	SB 370 (Nevada)	My Health My Data Act (Washington)	Amendments to SB 3 (Connecticut)
Effective Date	March 31, 2024	The majority of obligations will be effective as of March 31, 2024 (June 30, 2024 for small businesses). Restrictions related to geofencing took effect on July 23, 2023.	July 1, 2023 (July 1, 2023 for the Connecticut Data Privacy Act)
Scope	The law imposes obligations on a "Regulated Entity," which is any person who: • Conducts business in Nevada or produces or provides products or services that are targeted to consumers in Nevada and • Alone or with other persons, determines the purpose and means of processing, sharing, or selling consumer health data.	The law imposes obligations on "regulated entities," "small businesses," and processors that process consumer health data on their behalf. Regulated entities are those that conduct business in Washington or produce or provide products or services that are targeted to consumers in Washington and that determine the purposes and means of processing consumer health data. "Small business" means a regulated entity that satisfies one or both of the following thresholds: • Collects, processes, sells, or shares consumer health data of fewer than 100,000 consumers during a calendar year; or • Derives less than 50 percent 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 25,000 consumers.	The law regulates a "consumer health data controller," which is defined as any controller that, alone or jointly with others, determines the purpose and means of processing consumer health data.
"Consumer	means a natural person who has requested a product or service from a regulated entity and who resides in this State or whose	means (a) a natural person who is a Washington resident; or (b) a natural person whose consumer health data is collected in Washington. "Consumer" means a natural	means an individual who is a resident of Connecticut

	consumer health data is collected in Nevada	person who acts only in an individual or household context, however identified, including by any unique identifier. "Consumer" does not include an individual acting in an employment context	Consumer does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within that context.
Definition of "Consumer Health Data"	The law applies to all "consumer health data," which is defined as "personally identifiable information that is linked or reasonably capable of being linked to a consumer and that a Regulated Entity **uses** to identify the past, present, or future health status of the consumer." This includes information relating to: • Any health condition or status, disease, or diagnosis. • Social, psychological, behavioral, or medical interventions. • Surgeries or other health-related procedures. • The use or acquisition of medication. • Bodily functions, vital signs, or symptoms. • Reproductive or sexual health care. • Gender-affirming care. • Biometric data or genetic data related to information described above. • Information related to the precise geolocation information of a consumer that a Regulated Entity uses to indicate an attempt by a	The law applies to "consumer health data," which is defined as "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." Examples of "physical or mental health status" include, but are not limited to: • Individual health conditions, treatment, diseases, or diagnosis. • Social, psychological, behavioral, and medical interventions. • Health-related surgeries or procedures. • Use or purchase of prescribed medication. • Bodily functions, vital signs, symptoms, or measurements. • Diagnoses or diagnostic testing, treatment, or medication. • Gender-affirming care information and reproductive or sexual health information. • Biometric data (data that is generated from the measurement or technological processing of an individual's physiological, biological, or behavioral characteristics that identifies a consumer and specifically includes imagery of the face and voice recordings from which an	"Consumer health data" means any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data.

	consumer to receive health care services or products. • Any information described above that is derived or extrapolated from information that is not consumer health data, including proxy, derivative, inferred, or emergent data derived through an algorithm, machine learning, or any other means. Exclude information related to : • Provide access to or enable gameplay by a person on a video game platform; or • Identify the shopping habits or interests of a consumer, if that information is not used to identify the specific past, present or future health status of the consumer	identifier template can be extracted, among other things). • Genetic data (any data that concerns a consumer's genetic characteristics). • Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies. • Data that identifies a consumer seeking "healthcare services" (any service provided to "assess, measure, improve, or learn about a person's mental or physical health" and includes, among other things, use or purchase of medication). • Any information that a regulated entity or small business, or their respective processor, processes to associate or identify a consumer with the data described above that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).	
Definition of Geofencing	"Geofence" means technology that uses coordinates for global positioning, connectivity to cellular towers, cellular data, radio frequency identification, wireless Internet data or any other form of detecting the physical location of a person to establish a virtual boundary with a radius of 1,750 feet or less around a specific physical location.	"Geofence" is defined to include technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wi-Fi data, and/or any other form of location detection to establish a virtual boundary around a specific physical location. For purposes of the Act, "geofence" means a virtual boundary that is 2,000 feet or less from the perimeter of the physical location.	"Geofence" means any technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, wireless fidelity technology data or any other form of location detection, or any combination of such coordinates, connectivity, data, identification or other form of location detection, to establish a virtual boundary. Controller is prohibited from establishing a geofence with 1,750 feet of any mental

