2026 -- H 7357

========
LC004350
========

S T A T E O F R H O D E I S L A N D

IN GENERAL ASSEMBLY

JANUARY SESSION, A.D. 2026

A N A C T

RELATING TO HEALTH AND SAFETY -- REPRODUCTIVE HEALTH AND GENDER-AFFIRMING HEALTHCARE DATA PRIVACY ACT

Introduced By: Representatives Knight, Boylan, McEntee, Speakman, Donovan, Carson, Diaz, Cortvriend, Spears, and Kazarian
Date Introduced: January 28, 2026

Referred To: House Judiciary

It is enacted by the General Assembly as follows:

SECTION 1. Title 23 of the General Laws entitled "HEALTH AND SAFETY" is hereby amended by adding thereto the following chapter:

CHAPTER 101.1

REPRODUCTIVE HEALTH AND GENDER-AFFIRMING HEALTHCARE DATA PRIVACY ACT

23-101.1-1. Title.

This chapter may be cited as the "Reproductive Health and Gender-Affirming Healthcare Data Privacy Act."

23-101.1-2. Definitions.

As used in this chapter:

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

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

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

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

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

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

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

(ii) Keystroke patterns or rhythms and gait patterns or rhythms that contain identifying information.

(4) "Collect" means to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any manner, including receiving the data from the individual, either actively or passively, or by observing or tracking the individual's online activity or precise location.

(5)(i) "Consent" means an affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement, which may include written consent provided by electronic means; provided:

(A) The request is provided to the consumer in a clear and conspicuous stand-alone disclosure;

(B) The request includes a description of the processing purpose for which the consumer's consent is sought and clearly states the specific categories of personal data that the regulated entity intends to collect, process, or transfer; and

(C) The request is made available to the consumer in each language in which the regulated entity provides a product or service for which authorization is sought and in a manner reasonably accessible to consumers with disabilities.

(ii) "Consent" may not be obtained by:

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

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

(C) A consumer's agreement obtained through the use of deceptive designs; or

(D) Inference from the inaction of a consumer or the consumer's continued use of a service or product provided by the regulated entity.

(6) "Consumer" means a natural person who is

(i) A Rhode Island resident, or a natural person whose consumer health data is collected while present in Rhode Island; and

(ii) Who is acting only in an individual or household context, however identified, including by any unique identifier.

(iii) "Consumer" does not include an individual acting in an employment context.

(7) "Consumer health data" means:

(i)(A) A consumer's gender-affirming care information;

(B) A consumer's reproductive or sexual health information; or

(ii) Any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the data described in subsection (7)(i) of this section that is derived or extrapolated from information that is not consumer health data (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).

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

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

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

(i) Takes reasonable measures to ensure that such data cannot be associated with a consumer;

(ii) Publicly commits to process such data only in a deidentified fashion and not attempt to reidentify such data; and

(iii) Contractually obligates any recipients of such data to satisfy the criteria set forth in this subsection.

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

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

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

(iii) Any gender-affirming care information that is derived, extrapolated, or inferred, including from information that is not consumer health data, such as proxy, derivative, inferred, emergent, or algorithmic data.

(11) "Gender-affirming care-related services" means health services or products relating to the treatment of gender dysphoria and gender incongruence that support and affirm an individual's gender identity including, but not limited to:

(i) Gender-affirming healthcare services as defined in § 23-101-2;

(ii) Individual health conditions, status, or diagnoses;

(iii) Psychological, behavioral, and medical interventions;

(iv) Surgeries or procedures;

(v) Use or purchase of medication including, but not limited to, medications for the purposes of gender-affirming hormone therapy;

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

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

(viii) Medical or nonmedical services related to and/or provided in conjunction with the treatment of gender dysphoria and gender incongruence including, but not limited to, associated diagnostics, counseling, supplies, and follow-up services.

