Major differences between the two data privacy bills

S.71	S.93
§ 2415. DEFINITIONS Biometric data Consent De-identified data (partial) Gender-affirming health data (partial) Identified or identifiable individual Publicly available information Sensitive data Targeted advertising	**§ 2415. DEFINITIONS**
§ 2416. APPLICABILITY applies to persons who controlled or processed the personal data of more than **25,000 consumers**, excluding payment data transactions or controlled or processed more than **12,500 consumers and derived 25% or more** of its gross revenue from the sale of personal data **S.71 decreases these numbers by 50% in 2027 and another 50% in 2028**	**§ 2416. APPLICABILITY** applies to persons who controlled or processed the personal data of more than **100,000 consumers**, excluding payment data transactions, or controlled or processed more than **25,000 consumers and derived 25%** or more of its gross revenue from the sale of personal data
§ 2417. EXEMPTIONS **In this section, underline means both bills share the same or similar exemption** (a) This chapter does not apply to: (1) a federal, state, tribal, or local government entity in the ordinary course of its operation; (2) protected health information under HIPAA;	**§ 2417. EXEMPTIONS** **In this section, underline means both bills share the same or similar exemption** (a) Except as provided in subsection (c) of this section, this chapter shall not apply to any: (1) body, authority, board, bureau, commission, district or agency of this State or of any political subdivision of this State;

(3) patient–identifying information, for purposes of 42 U.S.C. § 290DD–2; (4)(i) information to the extent it is used for public health, community health, or population health activities and purposes, as authorized by HIPAA, when provided by or to a covered entity or when provided by or to a business associate in accordance with the business associate agreement with a covered entity; (ii) information that is a health care record, as that term is defined in 18 V.S.A. § 9419, if the information is held by an entity that is a covered entity or business associate under HIPAA because it collects, uses, or discloses protected health information; (iii) information that is de-identified in accordance with the requirements for de-identification set forth in 45 C.F.R. 164.514 and that is derived from individually identifiable health information as described in HIPAA; and (iv) personal information consistent with the human subject protection requirements of the U.S. Food and Drug Administration; (5) information used only for public health activities and purposes described in 45 C.F.R. § 164.512 (disclosure of protected health information without authorization); (6) information that identifies a consumer in connection with: (A) activities that are subject to the Federal Policy for the Protection of Human Subjects, codified as 45 C.F.R. Part 46 (HHS protection of human subjects) and in various other federal regulations; (B) activities that are subject to the protections provided in 21 C.F.R. Parts 50 (FDA clinical investigations protection of human subjects) and 56 (FDA clinical investigations institutional review boards); or (C) research conducted in accordance with the requirements set forth in subdivisions (A) and (B) of this subdivision (a)(6) or otherwise in accordance with applicable law; (7) patient identifying information that is collected and processed in accordance with 42 C.F.R. Part 2 (confidentiality of substance use disorder patient records);	(2) person who has entered into a contract with an entity described in subdivision (1) of this subsection to process consumer health data on behalf of the entity; (3) nonprofit organization; **S.71 exempts only certain nonprofits** (4) institution of higher education; (5) national securities association that is registered under 15 U.S.C. 78o-3 of the Securities Exchange Act of 1934, as may be amended; (6) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, and regulations adopted to implement that act; (7) covered entity or business associate, as defined in 45 C.F.R. § 160.103; (8) tribal nation government organization; or (9) air carrier, as: (A) defined in 49 U.S.C. § 40102, as may be amended; and (B) regulated under the Federal Aviation Act of 1958, 49 U.S.C. § 40101 et seq. and the Airline Deregulation Act of 1978, 49 U.S.C. § 41713, as may be amended. (b) The following information, data, and activities are exempt from this chapter: (1) protected health information under HIPAA; (2) patient identifying information that is collected and processed in accordance with 42 C.F.R. Part 2 (confidentiality of substance use disorder patient records); (3) identifiable private information:

