

HOUSE No.

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:
<i>Lindsay N. Sabadosa</i>	<i>1st Hampshire</i>	<i>1/12/2025</i>
<i>Steven Owens</i>	<i>29th Middlesex</i>	<i>1/12/2025</i>

HOUSE No.

[Pin Slip]

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:

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

3 Chapter 93M. Consumer Health Data Act

4 Section 1. Definitions

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

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

10 (a) Ownership of, or the power to vote, more than fifty percent of the outstanding shares
11 of any class of voting security of a company;

12 (b) Control in any manner over the election of a majority of the directors or of individuals
13 exercising similar functions; or

14 (c) The power to exercise controlling influence over the management of a company.

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

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

22 “Collect,” to buy, rent, access, retain, receive, or acquire Consumer Health Data in any
23 manner.

24 “Consent,” a clear affirmative act by a consumer that openly communicates a consumer’s
25 freely given, informed, opt-in, voluntary, specific, and unambiguous agreement (which may
26 include written consent provided by electronic means). Consent cannot be obtained by:

27 (i) A consumer’s acceptance of a general or broad Terms of Use agreement or a similar
28 document that contains descriptions of personal data processing along with other, unrelated
29 information;

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

31 (iii) A consumer’s agreement obtained through the use of deceptive designs,

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

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

- 40 (i) Individual health conditions, treatment, status, diseases, or diagnoses;
- 41 (ii) Social, psychological, behavioral, and medical interventions;
- 42 (iii) Health related surgeries or procedures;
- 43 (iv) Use or purchase of medication;
- 44 (v) Bodily functions, vital signs, measurements, or symptoms;
- 45 (vi) Diagnoses or diagnostic testing, treatment, or medication;
- 46 (vii) Efforts to research or obtain health services or supplies;
- 47 (viii) Precise location information that a Regulated Entity uses to determine a consumer’s
48 primary purpose to acquire or receive health services or supplies; and
- 49 (ix) Any information described in subparagraphs (i) through (ix) that is derived or
50 extrapolated from non-health information (such as proxy, derivative, inferred, or emergent data
51 by any means, including algorithms or machine learning).

52 (b) Consumer Health Data does not include:

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

55 (ii) Personal Information that is used to engage in public or peer-reviewed scientific,
56 historical, or statistical research in the public interest that adheres to all other applicable ethics
57 and privacy laws and is approved, monitored, and governed by an institutional review board,
58 human subjects research ethics review board, or a similar independent oversight entity that
59 determines that the Regulated Entity has implemented reasonable safeguards to mitigate privacy
60 risks associated with research, including any risks associated with reidentification, so long as
61 consent has first been obtained;

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

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

68 “Personal Information,” information that identifies, is reasonably capable of being
69 associated with, or linked, with a particular consumer. Personal information does not include
70 publicly available information or de-identified data. For purposes of this paragraph, “publicly
71 available information” means information that has been lawfully made available from federal,
72 state, or local government records, that a controller has a reasonable basis to believe is widely
73 available to the general public, or is a disclosure to the general public that is required to be made

74 by federal, state, or local law. For purposes of this paragraph, “de-identified” data means data
75 that cannot be reasonably linked to, a particular consumer, or a device linked to such consumer,
76 if the Regulated Entity that that possesses such data (A) takes reasonable measures to ensure that
77 such data cannot be associated with a consumer, (B) publicly commits to process such data only
78 in a de-identified fashion and not attempt to re-identify such data, and (C) contractually obligates
79 any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this
80 subdivision.

81 “Precise Location Information,” information derived from technology, including but not
82 limited to global positioning system level latitude and longitude coordinates or other
83 mechanisms, that directly identifies the specific location of an individual with precision and
84 accuracy within a radius of one thousand seven hundred fifty feet. “Precise Location
85 Information” does not include the content of communications or any data generated by or
86 connected to advanced utility metering infrastructure systems or equipment for use by a utility.