(12) "Geofence" 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, or to locate a consumer within a virtual boundary. For purposes of this definition, "geofence" means a virtual boundary that is two thousand feet (2,000') or less from the perimeter of the physical location.

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

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

a government agency.

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

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

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

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

(19) "Publicly available information" means information that:

(i) Is made available through federal, state, or municipal government records or widely distributed media;

(ii) Is released in a disclosure to the general public as required by federal, state, or local law; or

(iii) A regulated entity or a small business has a reasonable basis to believe a consumer has made available in such a way that the consumer no longer maintains a reasonable expectation of privacy in the information. Provided, "publicly available information" does not include any biometric data collected about a consumer by a business without the consumer's consent or publicly available information combined or intermixed with personal information.

(20) "Regulated entity" means any legal entity that:

(i) Provides gender-affirming care-related services or reproductive or sexual health-related services in Rhode Island, or produces or provides gender-affirming care-related services or reproductive or sexual health-related services that are targeted to consumers in Rhode Island;

(ii) Alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data; and

(iii) Collects consumer health data directly from consumers. "Regulated entity" does not mean government agencies, tribal nations, or contracted service providers when processing

consumer health data on behalf of the government agency.

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

(i) Precise location information that could reasonably indicate a consumer's attempt to acquire or receive reproductive or sexual health-related services;

(ii) Efforts to research or obtain reproductive or sexual health-related services; or

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

(22) "Reproductive or sexual health-related services" means health services or products that support or relate to a consumer's reproductive system or sexual well-being including, but not limited to, services or products relating to:

(i) Reproductive healthcare services as defined in § 23-101-2;

(ii) Individual health conditions, status, or diagnoses;

(iii) Psychological, behavioral, and medical interventions;

(iv) Surgeries or procedures including, but not limited to, abortions;

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

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

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

(vii) Medical or nonmedical services related to or provided in conjunction with pregnancy, contraception, assisted reproduction, pregnancy loss management, or the termination of a pregnancy including, but not limited to, associated diagnostics, counseling, supplies, and follow-up services.

(23) "Sell" or "sale" means the sharing of consumer health data in exchange for monetary or other valuable consideration.

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

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

(A) The disclosure of consumer health data by a regulated entity or a small business to a

processor when such sharing is to provide goods or services in a manner consistent with the purpose for which the consumer health data was collected and disclosed to the consumer;

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

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

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

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

(C) The disclosure or transfer of consumer health data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the regulated entity's or the small business's assets and complies with the requirements and obligations in this chapter, but only if the regulated entity or small business, in a reasonable time before the disclosure, provides the affected consumer with both of the following:

(I) A notice describing the transfer, including the name of the entity receiving the individual's consumer health data and the applicable privacy policies of the entity; and

(II) A reasonable opportunity to withdraw previously provided consent related to the individual's consumer health data and request the deletion of the individual's consumer health data;

(D) The disclosure is of publicly available information.

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

(i) Collects, processes, sells, or shares consumer health data of fewer than one hundred thousand (100,000) consumers during a calendar year; or

(ii) Derives less than fifty percent (50%) of gross revenue from the collection, processing, selling, or sharing of consumer health data, and controls, processes, sells, or shares consumer health data of fewer than twenty-five thousand (25,000) consumers.

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

23-101.1-3. Consumer health data privacy policy.

(a)(1) A regulated entity, by January 1, 2027, and a small business, by April 1, 2027, shall maintain a consumer health data privacy policy that clearly and conspicuously discloses:

(i) The categories of consumer health data collected and the purpose for which the data is

collected, including how the data will be used;

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

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

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

(v) How a consumer can exercise the rights provided in §23-101.1- 5.

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

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

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

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

23-101.1-4. Collection or sharing of consumer health data.

