 12 (5) Bodily functions, vital signs, symptoms, or
13 measurements of the information described in this
14 definition;
- 15 (6) Diagnoses or diagnostic testing, treatment, or
16 medication;
- 17 (7) Gender-affirming care information;
- 18 (8) Reproductive or sexual health information;
- 19 (9) Biometric data;
- 20 (10) Genetic data;



- 1 (11) Precise location information that could reasonably
- 2 indicate a consumer's attempt to acquire or receive
- 3 health services or supplies;
- 4 (12) Data that identifies a consumer seeking health care
- 5 services; or
- 6 (13) Any information that a regulated entity or a small
- 7 business, or their respective processor, processes to
- 8 associate or identify a consumer with the data
- 9 described in paragraphs (1) through (12) that is
- 10 derived or extrapolated from nonhealth information
- 11 (such as proxy, derivative, inferred, or emergent data
- 12 by any means, including algorithms or machine
- 13 learning).
- 14 "Consumer health data" does not include personal information
- 15 that is used to engage in public or peer-reviewed scientific,
- 16 historical, or statistical research in the public interest that
- 17 adheres to all other applicable ethics and privacy laws and is
- 18 approved, monitored, and governed by an institutional review
- 19 board, human subjects research ethics review board, or a similar
- 20 independent oversight entity that determines that the regulated
- 21 entity or the small business has implemented reasonable



1 safeguards to mitigate privacy risks associated with research,
2 including any risks associated with reidentification.

3 "Deceptive design" means a user interface designed or
4 manipulated with the effect of subverting or impairing user
5 autonomy, decision making, or choice.

6 "Deidentified data" means data that cannot reasonably be
7 used to infer information about, or otherwise be linked to, an
8 identified or identifiable consumer, or a device linked to a
9 consumer, if the regulated entity or the small business that
10 possesses data:

- 11 (1) Takes reasonable measures to ensure that the data
12 cannot be associated with a consumer;
- 13 (2) Publicly commits to process data only in a
14 deidentified fashion and not attempt to reidentify
15 data; and
- 16 (3) Contractually obligates any recipients of data to
17 satisfy the criteria set forth in this definition.

18 "Gender-affirming care information" means personal
19 information relating to seeking or obtaining past, present, or
20 future gender-affirming care services. "Gender-affirming care
21 information" includes, but is not limited to:



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

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

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

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

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



- 1 (1) Raw sequence data that result from the sequencing of a
- 2 consumer's complete extracted deoxyribonucleic acid
- 3 (DNA) or a portion of the extracted DNA;
- 4 (2) Genotypic and phenotypic information that results from
- 5 analyzing the raw sequence data; and
- 6 (3) Self-reported health data that a consumer submits to a
- 7 regulated entity or a small business and that is
- 8 analyzed in connection with consumer's raw sequence
- 9 data.

10 "Geofence" means technology that uses global positioning
11 coordinates, cell tower connectivity, cellular data, radio
12 frequency identification, Wifi data, or any other form of
13 spatial or location detection to establish a virtual boundary
14 around a specific physical location, or to locate a consumer
15 within a virtual boundary that is two thousand feet or less from
16 the perimeter of the physical location.

17 "Health care services" means any service provided to a
18 person to assess, measure, improve, or learn about a person's
19 mental or physical health, including but not limited to:

- 20 (1) Individual health conditions, status, diseases, or
- 21 diagnoses;



- 1 (2) Social, psychological, behavioral, and medical
- 2 interventions;
- 3 (3) Health-related surgeries or procedures;
- 4 (4) Use or purchase of medication;
- 5 (5) Bodily functions, vital signs, symptoms, or
- 6 measurements of the information described in this
- 7 subsection;
- 8 (6) Diagnoses or diagnostic testing, treatment, or
- 9 medication;
- 10 (7) Reproductive health care services; or
- 11 (8) Gender-affirming care services.

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

19 "Person" means, where applicable, natural persons,
20 corporations, trusts, unincorporated associations, and
21 partnerships. "Person" does not include government agencies,



1 tribal nations, or contracted service providers when processing
2 consumer health data on behalf of a government agency.

