SENATE DOCKET, NO. 1696 FILED ON: 1/16/2025

SENATE . . . . . No.

The Commonwealth of Massachusetts

PRESENTED BY:

Robyn K. Kennedy

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act relative to consumer health data.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
Robyn K. Kennedy	*First Worcester*

SENATE DOCKET, NO. 1696 FILED ON: 1/16/2025

SENATE . . . . . No.

[Pin Slip]

[SIMILAR MATTER FILED IN PREVIOUS SESSION
SEE SENATE, NO. *184* OF 2023-2024.]

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Fourth General Court
(2025-2026)

An Act relative to consumer health data.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. The General Laws, as appearing in the 2018 Official Edition, are hereby amended by inserting after chapter 93M the following chapter:

Chapter 93M. Consumer Health Data Act

Section 1. Definitions

As used in this chapter, the following words shall, unless the context clearly requires otherwise, have the following meanings:—

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

(a) Ownership of, or the power to vote, more than fifty 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.

"Biometric data," means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that a Regulated Entity uses to identify a specific individual.

"Biometric data" does not include a physical or digital photograph or a video or audio recording. or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996 and its implementing regulations.

"Collect," to buy, rent, access, retain, receive, or acquire Consumer Health Data in any manner.

"Consent," a clear affirmative act by a consumer that openly communicates a consumer's freely given, informed, opt-in, voluntary, specific, and unambiguous agreement (which may include written consent provided by electronic means). Consent cannot 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,

"Consumer," a natural person who is a Massachusetts resident acting only in an individual or household context, however identified, including by any unique identifier. A person that a Regulated Entity knows to be located in Massachusetts when their Consumer Health Data is collected by such Regulated Entity will create a presumption that the person is a Massachusetts resident for purposes of enforcing this chapter.

"Consumer Health Data," personal information a Regulated Entity uses to identify the past, present, or future physical or mental health of a consumer, including any personal information relating to:

(i) Individual health conditions, treatment, status, diseases, or diagnoses;

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

(iii) Health related surgeries or procedures;

(iv) Use or purchase of medication;

(v) Bodily functions, vital signs, measurements, or symptoms;

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

(vii) Efforts to research or obtain health services or supplies;

(viii) Precise location information that a Regulated Entity uses to determine a consumer's primary purpose to acquire or receive health services or supplies; and

(ix) Any information described in subparagraphs (i) through (ix) that is derived or extrapolated from non-health information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).

(b) Consumer Health Data does not include:

(i) Data processed or maintained in the course of employment, including applications for employment and the administration of benefits; or

(ii) 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 has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification, so long as consent has first been obtained;

"Deceptive design," a user interface knowingly designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.

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

"Personal Information," information that identifies, is reasonably capable of being associated with, or linked, with a particular consumer. Personal information does not include

publicly available information or de-identified data. For purposes of this paragraph, "publicly available information" means information that has been lawfully made available from federal, state, or local government records, that a controller has a reasonable basis to believe is widely available to the general public, or is a disclosure to the general public that is required to be made by federal, state, or local law. For purposes of this paragraph, "de-identified" data means data that cannot be reasonably linked to, a particular consumer, or a device linked to such consumer, if the Regulated Entity that that possesses such data (A) takes reasonable measures to ensure that such data cannot be associated with a consumer, (B) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and (C) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision.

"Precise Location Information," information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet. "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.

"Regulated Entity," any legal entity that (a) conducts business in Massachusetts or produces products or services that are targeted to consumers in Massachusetts and (b) collects, shares, or sells Consumer Health Data. Regulated Entity does not mean government agencies, tribal nations, or an individual acting in a non-commercial manner.

"Sell" or "Sale," the sharing of Consumer Health Data for monetary or other valuable consideration to a Third Party. Sell or Sale does not include the sharing of Consumer Health Data for monetary or other valuable consideration to:

(i) 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 assets that shall comply with the requirements and obligations in this chapter;

(ii) A Third Party at the direction of a consumer; or

(iii) A Third Party where the Regulated Entity maintains control and ownership of the Consumer Health Data, and the third-party only uses the Consumer Health Data at direction from the Regulated Entity and consistent with the purpose for which it was collected and disclosed to the consumer.