(a)(1) A regulated entity, by January 1, 2027, and a small business, by April 1, 2027, may not collect or share any consumer health data, including the sale of consumer health data, except:

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

(ii) If the consumer health data is collected or shared only for one or more of the following permissible purposes:

(A) As necessary to provide a product, service, or service feature to the individual to whom the consumer health data pertains when requested by that individual;

(B) To initiate, manage, execute, or complete a financial or commercial transaction or to fulfill an order for a specific product or service requested by an individual to whom the consumer health data pertains, including, but not limited to, associated routine administrative, operational, and account servicing activity such as billing, shipping, storage, and accounting;

(C) To comply with an obligation under a law of this state or federal law;

(D) To protect public safety or public health;

(E) To prevent, detect, protect against, or respond to a security incident, identity theft,

fraud, harassment, malicious or deceptive activities, or activities that are illegal under the laws of this state;

(F) To preserve the integrity or security of systems; and

(G) To investigate, report, or prosecute persons responsible for activities that are illegal under the laws of this state.

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

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

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

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

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

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

23-101.1-5. Consumer rights and requests -- Refusal -- Appeal.

(a) A consumer has the right to confirm whether a regulated entity or a small business is collecting, sharing, or selling consumer health data concerning the consumer and to access such data, including a list of all third parties and affiliates with whom the regulated entity or the small business has shared or sold the consumer health data and an active email address or other online mechanism that the consumer may use to contact these third parties.

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

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

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

(i) Delete the consumer health data from its records, including from all parts of the regulated entity's or the small business's network, including archived or backup systems pursuant to subsection (c)(3) of this section; and

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

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

(3) If consumer health data that a consumer requests to be deleted is stored on archived or backup systems, then the request for deletion may be delayed to enable restoration of the archived or backup systems; provided that, such delay may not exceed six (6) months from authenticating the deletion request.

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

(e) If a regulated entity or a small business is unable to authenticate the request using commercially reasonable efforts, the regulated entity or the small business is not required to comply with a request to initiate an action under this section and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

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

(g) A regulated entity and a small business shall comply with the consumer's requests under subsections (a) through (d) of this section within forty-five (45) days of receipt of the request submitted pursuant to the methods described in this section. A regulated entity and a small business shall promptly take steps to authenticate a consumer request, but this shall not extend the regulated entity's and the small business's duty to comply with the consumer's request within forty-five (45) days of receipt of the consumer's request. The response period may be extended once by forty-five

(45) additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the regulated entity or the small business informs the consumer of any such extension within the initial forty-five (45) day response period, together with the reason for the extension.

(h) A regulated entity shall comply with this section by January 1, 2027, and a small business shall comply with this section beginning April 1, 2027.

23-101.1-6. Data security practices.

A regulated entity, by January 1, 2027, and a small business, by April 1, 2027, shall:

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

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

23-101.1-7. Processors.

(a)(1) By January 1, 2027, for a regulated entity and April 1, 2027, for a small business, a processor may process consumer health data only pursuant to a binding contract between the processor and the regulated entity or the small business that sets forth the processing instructions and limit the actions the processor may take with respect to the consumer health data it processes on behalf of the regulated entity or the small business.

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

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

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

23-101.1-8. Valid authorization to sell -- Defects -- Provision to consumer.

(a) Subject to the requirements of § 23-101.1-4, by January 1, 2027, for a regulated entity and April 1, 2027, for a small business, it is unlawful for any person to sell or offer to sell consumer health data concerning a consumer without first obtaining valid authorization from the consumer. The sale of consumer health data shall be consistent with the valid authorization signed by the consumer. This authorization shall be separate and distinct from the consent obtained to collect or share consumer health data, as required under the provisions of § 23-101.1-4.

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

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

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

(3) The name and contact information of the person purchasing the consumer health data from the seller identified in subsection (b) of this section;

(4) A description of the purpose for the sale, including how the consumer health data will be gathered and how it will be used by the purchaser identified in subsection (b)(3) of this section when sold;

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

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

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

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

(9) The signature of the consumer and date.

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

(1) The expiration date has passed;

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

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

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

(5) The provision of goods or services is conditioned on the consumer signing the

authorization.

