S.74

Introduced by Senators Lyons, Gulick and Harrison

Referred to Committee on

Date:

Subject: Health; health information; data privacy

Statement of purpose of bill as introduced: This bill proposes to regulate the collection, sharing, and selling of consumer health data in Vermont.

An act relating to the collection, sharing, and selling of consumer health data

It is hereby enacted by the General Assembly of the State of Vermont:

Sec. 1. 18 V.S.A. chapter 42B is amended to read:

42B. HEALTH CARE PRIVACY

Subchapter 1. Disclosure of Protected Health Information

§ 1881. DISCLOSURE OF PROTECTED HEALTH INFORMATION PROHIBITED

* * *

Subchapter 2. Vermont My Health My Data Act

§ 1891a. SHORT TITLE

This subchapter shall be known and may be cited as the "Vermont My Health My Data Act."

§ 1891b. FINDINGS AND INTENT

(a) Findings. The General Assembly finds that:

(1) The residents of Vermont regard their privacy as a fundamental right and an essential element of their individual freedom. Fundamental privacy rights have long been and continue to be integral to protecting Vermonters and to safeguarding our democratic republic.

(2) Information related to an individual's health conditions or attempts to obtain health care services is among the most personal and sensitive categories of data collected. Vermonters expect that their health data is protected under laws like the Health Insurance Portability and Accountability Act of 1996 (HIPAA). However, HIPAA only covers health data collected by specific health care entities, including most health care providers. Health data collected by noncovered entities, including certain applications and websites, are not afforded the same protections. This act works to close the gap between consumer knowledge and industry practice by providing stronger privacy protections for all of Vermont consumers' health data.

(b) Intent. By enacting this subchapter, it is the intent of the General Assembly to provide heightened protections for Vermonters' health data by:

(1) requiring additional disclosures and consumer consent regarding the collection, sharing, and use of their health data;

(2) empowering consumers with the right to have their health data deleted;

(3) prohibiting the selling of consumer health data without valid authorization signed by the consumer; and

(4) making it unlawful to utilize a geofence around a facility that provides health care services.

§ 1891c. DEFINITIONS

As used in this subchapter:

(1) "Abortion" means any medical treatment intended to induce the termination of, or to terminate, a clinically diagnosable pregnancy except for the purpose of producing a live birth.

(2) "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 purposes of this definition, "control" or "controlled" means any one or more of the following:

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

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

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

(3) "Area agency on aging" has the same meaning as in 33 V.S.A. § 6203.

(4) "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 those consumer rights with respect to the consumer health data at issue.

(5) "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:

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

(B) keystroke patterns or rhythms and gait patterns or rhythms that contain identifying information.

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

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

(B) "Consent" shall not be obtained by:

(i) 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;

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

(iii) a consumer's agreement obtained through the use of deceptive designs.

(8)(A) "Consumer" means a natural person who meets one or both of the following conditions:

(i) the person is a Vermont resident; or

(ii) the person's consumer health data is collected in Vermont.

(B) "Consumer" means a natural person who acts only in an individual or household context, however identified, including by any unique identifier. The term does not include an individual acting in an employment context.

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

(B) For purposes of this definition, physical or mental health status includes:

(i) individual health conditions, treatment diseases, or diagnosis;

(ii) social, psychological, behavioral, and medical interventions;

(iii) health-related surgeries or procedures;

(iv) use or purchase of prescribed medication;

(v) bodily functions, vital signs, symptoms, or measurements of the information described in this subdivision (B);

(vi) diagnoses or diagnostic testing, treatment, or medication;

(vii) gender-affirming care information;

(viii) reproductive or sexual health information;

(ix) biometric data;

(x) genetic data;

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

(xii) data that identifies a consumer seeking health care services; or

(xiii) any information that a regulated entity or a small business, or its respective processor, processes to associate or identify a consumer with the data described in subdivisions (i)–(xii) of this subdivision (B) that is derived or extrapolated from nonhealth information, such as proxy, derivative, inferred, or emergency data by any means, including algorithms or machine learning.

(C) "Consumer health data" does not include 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.

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

(11) "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 the data does all of the following:

(A) takes reasonable measures to ensure that the data cannot be associated with a consumer;

(B) publicly commits to process the data only in a deidentified fashion and not to attempt to reidentify the data; and

(C) contractually obligates any recipients of the data to satisfy the criteria set forth in this subdivision (11).

(12) "Gender-affirming care information" means personal information relating to seeking or obtaining past, present, or future gender-affirming health care services. "Gender-affirming care information" includes:

(A) precise location information that could reasonably indicate a consumer's attempt to acquire or receive gender-affirming health care services;

(B) efforts to research or obtain gender-affirming health care services; or

(C) any gender-affirming care information that is derived, extrapolated, or inferred, including from nonhealth information such as proxy, derivative, inferred, emergent, or algorithmic data.

(13) "Gender-affirming health care services" has the same meaning as in 1 V.S.A. § 150.