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

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



1 "Process" or "processing" means any operation or set of
2 operations performed on consumer health data.

3 "Processor" means a person that processes consumer health
4 data on behalf of a regulated entity or a small business.

5 "Publicly available information" means information that:

6 (1) Is lawfully made available through federal, state, or
7 local government records or widely distributed media;
8 and

9 (2) A regulated entity or a small business has a
10 reasonable basis to believe a consumer has lawfully
11 made available to the general public.

12 "Publicly available information" does not include any biometric
13 data collected about a consumer by a business without the
14 consumer's consent.

15 "Regulated entity" means any legal entity that:

16 (1) Conducts business in the State, or produces or
17 provides products or services that are targeted to
18 consumers in the State; and

19 (2) Alone or jointly with others, determines the purpose
20 and means of collecting, processing, sharing, or
21 selling of consumer health data. "Regulated entity"



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

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

- 8 (1) Precise location information that could reasonably
9 indicate a consumer's attempt to acquire or receive
10 reproductive or sexual health services;
- 11 (2) Efforts to research or obtain reproductive or sexual
12 health services; or
- 13 (3) Any reproductive or sexual health information that is
14 derived, extrapolated, or inferred, including from
15 nonhealth information (such as proxy, derivative,
16 inferred, emergent, or algorithmic data).

17 "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
20 limited to:



- 1 (1) Individual health conditions, status, diseases, or
2 diagnoses;
- 3 (2) Social, psychological, behavioral, and medical
4 interventions;
- 5 (3) Health-related surgeries or procedures, including but
6 not limited to abortions;
- 7 (4) Use or purchase of medication, including but not
8 limited to medications for the purposes of abortion;
- 9 (5) Bodily functions, vital signs, symptoms, or
10 measurements of the information described in this
11 definition;
- 12 (6) Diagnoses or diagnostic testing, treatment, or
13 medication; or
- 14 (7) Medical or nonmedical services related to and provided
15 in conjunction with an abortion, including but not
16 limited to associated diagnostics, counseling,
17 supplies, and follow-up services.

18 "Sell" or "sale" means the exchange of consumer health data
19 for monetary or other valuable consideration. "Sell" or "sale"
20 does not include the exchange of consumer health data for
21 monetary or other valuable consideration:



1 (1) To a third party as an asset that is part of a merger,
2 acquisition, bankruptcy, or other transaction in which
3 the third party assumes control of all or part of the
4 regulated entity's or the small business' assets that
5 complies with the requirements and obligations in this
6 chapter; or

7 (2) By a regulated entity or a small business to a
8 processor when the exchange is consistent with the
9 purpose for which the consumer health data was
10 collected and disclosed to the consumer.

11 "Share" or "sharing" means to release, disclose,
12 disseminate, divulge, make available, provide access to,
13 license, or otherwise communicate orally, in writing, or by
14 electronic or other means, consumer health data by a regulated
15 entity or a small business to a third party or affiliate. The
16 term "share" or "sharing" does not include:

17 (1) The disclosure of consumer health data by a regulated
18 entity or a small business to a processor when the
19 sharing is to provide goods or services in a manner
20 consistent with the purpose for which the consumer



1 health data was collected and disclosed to the
2 consumer;

3 (2) The disclosure of consumer health data to a third
4 party with whom the consumer has a direct relationship
5 when:

6 (A) The disclosure is for purposes of providing a
7 product or service requested by the consumer;

8 (B) The regulated entity or the small business
9 maintains control and ownership of the data; and

10 (C) The third party uses the consumer health data
11 only at direction from the regulated entity or
12 the small business and consistent with the
13 purpose for which it was collected and consented
14 to by the consumer; or

15 (3) The disclosure or transfer of personal data to a third
16 party as an asset that is part of a merger,
17 acquisition, bankruptcy, or other transaction in which
18 the third party assumes control of all or part of the
19 regulated entity's or the small business' assets and
20 complies with the requirements of this chapter.