			health facility, reproductive or sexual health facility for the purpose of identifying, tracking, or collecting data from or sending any notification to a consumer concerning their consumer health data.
Consent	The law requires the "**affirmative**, voluntary consent" of the consumer.	Defined as a clear affirmative act that signifies a consumer's freely given, specific, informed, **opt-in**, voluntary, and unambiguous agreement. Such consent may not be obtained by: • a consumer's acceptance of a general terms • a consumer hovering over or closing any content or • a consumer's agreement obtained through the use of deceptive designs.	Defined as a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, or any other unambiguous **affirmative** action. It does not include: • acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information, • hovering over, muting, pausing or closing a given piece of content, or • agreement obtained through the use of dark patterns.
Consumer Rights	Upon request, Regulated Entities must: • Confirm whether the Regulated Entity collects, shares, or sells consumer health data concerning the consumer. • Provide the consumer with a list of third parties with whom the Regulated Entity has shared or to whom the Regulated Entity has sold consumer health data relating to the consumer.	• To confirm whether a regulated entity is collecting, sharing, or selling consumer health data and to access such data (including a list of all third parties and affiliates with whom the regulated entity has shared or sold the consumer health data and an active email address or other online mechanism for contacting these third parties); • To withdraw consent;	Consumers have the right to • Confirm whether a controller is processing a consumer's personal data and has access to such personal data, unless the access would reveal a trade secret • Correct inaccuracies in the consumer's personal data • Delete personal data • Obtain a copy of the consumer's personal data

	• Cease collecting, sharing, or selling consumer health data relating to the consumer. • Delete consumer health data concerning the consumer.	• To request deletion of their consumer health data, including information shared or processed by affiliates, processors, contractors, or other third parties, as well as archived or backup systems.	
Processor Obligations/Contract Requirements	Processors may only process consumer health data pursuant to a contract between the processor and a Regulated Entity. Regulated Entity prohibited from entering into a contract that is inconsistent with its Policy concerning consumer health data. A person is prohibited from selling or offering to sell consumer health data without the written authorization of the consumer to whom the data pertains or if the consumer provides such authorization, a person may not sell or offer to sell in a manner outside the scope of or inconsistent with the written authorization.	A processor may only process consumer health data pursuant to a binding contract with a regulated entity or a small business that includes required security and privacy provisions, including limiting the actions the processor may take with respect to the consumer health data.	The law prohibits providing any processor with access to consumer health data unless that processor complies with CTDPA obligations on processors, such as the obligation to help controllers meet their obligations under CTDPA, notify controllers of data breaches, and have a written contract that governs the processor's data processing activities. The law prohibits selling or offering to sell consumer health data without first obtaining the consumer's consent.
Definition of "Sale"	"Sell" means to exchange consumer health data for money or other valuable consideration and does **not include** the exchange of consumer health data for money or other valuable consideration with: • A processor in a manner consistent with the purpose for which the consumer health data was collected, as disclosed to the consumer to whom the consumer health data pertains pursuant to section 22 of the act;	"Sale" or "Sell" means the exchange of consumer health data for monetary or other valuation consideration and does not include exchange of consumer health data for monetary or other valuable consideration: • 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 party of the regulated entity or small business's assets that complies with the requirements and obligations in this chapter; or	Sale means the exchange of personal data for monetary or other valuable consideration by the controller to a third party and it does not include: • The disclosure of personal data to a processor that processes the personal data on behalf of the controller; • The disclosure of personal data to a third party for purposes providing a product or service requested by the consumer;