(14) "Genetic data" means any data, regardless of its format, that concerns a consumer's genetic characteristics. "Genetic data" includes:

(A) raw sequence data that result from the sequencing of a consumer's complete extracted deoxyribonucleic acid (DNA) or a portion of the extracted DNA;

(B) genotypic and phenotypic information that results from analyzing the raw sequence data; and

(C) self-reported health data that a consumer submits to a regulated entity or a small business and that is analyzed in connection with the consumer's raw sequence data.

(15) "Geofence" means technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wi-Fi data, or any other form of spatial or location detection, individually or in combination, to establish a virtual boundary around a specific physical location or to locate a consumer within a virtual boundary.

(16) "Health care service" means any service provided to a person to assess, measure, improve, or learn about a person's mental or physical health, including:

(A) individual health conditions, status, diseases, or diagnoses;

(B) social, psychological, behavioral, and medical interventions;

(C) health-related surgeries or procedures;

(D) use or purchase of medication;

(E) bodily functions, vital signs, symptoms, or measurements of the information described in this subdivision (16);

(F) diagnoses or diagnostic testing, treatment, or medication;

(G) reproductive health services; or

(H) gender-affirming health care services.

(17) "Homepage" means the introductory page of an internet website and any internet web page on which 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 or the "about," "information," or "settings" page.

(18) "Person" means, where applicable, a natural person, corporation, trust, unincorporated association, or partnership. The term does not include a government agency, tribal nation, or a contracted service provider when processing consumer health data on behalf of a government agency.

(19)(A) "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 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.

(B) "Personal information" does not include publicly available information or deidentified data.

(20) "Precise location information" means information derived from technology, including global positioning system level latitude and longitude coordinates and other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,850 feet.

"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.

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

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

(23)(A) "Publicly available information" means information that:

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

(ii) a regulated entity or a small business has a reasonable basis to believe a consumer has lawfully made available to the general public.

(B) "Publicly available information" does not include any biometric data collected about a consumer by a business without the consumer's consent.

(24)(A) "Regulated entity" means any legal entity that:

(i) conducts business in Vermont, or produces or provides products or services that are targeted to consumers in Vermont; and

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

(B) "Regulated entity" does not mean government agencies or contracted service providers when processing consumer health data on behalf of a government agency.

(25)(A) "Reproductive or sexual health information" means personal information relating to seeking or obtaining past, present, or future reproductive or sexual health services.

(B) "Reproductive or sexual health information" includes:

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

(ii) efforts to research or obtain reproductive or sexual health 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.

(26) "Reproductive or sexual health services" means health services or products that support or relate to a consumer's reproductive system or sexual well-being, including:

(A) individual health conditions, status, diseases, or diagnoses;

(B) social, psychological, behavioral, and medical interventions;

(C) health-related surgeries or procedures, including abortions;

(D) use or purchase of medication, including medications for the purposes of abortion;

(E) bodily functions, vital signs, symptoms, or measurements of the information described in this subdivision (26);

(F) diagnoses or diagnostic testing, treatment, or medication;

(G) medical or nonmedical services related to and provided in conjunction with an abortion, including associated diagnostics, counseling, supplies, and follow-up services; and

(H) any other services included in the definition of "reproductive health care services" in 1 V.S.A. § 150.

(27)(A) "Sell" or "sale" means the exchange of consumer health data for monetary or other valuable consideration.

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

(i) 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; or

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

(28)(A) "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.

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

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

(ii) 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 the direction of the regulated entity or the small business and consistent with the purpose for which it was collected and consented to by the consumer; or

(iii) the disclosure or transfer of personal 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.

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

(A) the entity collects, processes, sells, or shares the consumer health data of fewer than 100,000 consumers during a calendar year; or

(B) the entity derives less than 50 percent of its gross revenue from the collection, processing, selling, or sharing of consumer health data and the entity controls, processes, sells, or shares consumer health data of fewer than 25,000 consumers.

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

§ 1891d. CONSUMER HEALTH DATA PRIVACY POLICY REQUIRED

(a) Each regulated entity or each small business shall maintain a consumer health data privacy policy that clearly and conspicuously discloses:

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

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

(3) the categories of consumer health data that is shared;

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

(5) how a consumer can exercise the rights provided in section 1891f of this chapter.

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

(c) A regulated entity or small business shall 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 the consumer health data.

(d) A regulated entity or small business shall 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 the consumer health data.

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

§ 1891e. COLLECTION AND SHARING OF CONSUMER HEALTH DATA

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

(1) with consent from the consumer for such collection for a specified purpose; or

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

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

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

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

(c) 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 must 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.

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

§ 1891f. CONSUMER RIGHTS

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

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

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

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

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

(B) 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 in accordance with the requirements of this subchapter.

(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 the delay shall not exceed six months from the date of authentication of the deletion request.

(d) Request requirements.

(1) A consumer may exercise the rights set forth in this chapter by submitting a request to a regulated entity or small business at any time. The

request may be made by a secure and reliable means established by the regulated entity or 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 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 small business shall not require a consumer to create a new account in order to exercise consumer rights pursuant to this subchapter but may require a consumer to use an existing account.

(2) If a regulated entity or small business is unable to authenticate the request using commercially reasonable efforts, the regulated entity or 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.