(8) patient safety work product that is created and used for purposes of patient safety improvement in accordance with 42 C.F.R. § 3, established in accordance with 42 U.S.C. §§ 299b–21 through 299b–26; (9) information or documents created for the purposes of the Healthcare Quality Improvement Act of 1986, 42 U.S.C. § 11101–11152, and regulations adopted to implement that act; (10) information processed or maintained solely in connection with, and for the purpose of, enabling notice of an emergency to persons that an individual specifies; (11) any activity that involves collecting, maintaining, disclosing, selling, communicating, or using information for the purpose of evaluating a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living if done strictly in accordance with the provisions of the Fair Credit Reporting Act, 15 U.S.C. § 1681–1681x, as may be amended, by: the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, furnisher, or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., as may be amended; (A) a consumer reporting agency; (B) a person who furnishes information to a consumer reporting agency under 15 U.S.C. § 1681s-2 (responsibilities of furnishers of information to consumer reporting agencies); or (C) a person who uses a consumer report as provided in 15 U.S.C. § 1681b(a)(3) (permissible purposes of consumer reports); (12) information collected, processed, sold, or disclosed under and in accordance with the following laws and regulations:	(A) for purposes of the Federal Policy for the Protection of Human Subjects, codified as 45 C.F.R. Part 46 (HHS protection of human subjects) and in various other federal regulations; and (B) that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; (4) information that identifies a consumer in connection with the protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal data used or shared in research, as defined in 45 C.F.R. § 164.501, that is conducted in accordance with the standards set forth in this subdivision and in subdivision (3) of this subsection, or other research conducted in accordance with applicable law; (5) information or documents created for the purposes of the Healthcare Quality Improvement Act of 1986, 42 U.S.C. §§ 11101–11152, and regulations adopted to implement that act; (6) patient safety work product that is created for purposes of improving patient safety under 42 C.F.R. Part 3 (patient safety organizations and patient safety work product); (7) information or documents created for the purposes of the Healthcare Quality Improvement Act of 1986, 42 U.S.C. §§ 11101–11152, and regulations adopted to implement that act; ** this is a duplicate of (5) ** (8) information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA; (9) information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection that is maintained by a covered entity or business associate, program, or qualified service

(A) the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721–2725; (B) data that is subject to the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and regulations adopted to implement that act; (C) data that is subject to the Airline Deregulation Act, Pub. L. No. 95-504, only to the extent that an air carrier collects information related to prices, routes, or services, and only to the extent that the provisions of the Airline Deregulation Act preempt this chapter; (D) data that is subject to the Farm Credit Act, Pub. L. No. 92-181, as may be amended; and (E) data that is subject to federal policy under 21 U.S.C. § 830 (regulation of listed chemicals and certain machines); (13) nonpublic personal information that is processed by a financial institution subject to the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, and regulations adopted to implement that act; (14) a state or federally chartered bank or credit union, or an affiliate or subsidiary that is principally engaged in financial activities, as described in 18 U.S.C. § 1843(k); (15) a person regulated pursuant to 8 V.S.A. part 3 (chapters 101–165) other than a person who, alone or in combination with another person, establishes and maintains a self-insurance program and who does not otherwise engage in the business of entering into policies of insurance; (16) a third-party administrator, as that term is defined in the Third Party Administrator Rule adopted pursuant to 18 V.S.A. § 9417; (17) personal data of a victim or witness of child abuse, domestic violence, human trafficking, sexual assault, violent felony, or stalking that a victim services organization collects, processes, or maintains in the course of its operation; (18) a nonprofit organization that is established to detect and prevent fraudulent acts in connection with insurance;	organization, as specified in 42 U.S.C. § 290dd-2, as may be amended; (10) information used for public health activities and purposes as authorized by HIPAA, community health activities, and population health activities; (11) the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, furnisher, or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., as may be amended; (12) personal data collected, processed, sold, or disclosed under and in compliance with: (A) the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721–2725; and (B) the Farm Credit Act, Pub. L. No. 92-181, as may be amended; (13) personal data regulated by the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, as may be amended; (14) data processed or maintained: (A) in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, consumer health data controller, or third party, to the extent that the data is collected and used within the context of that role; (B) as the emergency contact information of a consumer pursuant to this chapter, used for emergency contact purposes, or (C) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information pursuant to subdivision (1) of this subsection (b) and used for the purposes of administering such benefits; and