1 "Small business" means a regulated entity that satisfies
2 one or both of the following thresholds:

3 (1) Collects, processes, sells, or shares consumer health
4 data of fewer than one hundred thousand consumers
5 during a calendar year; or

6 (2) Derives less than fifty per cent of gross revenue from
7 the collection, processing, selling, or sharing of
8 consumer health data, and controls, processes, sells,
9 or shares consumer health data of fewer than twenty-
10 five thousand consumers.

11 "Third party" means an entity other than a consumer,
12 regulated entity, processor, small business, or affiliate of the
13 regulated entity or the small business.

14 § -2 Consumer health data privacy policy. (a) A
15 regulated entity and a small business shall maintain a consumer
16 health data privacy policy that clearly and conspicuously
17 discloses:

18 (1) The categories of consumer health data collected and
19 the purpose for which the data is collected, including
20 how the data will be used;



- 1 (2) The categories of sources from which the consumer
- 2 health data is collected;
- 3 (3) The categories of consumer health data that is shared;
- 4 (4) A list of the categories of third parties and specific
- 5 affiliates with whom the regulated entity or the small
- 6 business shares the consumer health data; and
- 7 (5) How a consumer can exercise the rights provided in
- 8 section -4.

9 (b) A regulated entity and a small business shall

10 prominently publish a link to its consumer health data privacy

11 policy on its homepage.

12 (c) A regulated entity or a small business shall not

13 collect, use, or share additional categories of consumer health

14 data not disclosed in the consumer health data privacy policy

15 without first disclosing the additional categories and obtaining

16 the consumer's affirmative consent prior to the collection, use,

17 or sharing of the consumer health data.

18 (d) A regulated entity or a small business shall not

19 collect, use, or share consumer health data for additional

20 purposes not disclosed in the consumer health data privacy

21 policy without first disclosing the additional purposes and



1 obtaining the consumer's affirmative consent prior to the
2 collection, use, or sharing of the consumer health data.

3 (e) It is a violation of this chapter for a regulated
4 entity or a small business to contract with a processor to
5 process consumer health data in a manner that is inconsistent
6 with the regulated entity's or the small business' consumer
7 health data privacy policy.

8 § -3 Consent to collect or share consumer health data.

9 (a) A regulated entity or a small business shall not collect
10 any consumer health data except:

11 (1) With consent from the consumer for the collection for
12 a specified purpose; or

13 (2) To the extent necessary to provide a product or
14 service that the consumer to whom the consumer health
15 data relates has requested from the regulated entity
16 or small business.

17 (b) A regulated entity or a small business shall not share
18 any consumer health data except:

19 (1) With consent from the consumer for the sharing that is
20 separate and distinct from the consent obtained to
21 collect consumer health data; or



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

5 (c) Consent required under this section shall be obtained
6 prior to the collection or sharing, as applicable, of any
7 consumer health data, and the request for consent shall clearly
8 and conspicuously disclose:

9 (1) The categories of consumer health data collected or
10 shared;

11 (2) The purpose of the collection or sharing of the
12 consumer health data, including the specific ways in
13 which it will be used;

14 (3) The categories of entities with whom the consumer
15 health data is shared; and

16 (4) How the consumer can withdraw consent from future
17 collection or sharing of the consumer's health data.

18 (d) A regulated entity or a small business shall not
19 unlawfully discriminate against a consumer for exercising any
20 rights included in this chapter.



1 § -4 Consumer rights. (a) A consumer shall have the
2 right to confirm whether a regulated entity or a small business
3 is collecting, sharing, or selling consumer health data
4 concerning the consumer and to access the data, including a list
5 of all third parties and affiliates with whom the regulated
6 entity or the small business has shared or sold the consumer
7 health data and an active email address or other online
8 mechanism that the consumer may use to contact the third
9 parties.

10 (b) A consumer shall have the right to withdraw consent
11 from the regulated entity's or the small business' collection
12 and sharing of consumer health data concerning the consumer.