"Share" or "Sharing," 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 to a Third Party where the Regulated Entity maintains control and ownership of the Consumer Health Data. The term share or sharing does not include:

(i) The disclosure of Consumer Health Data to an entity who collects and/or processes the personal data on behalf of the Regulated Entity, when the Regulated Entity maintains control and ownership of the data and the Third Party only uses the Consumer Health Data at direction from the Regulated Entity and consistent with the purpose for which it was collected and disclosed to the consumer;

(ii) The disclosure of Consumer Health Data to a Third Party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer when the Regulated Entity maintains control and ownership of the data and the Third Party only uses the Consumer Health Data at direction from the Regulated Entity and consistent with the purpose for which it was collected and disclosed to 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 assets and shall comply with the requirements and obligations in this chapter.

"Third Party," any legal entity other than a consumer, Regulated Entity, or an affiliate of the Regulated Entity.

Section 2. Consumer Health Data Privacy Policy.

(1) A Regulated Entity shall maintain a Consumer Health Data Privacy Policy that clearly and conspicuously discloses:

(a) The specific types of Consumer Health Data collected and the purpose for which the data is collected, including the specific ways in which it will be used;

(b) The specific sources from which the Consumer Health Data is collected;

(c) The specific Consumer Health Data that is shared;

(d) A list of specific Third Parties with whom the Regulated Entity shares the Consumer Health Data, including an active electronic mail address or other online mechanism that the consumer may use to contact these third parties and affiliates; and

(e) How a consumer can exercise the rights provided in Section 6.

(2) A Regulated Entity shall prominently publish or link to its Consumer Health Privacy Policy on its homepage, or in another manner that is clear and conspicuous to consumers.

(3) A Regulated Entity shall not collect 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 consent prior to the collection or sharing of such Consumer Health Data.

(4) A Regulated Entity shall not collect 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 consent prior to the collection or sharing of such Consumer Health Data.

Section 3. Consent to Collect and Share Consumer Health Data.

(1) A Regulated Entity shall not collect any Consumer Health Data except:

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

(b) To the extent strictly necessary to provide a product or service that the consumer to whom such Consumer Health Data relates has requested from such Regulated Entity.

(2) A Regulated Entity shall not share any Consumer Health Data except:

(a) With consent from the consumer for such sharing that is separate and distinct from the consent obtained to collect Consumer Health Data; or

(b) To the extent strictly necessary to provide a product or service that the consumer to whom such Consumer Health Data relates has requested from such Regulated Entity.

(3) Consent required under this section must 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:

(a) the categories of Consumer Health Data collected or shared,

(b) the purpose of the collection or sharing of the Consumer Health Data, including the specific ways in which it will be used, and

(c) how the consumer can withdraw consent from future collection or sharing of their Consumer Health Data.

(4) Consent required under this section must be obtained prior to the use of any Consumer Health Data for any purpose not reasonably aligned with a consumer's consent for the use of such Consumer Health Data.

(5) A Regulated Entity shall not discriminate against a consumer for exercising any rights included in this chapter.

Section 4. Consumer Health Data Rights.

(1) A consumer has the right to know whether a Regulated Entity is collecting or sharing their Consumer Health Data.

(2) A consumer has the right to withdraw consent from the Regulated Entity's collection and sharing of their Consumer Health Data.

(3) A consumer has the right to have their Consumer Health Data deleted by informing the Regulated Entity of their request for deletion.

(a) A Regulated Entity that receives a consumer's request to delete any of their Consumer Health Data shall without unreasonable delay and no more than forty-five calendar days from receiving the deletion request:

(i) Delete the Consumer Health Data from its records, including from all parts of the Regulated Entity's network; and

(ii) Notify all affiliates, service providers, contractors, and Third Parties with whom the Regulated Entity has shared Consumer Health Data of the deletion request.

(b) If a regulated entity stores any health data on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to the health data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used.

(c) All affiliates, service providers, contractors, and 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, including from all parts of its network.