(19) information that is processed for purposes of compliance, enrollment or degree verification, or research services by a nonprofit organization that is established to provide enrollment data reporting services on behalf of postsecondary schools as that term is defined in 16 V.S.A. § 176; or (20) noncommercial activity of: (A) a publisher, editor, reporter, or other person who is connected with or employed by a newspaper, magazine, periodical, newsletter, pamphlet, report, or other publication in general circulation; (B) a radio or television station that holds a license issued by the Federal Communications Commission; (C) a nonprofit organization that provides programming to radio or television networks; or (D) a press association or wire service.	(15) personal data collected, processed, sold, or disclosed in relation to price, route, or service, as such terms are used in the Federal Aviation Act of 1958, 49 U.S.C. § 40101 et seq., as may be amended, and the Airline Deregulation Act of 1978, 49 U.S.C.§ 41713, as may be amended.
§ 2418. CONSUMER PERSONAL DATA RIGHTS A consumer shall have the right to: know whether a consumer's personal data is or will be used in any artificial intelligence system and for what purpose; obtain from a controller a list of third parties to which the controller has disclosed the consumer's personal data or, if the controller does not maintain this information in a format specific to the consumer, a list of third parties to which the controller has disclosed personal data; (3)(A) Information provided in response to a consumer request shall be provided by a controller, free of charge, once per consumer during any 12-month period **or after every time the controller makes material changes to its personal data practices and policies.** (D) When a controller determines a consumer request is manifestly unfounded, excessive, or repetitive, the controller shall inform the consumer and share the controller's justification prior to disregarding	**§ 2418. CONSUMER RIGHTS; COMPLIANCE BY CONTROLLERS; APPEALS** A consumer shall have the right to: X X (3)(A) Information provided in response to a consumer request shall be provided by a controller, free of charge, once per consumer during any 12-month period. X

the request or charging the consumer a processing fee. That notice shall include instructions for appealing the decision. (5) A controller shall not condition the exercise of a right under this section through: (A) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or (B) the employment of any dark pattern.	(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete the data pursuant to subdivision (a)(3) of this section by: (A) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and not using the retained data for any other purpose pursuant to the provisions of this chapter; or (B) opting the consumer out of the processing of the personal data for any purpose except for those exempted pursuant to the provisions of this chapter.
(d) A controller shall establish a process by means of which a consumer may appeal the controller's refusal to take action on a request under subsection (b) of this section. The controller's process shall: (1) Allow a reasonable period of time after the consumer receives the controller's refusal within which to appeal. (2) Be conspicuously available to the consumer. (3) Be similar to the manner in which a consumer must submit a request under subsection (b) of this section. (4) Require the controller to approve or deny the appeal within 45 days after the date on which the controller received the appeal and to notify the consumer in writing of the controller's decision and the reasons for the decision. If the controller denies the appeal, the notice must provide or specify information that enables the consumer to contact the Attorney General to submit a complaint.	(d)(1) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. (2) The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. (3) Not later than 60 days after receipt of an appeal, a controller 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. (4) If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.
(f) In response to a consumer request under subdivision (a)(1) of this section, a controller shall not disclose the following information about a consumer, but shall instead inform the consumer with sufficient particularity that the controller has collected that type of information: (1) Social Security number; (2) driver's license number or other government-issued identification number; (3) financial account number; (4) health insurance account number or medical identification number; (5) account password, security questions, or answers; or (6) biometric data.	X