13 (c) A consumer shall have the right to have consumer
14 health data concerning the consumer deleted and may exercise
15 that right by informing the regulated entity or the small
16 business of the consumer's request for deletion; provided that:

17 (1) A regulated entity or a small business that receives a
18 consumer's request to delete any consumer health data
19 concerning the consumer shall:

20 (A) Delete the consumer health data from its records,
21 including from all parts of the regulated



- 1 entity's or the small business' network,
2 including archived or backup systems pursuant to
3 paragraph (3) of this subsection; and
- 4 (B) Notify all affiliates, processors, contractors,
5 and other third parties with whom the regulated
6 entity or the small business has shared consumer
7 health data of the deletion request;
- 8 (2) All affiliates, processors, contractors, and other
9 third parties that receive notice of a consumer's
10 deletion request shall honor the consumer's deletion
11 request and delete the consumer health data from its
12 records, subject to the same requirements of this
13 chapter; and
- 14 (3) If consumer health data that a consumer requests to be
15 deleted is stored on archived or backup systems, then
16 the request for deletion may be delayed to enable
17 restoration of the archived or backup systems and the
18 delay may not exceed six months from authenticating
19 the deletion request.
- 20 (d) A consumer may exercise the rights set forth in this
21 chapter by submitting a request, at any time, to a regulated



1 entity or a small business. The request may be made by a secure
2 and reliable means established by the regulated entity or the
3 small business and described in its consumer health data privacy
4 policy. The method shall take into account the ways in which
5 consumers normally interact with the regulated entity or the
6 small business, the need for secure and reliable communication
7 of the requests, and the ability of the regulated entity or the
8 small business to authenticate the identity of the consumer
9 making the request. A regulated entity or a small business
10 shall not require a consumer to create a new account to exercise
11 consumer rights pursuant to this chapter but may require a
12 consumer to use an existing account.

13 (e) If a regulated entity or a small business is unable to
14 authenticate the request using commercially reasonable efforts,
15 the regulated entity or the small business shall not be required
16 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
19 and the consumer's request.

20 (f) Information provided in response to a consumer request
21 shall be provided by a regulated entity and a small business



1 free of charge, up to twice annually per consumer. If requests
2 from a consumer are manifestly unfounded, excessive, or
3 repetitive, the regulated entity or the small business may
4 charge the consumer a reasonable fee to cover the administrative
5 costs of complying with the request or decline to act on the
6 request. The regulated entity and the small business shall bear
7 the burden of demonstrating the manifestly unfounded, excessive,
8 or repetitive nature of the request.

9 (g) A regulated entity and a small business shall comply
10 with the consumer's requests under subsections (a) through (c)
11 within forty-five days of receipt of the consumer's request. A
12 regulated entity and a small business shall promptly take steps
13 to authenticate a consumer request; provided that the entity and
14 small business shall comply with the consumer's request within
15 forty-five days of receipt of the consumer's request. The
16 response period may be extended once by forty-five additional
17 days when reasonably necessary, taking into account the
18 complexity and number of the consumer's requests, so long as the
19 regulated entity or the small business informs the consumer of
20 any extension within the initial forty-five-day response period,
21 together with the reason for the extension.



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

16 § -5 **Restrictions and security requirements.** A
17 regulated entity and a small business shall:

18 (1) Restrict access to consumer health data by the
19 employees, processors, and contractors of the
20 regulated entity or small business to only those
21 employees, processors, and contractors for which



1 access is necessary to further the purposes for which
2 the consumer provided consent or where necessary to
3 provide a product or service that the consumer to whom
4 the consumer health data relates has requested from
5 the regulated entity or small business; and

6 (2) Establish, implement, and maintain administrative,
7 technical, and physical data security practices that,
8 at a minimum, satisfy reasonable standards of care
9 within the regulated entity's or the small business'
10 industry to protect the confidentiality, integrity,
11 and accessibility of consumer health data appropriate
12 to the volume and nature of the consumer health data
13 at issue.

14 § -6 Consumer rights. (a) A processor shall process
15 consumer health data only pursuant to a binding contract between
16 the processor and the regulated entity or the small business
17 that sets forth the processing instructions and limit the
18 actions the processor may take with respect to the consumer
19 health data it processes on behalf of the regulated entity or
20 the small business. A processor shall process consumer health
21 data only in a manner that is consistent with the binding



1 instructions set forth in the contract with the regulated entity
2 or the small business.