(4) (a) A consumer or a consumer's authorized agent may exercise the rights set forth in this chapter by contacting the Regulated Entity through the manner included in its Consumer Health Privacy policy; or

(b) In the case of collecting Consumer Health Data concerning a consumer subject to guardianship, conservatorship, or other protective arrangement under the Consumer Protection

Act, the guardian or the conservator of the consumer may exercise the rights of this chapter on the consumer's behalf.

(5) A Regulated Entity shall not be required to comply with a consumer's request to delete the consumer's health data if it is necessary for the Regulated Entity to maintain the consumer's Consumer Health Data to:

(a) Complete the transaction for which the Consumer Health Data was collected, provide a good or service requested by the consumer, or otherwise fulfill the requirements of an agreement between the Regulated Entity and the consumer;

(b) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, provided that the use of Consumer Health Data for such purposes is limited. In time;

(c) 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, when the Regulated Entity's deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided consent to such use of their Consumer Health Data;

(d) Comply with to comply with an applicable legal obligation; or

(e) Otherwise use the consumer's Consumer Health Data, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

Section 5. Consumer Health Data Security and Minimization.

(1) A Regulated Entity shall restrict access to Consumer Health Data by the employees, service providers, and contractors of such Regulated Entity to only those employees, services

providers, and contractors for which access is necessary to provide a product or service that the consumer to whom such data and information relates has requested from such Regulated Entity.

(2) A Regulated Entity shall establish, implement and maintain administrative, technical and physical data security practices that at least satisfy reasonable standard of care within the Regulated Entity's industry to protect the confidentiality, integrity and accessibility of Consumer Health Data appropriate to the volume and nature of the personal data at issue.

(3) A Regulated Entity shall document the measures used to ensure compliance.

Section 6. Unlawful to Sell Consumer Health Data.

(1) It shall be unlawful for a Regulated Entity to sell Consumer Health Data concerning 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.

(2) A valid authorization to sell Consumer Health Data is an agreement consistent with this section and must be written in plain language. The valid authorization to sell Consumer Health Data must contain the following:

(a) The specific Consumer Health Data concerning the consumer that the person intends to sell;

(b) The name and contact information of any person(s) or entity collecting and selling the Consumer Health Data;

(c) The name and contact information of any person(s) or entity purchasing the Consumer Health Data from the seller identified in (b) of this subsection;

(d) 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 (c) of this subsection when sold;

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

(f) A statement that the consumer has a right to revoke the valid authorization at any time and a description on how a. consumer may revoke the valid authorization; and

(g) 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.

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

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

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

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

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

(4) A copy of the signed valid authorization must be provided to the consumer.

(5) The seller and purchaser of Consumer Health Data must retain a copy of all valid authorizations for 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.

Section 7. Enforcement - Consumer Protection Act.

(1) The legislature finds that the practices covered by this chapter are matters vitally affecting the public interest for the purpose of applying the Consumer Protection Act. A violation of this chapter is not reasonable in relation to the development and preservation of business, and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the Consumer Protection Act.

(2) The Attorney General shall have exclusive authority to enforce the provisions of this chapter.

(3) Nothing in this chapter shall be construed as providing the basis for, or be subject to, a private right of action for violations of said sections or any other law.

(4) Prior to initiating any action for a violation of any provision of this chapter, the Attorney General shall provide a Regulated Entity forty-five days' written notice identifying the specific provisions of this chapter the Attorney General alleges have been or are being violated. If within the forty-five day period the Regulated Entity cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured, no action shall be initiated against the Regulated Entity.

Section 8. Exemptions.

(1) This chapter does not apply to protected health information collected, used, or disclosed by covered entities and business associates when the protected health information is collected, used, or disclosed in accordance with the federal health insurance portability and accountability act of 1996 and its implementing regulations and afforded all the privacy

protections and security safeguards of that federal law. For the purpose of this subsection (1), "protected health information," "covered entity," and "business associate" have the same meaning as in the federal health insurance portability and accountability act of 1996 and its implementing regulations.

(2) Nothing in this chapter shall be construed to prohibit disclosure as required by law.

(3) If any provision of this chapter, or the application thereof to any person or circumstance, is held invalid, the remainder of this chapter and the application of such provision to other persons not similarly situated or to other circumstances shall not be affected by the invalidation.