(g)(1) A controller may use the following types of information to display a contextual advertisement: (A) technical specifications as are necessary for the ad to be delivered and displayed properly on a given device; (B) a consumer's immediate presence in a geographic area with a radius not smaller than 10 miles, or an area reasonably estimated to include online activity from at least 5,000 users, but not including precise geolocation data; and (C) the consumer's language preferences, as inferred from context, browser settings, or user settings. (2) A controller using information pursuant to subdivision (1) of this subsection to display a contextual advertisement shall not use that information to make inferences about a consumer, profile a consumer, or for any other purpose, and the controller shall not prohibit a consumer from using technical means to obfuscate or change a consumer's physical location to specify a language preference.	X
The language in S.93 is mostly covered in 2418, above	§ 2419. AUTHORIZED AGENTS AND CONSUMER OPT-OUT
§ 2419. DUTIES OF CONTROLLERS (a) A controller shall: (1) limit the collection and processing of personal data to what is reasonably necessary and proportionate to provide or maintain: (A) a specific product or service requested by the consumer to whom the data pertains; and (B) a communication, that is not an advertisement, by the controller to the consumer that is reasonably anticipated within the context of the relationship between the controller and the consumer; (2) establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue, **including disposing of personal data in accordance with a retention schedule that requires the deletion of personal data when the data is required**	§ 2420. CONTROLLERS' DUTIES; SALE OF PERSONAL DATA TO THIRD PARTIES; NOTICE AND DISCLOSURE TO CONSUMERS; CONSUMER OPT-OUT (a) A controller: (1) shall limit the collection of personal data to what is **adequate, relevant,** and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer; X (3) shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue;

to be deleted by law or is no longer necessary for the purpose for which the data was collected or processed; and (b)(1) A controller that offers any online service, product, or feature to a consumer whom the controller knows is a minor shall: (A) use reasonable care to avoid any heightened risk of harm to minors caused by processing of personal data in the course of providing the online service, product, or feature; (B) provide to the minor a conspicuous signal indicating that the controller is collecting the minor's precise geolocation data and make the signal available to the minor for the entire duration of the collection of the minor's precise geolocation data; and (C) not process the personal data of a minor for the purposes of targeted advertising or sell the personal data of a minor. (c) A controller shall not: (1) process sensitive data concerning a consumer **except when the processing is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the sensitive data pertains;** (2) **sell sensitive data;**	X (minors are partially protected in (4), below) (4) shall not process sensitive data concerning a consumer without obtaining the consumer's consent or, in the case of the processing of sensitive data concerning a known child, without processing the data in accordance with COPPA;
§ 2420. DUTIES OF PROCESSORS (a) A processor shall adhere to a controller's instructions and shall assist the controller in meeting the controller's obligations under this chapter. In assisting the controller, the processor must: (2) adopt administrative, technical, and physical safeguards that are reasonably designed to protect the security and confidentiality of the personal data the processor processes, taking into account how the processor processes the personal data and the information available to the processor; and	§ 2421. PROCESSORS' DUTIES; CONTRACTS BETWEEN CONTROLLERS AND PROCESSORS (a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this chapter, including (2) taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and **in relation to the notification of a data broker security breach or security breach, as defined in section 2430 of this title, of the system of the processor, in order to meet the controller's obligations; and**