(3) Information provided in response to a consumer request shall be provided by a regulated entity or 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 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 or small

business bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.

(4) A regulated entity or small business shall comply with a consumer's requests under subsections (a) through (c) of this section without undue delay, but in all cases within 45 days following receipt of the request submitted pursuant to the methods described in this section. A regulated entity or small business shall promptly take steps to authenticate a consumer request; provided, however, that completion of these steps does not extend the regulated entity's or small business's duty to comply with the consumer's request within 45 days following receipt of the consumer's request. The response period may be extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, provided the regulated entity or small business informs the consumer of any such extension within the initial 45-day response period, together with the reason for the extension.

(e) Consumer appeal. A regulated entity or small business shall establish a process for a consumer to appeal the regulated entity's or small business's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Within 45 days following receipt of an appeal, a

regulated entity or small business shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the regulated entity or small business shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Office of the Attorney General to submit a complaint.

§ 1891g. PROTECTION OF CONSUMER HEALTH DATA

A regulated entity or small business shall:

(1) restrict access to consumer health data by the regulated entity's or small business's employees, processors, and contractors to only those employees, processors, and contractors for whom 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 the regulated entity or small business; and

(2) establish, implement, and maintain administrative, technical, and physical data security practices that, at a minimum, satisfy reasonable standards of care within the regulated entity's or 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.

§ 1891h. PROCESSORS OF CONSUMER HEALTH DATA

(a) Contract required.

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

(b) Obligation to assist. To the extent possible, a processor shall use appropriate technical and organizational measures to assist the regulated entity or small business in fulfilling the regulated entity's and the small business's obligations under this chapter.

(c) Failure to adhere. If a processor fails to adhere to the regulated entity's or 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 small business, the processor is considered a regulated entity or small business with respect to the data and is subject to all the requirements of this chapter with regard to the data.

§ 1891i. LIMITATIONS ON SALE OF CONSUMER HEALTH DATA

(a) Authorization required. It is unlawful for any person to sell or offer to sell consumer health data regarding a consumer without first obtaining valid authorization from the consumer. The sale of consumer health data must 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 section 1891e of this chapter.

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

(1) the specific consumer health data regarding 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 subdivision (2) of this subsection;

(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 subdivision (3) of this subsection when sold;

(5) a statement that the provision of goods or services shall 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 of 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 after the consumer signs the valid authorization; and

(9) the signature of the consumer and date.

(c) Invalid authorizations. 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 of 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) Copies and retention.

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

(2) A seller or purchaser of consumer health data shall retain a copy of each valid authorization for the sale of consumer health data for six years from the date of its signature or the date when it was last in effect, whichever is later.

§ 1891j. GEOFENCES PROHIBITED

It is unlawful for any person to implement a geofence to establish a virtual boundary that is within 1,850 feet of any health care facility, including any mental health facility or reproductive or sexual health facility, for the purpose of identifying, tracking, collecting data from, or sending any notification to a consumer regarding the consumer's consumer health data.

§ 1891k. VIOLATIONS; ENFORCEMENT

(a) A violation of this subchapter shall be deemed a violation of the Consumer Protection Act, 9 V.S.A. chapter 63. The Attorney General has the same authority to make rules, conduct civil investigations, enter into assurances of discontinuance, and bring civil actions, and private parties have the same rights and remedies, as provided under 9 V.S.A. chapter 63, subchapter 1.

(b) Nothing in this section shall be construed to preclude or supplant any other statutory or common law remedies.

§ 1891l. EXEMPTIONS

(a) This subchapter shall not apply to:

(1) information that meets the definition of:

(A) protected health information for purposes of the federal Health Insurance Portability and Accountability Act of 1996 and related regulations;

(B) 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; or

(C) 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 (a);

(2) information and documents created specifically for, and collected and maintained as part of, the patient safety surveillance and improvement system established pursuant to chapter 43A of this title;

(3) information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, and related regulations;

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

(5) information that is deidentified in accordance with the requirements for deidentification set forth in 45 C.F.R. Part 164;

(6) information originating from, and intermingled so as to be indistinguishable with, information described under subdivisions (1)–(5) of this subsection that is maintained by:

(A) a covered entity that is not a hybrid entity, any health care component of a hybrid entity, or a business associate as those terms are defined by the Health Insurance Portability and Accountability Act of 1996 and related regulations;

(B) a health care facility or health care provider, as defined in section 9402 of this title; or

(C) 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;

(7) information used only for public health activities and purposes as described in 45 C.F.R. § 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

(8) an area agency on aging.

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

(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 and 34 C.F.R. Part 99; and

(5) the Vermont Health Benefit Exchange, 33 V.S.A. chapter 18, subchapter 1, and related federal laws and Vermont rules, including 45 C.F.R. § 155.260.

(c) The obligations imposed on regulated entities, small businesses, and processors under this subchapter shall not be construed to restrict a regulated entity's, small business's, or processor's ability to collect, use, or disclose 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 Vermont 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 Vermont or federal law.

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

Sec. 2. EFFECTIVE DATE

This act shall take effect on January 1, 2026.