	• A third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction through which the third party assumes control of all or part of the assets of the regulated entity; • a third party for the purpose of providing a product or service requested by the consumer to whom the consumer health data pertains; • An affiliate of the person who is providing or disclosing the consumer health data; • The consumer to whom the consumer health data pertains as directed or where the consumer to whom the consumer health data pertains intentionally uses the person who is providing or disclosing the consumer health data to interact with the third party to whom the consumer health data is provided or disclosed; or • the consumer who has intentionally made the consumer health data available to the general public through mass media that was not restricted to a specific audience.	• 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 disclosed to the consumer.	• The disclosure or transfer of personal data to an affiliate of the controller; • The disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally used the controller to interact with a third party; • The disclosure of personal data that the consumer intentionally made available to the general public via channel of mass media and did not restrict to a specific audience; or • The disclosure or transfer of personal data to a third party as an asset as a party of a merger, acquisition, bankruptcy, or other transaction, in which the third party assumes control of all or party of the controller's assets.
Other Business Obligations	The law requires Regulated Entities to develop and maintain a policy concerning the privacy of consumer health data that clearly and conspicuously states: • Categories of consumer health data being collected by the Regulated	The law requires companies to maintain a "consumer health privacy policy" which must include: • the categories of consumer health data collected and the purposes for which	The law requires controllers to: • Conduct a data protection assessment for processing activities that present a "heightened risk of harm to a

	Entity and the manner in which the consumer health data will be used. • Categories of sources from which consumer health data is collected. • Categories of consumer health data that are shared by the Regulated Entity. • Categories of consumer health data that are shared by the Regulated Entity. • Categories of third parties and affiliates with whom the Regulated Entity shares consumer health data. • The purposes of collecting, using, and sharing consumer health data. • The manner in which consumer health data will be processed. • How consumers can exercise the rights granted under the law. • The process, if any, for a consumer to review and request changes to any of their consumer health data that is collected by the Regulated Entity. • The process by which the Regulated Entity will notify consumers of material changes to the privacy policy. • Whether a third party may collect consumer health data over time and across different websites or online services when the consumer uses any website or online service of the Regulated Entity.	the data is collected, including how it will be used; • the categories of sources from which the consumer health data is collected; • the categories of consumer health data that is shared; • a list of the categories of third parties and specific affiliates with whom the Covered Entity shares consumer health data; and • how consumers can exercise the right granted under the Act. A regulated entity and a small business should: • prominently publish a link to its consumer health data privacy policy on its homepage; • restrict access to consumer health data to employees, processors or contractors necessary to further the purposes for which the consumer provided consent or where necessary to provide a product or service the consumer has requested; • implement administrative, technical and physical data security practices to satisfy a reasonable standard of care within the industry to protect consumer health data based on the volume and nature of data at issue.	consumer," including processing sensitive data. • Obtain consent from the consumer before processing consumer health data. • Not provide an employee or contractor with access to consumer heald data unless they are subject to a contractual or statutory duty of confidentiality

	• The effective date of the privacy policy. • A Regulated Entity must post the notice on its website or otherwise provide the policy to consumers in a manner that is clear and conspicuous. List of all Third parties Ensure that only employees and processors with a "need to know" the consumer's health data have access Establish and implement policies and procedures for the administrative, technical, and physical security of consumer health data.		
Exceptions	The law exempts certain information, including: • information governed by FCRA, FERPA, processed by any governmental entity, or information that is collected or shared as expressly authorized by a provision of federal or state law; and • deidentified data.	The law does not apply to: • information regulated under other sectoral privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Federal Education Rights and Privacy Act (FERPA), and the Fair Credit Reporting Act (FCRA), in addition to various Washington state laws; • information in public or peer-reviewed scientific, historical, or statistical research in the public interest; • publicly available information; and • de-identified data.	The law provides exemptions for: • Connecticut's state and local government agencies, • entities contracting with government agencies, • institutions of higher education, and • entities governed by the GLBA, HIPAA and other federal laws.

Enforcement	Except in narrow circumstances applicable to processors (Section 29) and entities such as consumer reporting agencies (Section 34), violations constitute a deceptive trade practice under the Nevada Consumer Protection Act. The attorney general may seek injunctive relief and monetary damages for violations of the law.	Violation of the law is an unfair or deceptive trade practice, and is an unfair method of competition under the Washington Consumer Protection Act. Both the attorney general and private plaintiffs may enforce the law through an action under the Washington Consumer Protection Act.	The Connecticut Attorney General has the exclusive enforcement authority.