(b) Processing by a processor must be governed by a contract between the controller and the processor. The contract must:	(b)(1) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller.
X	(4) A processor shall provide a report of an assessment to the controller upon request.
(8)(A) allow the controller, the controller's designee, or a qualified and independent person the processor engages, in accordance with an appropriate and accepted control standard, framework, or procedure, to assess the processor's policies and technical and organizational measures for complying with the processor's obligations under this chapter; (B) require the processor to cooperate with the assessment; and (C) at the controller's request, report the results of the assessment to the controller; (9) prohibit the processor from combining personal data obtained from the controller with personal data that the processor: (A) receives from or on behalf of another controller or person; or (B) collects directly from an individual; and (10) require the processor to adhere to equivalent or greater de-identification standards.	X
(d)(1) For purposes of determining obligations under this chapter, a person is a controller with respect to processing a set of personal data and is subject to an action under section 2424 of this title to punish a violation of this chapter, if the person: (A) does not adhere to a controller's instructions to process the personal data; or (B) begins at any point to determine the purposes and means for processing the personal data, alone or in concert with another person. (2) A determination under this subsection is a fact-based determination that must take account of the context in which a set of personal data is processed. (3) A processor that adheres to a controller's instructions with respect to a specific processing of personal data remains a processor.	(d)(1) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. (2) A person who is not limited in the person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to the instructions, is a controller and not a processor with respect to a specific processing of data. (3) A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. (4) If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to the processing and may be subject to an enforcement action under section 2425 of this title.
§ 2421. DATA PROTECTION ASSESSMENTS FOR PROCESSING ACTIVITIES THAT PRESENT A HEIGHTENED RISK OF HARM TO A CONSUMER	§ 2422. CONTROLLERS' DATA PROTECTION ASSESSMENTS; DISCLOSURE TO ATTORNEY GENERAL

(f) A controller shall update the data protection assessment as often as appropriate considering the type, amount, and sensitivity of personal data collected or processed and level of risk presented by the processing throughout the processing activity's lifecycle in order to: (1) monitor for harm caused by the processing and adjust safeguards accordingly; and (2) ensure that data protection and privacy are considered as the controller makes new decisions with respect to the processing. (g) A controller shall retain for at least three years all data protection assessments the controller conducts under this section.	(f) Data protection assessment requirements shall apply to processing activities created or generated after July 1, 2025 and are not retroactive.
§ 2422. DE-IDENTIFIED DATA (a) A controller in possession of de-identified data shall: (1) take reasonable measures to ensure that the data cannot be used to reidentify an identified or identifiable individual **or be associated with an individual or device that identifies or is linked or reasonably linkable to an individual or household;** X X	§ 2423. DE-IDENTIFIED AND PSEUDONYMOUS DATA; CONTROLLERS' DUTIES; EXCEPTIONS; APPLICABILITY OF CONSUMERS' RIGHTS; DISCLOSURE AND OVERSIGHT (a) A controller in possession of de-identified data shall: (1) take reasonable measures to ensure that the data cannot be associated with an individual; (c) This chapter shall not be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller: (3) does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section. (d) The rights afforded under subdivisions 2418(a)(1)–(4) of this title shall not apply to pseudonymous data in cases where the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.
§ 2423. CONSTRUCTION OF DUTIES OF CONTROLLERS AND PROCESSORS (a) This chapter shall not be construed to restrict a controller's, processor's, or consumer health data controller's ability to:	§ 2424. CONSTRUCTION OF CONTROLLERS' AND PROCESSORS' DUTIES (a) This chapter shall not be construed to restrict a controller's, processor's, or consumer health data controller's ability to:

(4) carry out obligations under a contract under subsection 2420(b) of this title for a federal or State agency or local unit of government;	X
(15) process personal data previously collected in accordance with this chapter such that the personal data becomes de-identified data, including to: (A) conduct internal research to develop, improve, or repair products, services, or technology; (B) identify and repair technical errors that impair existing or intended functionality; (C) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party; or (D) conduct a public or peer-reviewed scientific, historical, or statistical research project that is in the public interest and adheres to all relevant laws and regulations governing such research, including regulations for the protection of human subjects.	(10) engage in public or peer-reviewed scientific 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 that determines, or similar independent oversight entities that determine: (A) whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller; (B) the expected benefits of the research outweigh the privacy risks; and (C) whether the controller or consumer health data controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;
X	(b) The obligations imposed on controllers, processors, or consumer health data controllers under this chapter shall not restrict a controller's, processor's, or consumer health data controller's ability to collect, use, or retain data for internal use to: (1) conduct internal research to develop, improve, or repair products, services, or technology; (2) effectuate a product recall; (3) identify and repair technical errors that impair existing or intended functionality; or (4) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or consumer health data controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.
(b) (3) Nothing in this chapter modifies 2020 Acts and Resolves No. 166, Sec. 14 or authorizes the use of facial recognition technology by law enforcement.	
(d) This chapter shall not be construed to:	