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

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

15 **§ -7 Sale of consumer health data.** (a) It is unlawful
16 for any person to sell or offer to sell consumer health data
17 concerning a consumer without first obtaining valid
18 authorization from the consumer. The sale of consumer health
19 data shall be consistent with the valid authorization signed by
20 the consumer. This authorization shall be separate and distinct



1 from the consent obtained to collect or share consumer health
2 data, as required under section -3.

3 (b) A valid authorization to sell consumer health data
4 shall be in the form of a document consistent with this section
5 and shall be written in plain language. The valid authorization
6 to sell consumer health data shall contain the following:

7 (1) The specific consumer health data concerning the
8 consumer that the person intends to sell;

9 (2) The name and contact information of the person
10 collecting and selling the consumer health data;

11 (3) The name and contact information of the person
12 purchasing the consumer health data from the seller
13 identified in paragraph (2);

14 (4) A description of the purpose for the sale, including
15 how the consumer health data will be gathered and how
16 it will be used by the purchaser identified in
17 paragraph (3) when sold;

18 (5) A statement that the provision of goods or services
19 may not be conditioned on the consumer signing the
20 valid authorization;



1 (6) A statement that the consumer has a right to revoke
2 the valid authorization at any time and a description
3 on how to submit a revocation of the valid
4 authorization;

5 (7) A statement that the consumer health data sold
6 pursuant to the valid authorization may be subject to
7 rediscovery by the purchaser and may no longer be
8 protected by this section;

9 (8) An expiration date for the valid authorization that
10 expires one year from when the consumer signs the
11 valid authorization; and

12 (9) The signature of the consumer and date.

13 (c) An authorization shall not be valid if the document
14 has any of the following defects:

15 (1) The expiration date has passed;

16 (2) The authorization does not contain all the information
17 required under this section;

18 (3) The authorization has been revoked by the consumer;

19 (4) The authorization has been combined with other
20 documents to create a compound authorization; or



1 (5) The provision of goods or services is conditioned on
2 the consumer signing the authorization.

3 (d) A copy of the signed valid authorization shall be
4 provided to the consumer.

5 (e) The seller and purchaser of consumer health data shall
6 retain a copy of all valid authorizations for sale of consumer
7 health data for six years from the date of its signature or the
8 date when it was last in effect, whichever is later.

9 § -8 **Prohibition of a geofence.** It is unlawful for any
10 person to implement a geofence around an entity that provides
11 in-person health care services where the geofence is used to:

- 12 (1) Identify or track consumers seeking health care
13 services;
- 14 (2) Collect consumer health data from consumers; or
- 15 (3) Send notifications, messages, or advertisements to
16 consumers related to their consumer health data or
17 health care services.

18 § -9 **Remedies.** The legislature finds that the practices
19 covered by this chapter are matters vitally affecting the public
20 interest. A violation of this chapter shall constitute an



1 unfair and deceptive act or practice in the conduct of any trade
2 or commerce pursuant to chapter 480.

3 § -10 Exceptions for disclosure of consumer health data.

4 (a) This chapter does not apply to information that meets the
5 definition of:

- 6 (1) Protected health information for purposes of the
7 federal Health Insurance Portability and
8 Accountability Act of 1996 and related regulations;
- 9 (2) Health care information collected, used, or disclosed
10 in accordance with part V of chapter 622;
- 11 (3) Patient identifying information collected, used, or
12 disclosed in accordance with title 42 Code of Federal
13 Regulations Part 2, established pursuant to title 42
14 United States Code section 290dd-2;
- 15 (4) Identifiable private information for purposes of the
16 federal policy for the protection of human subjects,
17 title 45 Code of Federal Regulations Part 46;
18 identifiable private information that is otherwise
19 information collected as part of human subjects
20 research pursuant to the good clinical practice
21 guidelines issued by the international council for



1 harmonization; the protection of human subjects under
2 title 21 Code of Federal Regulations Parts 50 and 56;
3 or personal data used or shared in research conducted
4 in accordance with one or more of the requirements set
5 forth in this subsection;