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

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

23-101.1-9. Geofence restrictions.

It is unlawful for any person to implement a geofence around an entity that provides in-person reproductive healthcare services, as defined in § 23-101-2, or gender-affirming healthcare services, as defined in § 23-101-2, where such geofence is used to:

(1) Identify or track consumers seeking reproductive healthcare services or gender-affirming healthcare services; or,

(2) Collect consumer health data from consumers.

23-101.1-10. Exemptions.

This chapter does not apply to:

(1) Information that meets the definition of:

(i) Protected health information for purposes of the federal health insurance portability and accountability act of 1996, Pub. L. No. 104-191 (1996), and related regulations;

(ii) Health care information collected, used, or disclosed in accordance with chapter 37.3 of title 5;

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

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

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

(A) A quality improvement program for purposes of chapter 17.17 of title 23;

(B) A peer review committee for purposes of § 23-17-25;

(C) A quality assurance committee for purposes of chapter 17.17 of title 23; or

(D) A hospital, for reporting of health care-associated adverse events for purposes § 23-17-40.

(vi) Information and documents created for purposes of the federal health care quality

improvement act of 1986, Pub. L. No. 99-660 (1986), and related regulations;

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

(viii) Information that is:

(A) Deidentified in accordance with the requirements for deidentification set forth in 45 C.F.R. Part 164; and

(B) Derived from any of the health care-related information listed or described in subsection (a)(1)(viii)(A) of this section;

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

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

(ii) A health care facility or health care provider; or

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

(3) Information used only for public health activities and purposes as described in 45 C.F.R. Sec. 164.512 or that is part of a limited data set, as defined, and is used, disclosed, and maintained in the manner required, by 45 C.F.R. § 164.514 or corresponding state law.

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

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

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

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

(4) The Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; Part 99 of Title 34, C.F.R.);

(5) The Rhode Island health benefit exchange and applicable statutes and regulations, including 45 C.F.R. § 155.260 and § 42-157-1 et seq.; or

(6) Chapter 17.17 of title 23; and

(7) Privacy rules adopted by the office of the health insurance commissioner.

(c) The obligations imposed on regulated entities, small businesses, and processors under this chapter does not restrict a regulated entity's, small businesses, or processor's ability for collection, use, or disclosure of consumer health data to prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any activity that is illegal under Rhode Island law or federal law; preserve the integrity or security of

systems; or investigate, report, or prosecute those responsible for any such action that is illegal under Rhode Island law or federal law.

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

23-101.1-11. Penalties and remedies.

(a) A person who alleges a violation of this chapter may bring a civil action for appropriate injunctive relief and compensatory and punitive damages in the superior court for the county where the alleged violation occurred, the county where the complainant resides, or the county where the person against whom the civil complaint is filed resides or has their principal place of business. A prevailing plaintiff shall be entitled to an award of reasonable attorneys' fees and costs.

(b) A violation of this chapter shall also constitute a deceptive trade practice in violation of the provisions of chapter 13.1 of title 6, and the attorney general may bring an enforcement action over violations of this chapter.

SECTION 2. This act shall take effect upon passage.

========
LC004350
========

EXPLANATION

BY THE LEGISLATIVE COUNCIL

OF

A N A C T

RELATING TO HEALTH AND SAFETY -- REPRODUCTIVE HEALTH AND GENDER-AFFIRMING HEALTHCARE DATA PRIVACY ACT

***

This act would create the reproductive health and gender-affirming healthcare data privacy act. This act would further protect reproductive and gender-affirming care data. The act would require the holders of such data, with certain exceptions, obtain consent from a consumer before collecting the data. The act would prohibit the sale of the data without the permission of the consumer. The act contains several enforcement mechanisms to ensure compliance with the law, including an individual cause of action and authority for the attorney general to bring enforcement of an action.

This act would take effect upon passage.

========
LC004350
========