HOUSE DOCKET, NO. 3855 FILED ON: 1/20/2023

HOUSE . . . . . No. 386

The Commonwealth of Massachusetts

PRESENTED BY:

Lindsay N. Sabadosa and Steven Owens

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:	DATE ADDED:
Lindsay N. Sabadosa	*1st Hampshire*	*1/20/2023*
Steven Owens	*29th Middlesex*	*1/20/2023*
Carmine Lawrence Gentile	*13th Middlesex*	*1/25/2023*
James K. Hawkins	*2nd Bristol*	*1/27/2023*

HOUSE DOCKET, NO. 3855 FILED ON: 1/20/2023

HOUSE . . . . . No. 386

By Representatives Sabadosa of Northampton and Owens of Watertown, a petition (accompanied by bill, House, No. 386) of Lindsay N. Sabadosa, Steven Owens and others relative to consumer health data. Consumer Protection and Professional Licensure.

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Third General Court
(2023-2024)

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," an individual's physiological, biological, or behavioral characteristics that can be used individually or in combination with other data to identify a consumer. Biometric data includes:

(a) An individual's deoxyribonucleic acid (DNA);

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

(c) Keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

"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 written consent (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, including by the use of pre-checked or pre-selected options.

"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 located in Massachusetts when their Consumer Health Data is collected by a Regulated Entity will create a presumption that the person is a Massachusetts resident for purposes of enforcing this chapter.

"Consumer Health Data," personal information relating to 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) Location information that could reasonably indicate a consumer's attempt 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 designed or manipulated with the potential effect of subverting or impairing user autonomy, decision making, or choice.

"Homepage," the introductory page of an internet website and any internet web page 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, relates to, describes, is reasonably capable of being associated with, or linked, directly or indirectly, with a particular consumer. Personal information does not include publicly available information. For purposes of this paragraph, “publicly available” means information that is lawfully made available from federal, state, or local government records. Any biometric data collected about a consumer by a business without the consumer's knowledge is not publicly available information.

“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. 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/or 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.

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 and affiliates 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 its Consumer Health Privacy Policy on its homepage.

(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 affirmative 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 affirmative 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) A Regulated Entity shall not discriminate against a consumer for exercising any rights included in this chapter including by means of a) refusing to do business with the consumer, b) charging a higher price to the consumer or c) providing a lower quality product or service to the consumer.

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 thirty 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 or backup systems; and

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

(b) All affiliates, service providers, contractors, 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, including from all parts of its network or backup systems.

(4) A consumer or a consumer's authorized agent may exercise the rights set forth in this chapter by submitting a request, at any time, to a Regulated Entity. Such a request may be made:

(a) By contacting the Regulated Entity through the manner included in its Consumer Health Privacy policy;

(b) By designating an authorized agent who may exercise the rights on behalf of the consumer; or

(c) 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.

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 and shall make this documentation publicly available.

Section 6. Unlawful to Sell Consumer Health Data.

It shall be unlawful for a Regulated Entity to sell Consumer Health Data.

Section 7. Enforcement - Consumer Protection Act.

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.

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.