(4) require, for employee data, deletion of personal data that would unreasonably interfere with the ordinary business operations of the controller or unreasonably adversely affect the rights of another employee, including under this chapter or pursuant to the protections set forth in 21 V.S.A chapter 5; or (5) require, for processors acting on the behalf of a federal, State, tribal, or local government entity, deletion of personal data or opt out of the processing of personal data that would unreasonably interfere with the provision of government services by or the ordinary operation of a government entity.	X
(e)(1) Personal data processed by a controller or consumer health data controller pursuant to this section may be processed to the extent that the processing is: (A)(i) reasonably necessary and proportionate to the purposes listed in this section; or (ii) **in the case of sensitive data, strictly necessary to the purposes listed in this section;** (B) adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section; and (C) **compliant with the antidiscrimination provisions set forth in subdivision 2419(c)(5) of this title.**	(f)(1) Personal data processed by a controller or consumer health data controller pursuant to this section may be processed to the extent that the processing is: (A) reasonably necessary and proportionate to the purposes listed in this section; and (B) adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section.
(g) This chapter shall not be construed to require a controller, processor, or consumer health data controller to implement an age-verification or age-gating system or otherwise affirmatively collect the age of consumers.	(h) Processing personal data for the purposes expressly identified in this section shall not solely make a legal entity a controller or consumer health data controller with respect to the processing.
§ 2424. ENFORCEMENT; ATTORNEY GENERAL'S POWERS	§ 2425. ENFORCEMENT BY ATTORNEY GENERAL; NOTICE OF VIOLATION; CURE PERIOD; REPORT; PENALTY
AG has enforcement except for a PRA in limited circumstances:	AG has sole enforcement; no PRA
against a data broker or large data holder's violation of (1) selling the sensitive data of consumers, (2) processing consumers sensitive data without consent, or (3) consumer health data protections. Otherwise, AG may offer a 60 day cure period before commencing civil action.	Before Jan 1, 2027, AG must issue a notice of violation before commencing civil action; after that date, cure period is optional for AG

§ 2425. CONFIDENTIALITY OF CONSUMER HEALTH DATA	§ 2426. CONSUMER HEALTH DATA PRIVACY
Except as provided in subsections 2417(a) and (b) of this title and section 2423 of this title, no person shall:	(a) Except as provided in subsections (b) and (c) of this section and subsections 2417(b) and (c) of this title, no person shall:
X	(4) sell, or offer to sell, consumer health data without first obtaining the consumer's consent.
X	(b) Notwithstanding section 2416 of this title, subsection (a) of this section, and the provisions of sections 2415–2425 of this title, inclusive, concerning consumer health data and consumer health data controllers, apply to persons that conduct business in this state and persons that produce products or services that are targeted to residents of this state. (c) Subsection (a) of this section shall not apply to any: (1) body, authority, board, bureau, commission, district or agency of this State or of any political subdivision of this State; (2) person who has entered into a contract with an entity described in subdivision (1) of this subsection to process consumer health data on behalf of the entity; (3) institution of higher education; (4) national securities association that is registered under 15 U.S.C. 78o-3 of the Securities Exchange Act of 1934, as may be amended; (5) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, and regulations adopted to implement that act; (6) covered entity or business associate, as defined in 45 C.F.R. § 160.103; (7) tribal nation government organization; or (8) air carrier, as: (A) defined in 49 U.S.C. § 40102, as may be amended; and (B) regulated under the Federal Aviation Act of 1958, 49 U.S.C. § 40101 et seq. and the Airline Deregulation Act of 1978, 49 U.S.C. § 41713, as may be amended.