6 (5) Information and documents created specifically for,
7 and collected and maintained by:

8 (A) The department of health for purposes of section
9 321-230;

10 (B) A health care peer review committee for purposes
11 of chapter 671D;

12 (C) A quality assurance committee for purposes of
13 section 624-25.5 or 663-1.7;

14 (D) A hospital, or licensed physician pursuant to
15 chapter 453, for reporting of health care-
16 associated infections for purposes of section
17 325-2.5, for the notification of an incident for
18 purposes of section 453-8.7, or reports regarding
19 adverse events for purposes of section 453-14; or

20 (E) A manufacturer, as defined in title 21 Code of
21 Federal Regulations section 820.3(o);



- 1 (6) Information and documents created for purposes of the
2 federal Health Care Quality Improvement Act of 1986,
3 and related regulations;
- 4 (7) Patient safety work product for purposes of title 42
5 Code of Federal Regulations Part 3, established
6 pursuant to title 42 United States Code sections
7 299b-21 through 299b-26;
- 8 (8) Information that is deidentified in accordance with
9 the requirements for deidentification set forth in
10 title 45 Code of Federal Regulations Part 164, and is
11 derived from any of the health care-related
12 information listed in paragraph (8);
- 13 (9) Information originating from, and intermingled to be
14 indistinguishable with, information under this
15 subsection that is maintained by:
 - 16 (A) A covered entity or business associate as defined
17 by the Health Insurance Portability and
18 Accountability Act of 1996 and related
19 regulations;
 - 20 (B) A health care facility or health care provider as
21 defined in section 323B-2; or



1 (C) A program or a qualified service organization as
2 defined by title 42 Code of Federal Regulations
3 Part 2, established pursuant to title 42 United
4 States Code section 290dd-2;

5 (10) Information used only for public health activities and
6 purposes as described in title 45 Code of Federal
7 Regulations section 164.512 or that is part of a
8 limited data set, as defined, and is used, disclosed,
9 and maintained in the manner required, by title 45
10 Code of Federal Regulations Section 164.514;

11 (b) Personal information that is governed by and
12 collected, used, or disclosed pursuant to the following
13 regulations, parts, titles, or acts, is exempt from this
14 chapter:

15 (1) The Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.)
16 and implementing regulations;

17 (2) Part C of Title XI of the Social Security Act (42
18 U.S.C. 1320d et seq.);

19 (3) The Fair Credit Reporting Act (15 U.S.C. 1681 et
20 seq.);



1 (4) The Family Educational Rights and Privacy Act (20
2 U.S.C. 1232g; 34 C.F.R. 99.0); or

3 (5) Privacy rules adopted by the insurance commissioner.

4 (c) The obligations imposed on regulated entities, small
5 businesses, and processors under this chapter shall not restrict
6 a regulated entity's, small business', or processor's ability
7 for collection, use, or disclosure of consumer health data to
8 prevent, detect, protect against, or respond to security
9 incidents, identity theft, fraud, harassment, malicious or
10 deceptive activities, or any activity that is illegal under
11 state or federal law; preserve the integrity or security of
12 systems; or investigate, report, or prosecute those responsible
13 for any action that is illegal under state or federal law.

14 (d) If a regulated entity, small business, or processor
15 processes consumer health data pursuant to subsection (c) of
16 this section, the entity shall bear the burden of demonstrating
17 that the processing qualifies for the exemption and complies
18 with the requirements of this section."

19 SECTION 2. If any provision of this Act, or the
20 application thereof to any person or circumstance, is held
21 invalid, the invalidity does not affect other provisions or



1 applications of the Act that can be given effect without the
2 invalid provision or application, and to this end the provisions
3 of this Act are severable.

4 SECTION 3. This Act shall take effect upon its approval.

5

INTRODUCED BY:





S.B. NO. 2696

Report Title:

Consumer Health Data; Privacy

Description:

Establishes standards for the collection, sale, and destruction of consumer health data by regulated entities and small businesses.

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.