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

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

94 (i) A Third Party as an asset that is part of a merger, acquisition, bankruptcy, or other
95 transaction in which the Third Party assumes control of all or part of the Regulated Entity's
96 assets that shall comply with the requirements and obligations in this chapter;

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

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

102 "Share" or "Sharing," to release, disclose, disseminate, divulge, make available, provide
103 access to, license, or otherwise communicate orally, in writing, or by electronic or other means,
104 Consumer Health Data by a Regulated Entity to a Third Party where the Regulated Entity
105 maintains control and ownership of the Consumer Health Data. The term share or sharing does
106 not include:

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

112 (ii) The disclosure of Consumer Health Data to a Third Party with whom the consumer
113 has a direct relationship for purposes of providing a product or service requested by the
114 consumer when the Regulated Entity maintains control and ownership of the data and the Third

115 Party only uses the Consumer Health Data at direction from the Regulated Entity and consistent
116 with the purpose for which it was collected and disclosed to the consumer; or

117 (iii) The disclosure or transfer of personal data to a Third Party as an asset that is part of a
118 merger, acquisition, bankruptcy, or other transaction in which the Third Party assumes control of
119 all or part of the Regulated Entity's assets and shall comply with the requirements and
120 obligations in this chapter.

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

123 Section 2. Consumer Health Data Privacy Policy.

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

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

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

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

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

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

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

136 (3) A Regulated Entity shall not collect or share additional categories of Consumer
137 Health Data not disclosed in the Consumer Health Data Privacy Policy without first disclosing
138 the additional categories and obtaining the consumer's consent prior to the collection or sharing
139 of such Consumer Health Data.

140 (4) A Regulated Entity shall not collect or share Consumer Health Data for additional
141 purposes not disclosed in the Consumer Health Data Privacy Policy without first disclosing the
142 additional purposes and obtaining the consumer's consent prior to the collection or sharing of
143 such Consumer Health Data.

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

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

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

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

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

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

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

154 (3) Consent required under this section must be obtained prior to the collection or
155 sharing, as applicable, of any Consumer Health Data, and the request for consent must clearly
156 and conspicuously disclose:

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

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

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

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

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

167 Section 4. Consumer Health Data Rights.

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

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

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

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

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

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

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

185 (c) All affiliates, service providers, contractors, and Third Parties that receive notice of a
186 consumer's deletion request shall honor the consumer's deletion request and delete the
187 Consumer Health Data from its records, including from all parts of its network.

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

191 (b) In the case of collecting Consumer Health Data concerning a consumer subject to
192 guardianship, conservatorship, or other protective arrangement under the Consumer Protection
193 Act, the guardian or the conservator of the consumer may exercise the rights of this chapter on
194 the consumer's behalf.

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

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

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

203 (c) Engage in public or peer-reviewed scientific, historical, or statistical research in the
204 public interest that adheres to all other applicable ethics and privacy laws, when the Regulated
205 Entity's deletion of the information is likely to render impossible or seriously impair the
206 achievement of such research, if the consumer has provided consent to such use of their
207 Consumer Health Data;

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

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

211 Section 5. Consumer Health Data Security and Minimization.

212 (1) A Regulated Entity shall restrict access to Consumer Health Data by the employees,
213 service providers, and contractors of such Regulated Entity to only those employees, services
214 providers, and contractors for which access is necessary to provide a product or service that the
215 consumer to whom such data and information relates has requested from such Regulated Entity.

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

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

221 Section 6. Unlawful to Sell Consumer Health Data.

222 (1) It shall be unlawful for a Regulated Entity to sell Consumer Health Data concerning a
223 consumer without first obtaining valid authorization from the consumer. The sale of Consumer
224 Health Data must be consistent with the valid authorization signed by the consumer.

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

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

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

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

234 (d) A description of the purpose for the sale, including how the Consumer Health Data
235 will be gathered and how it will be used by the purchaser identified in (c) of this subsection when
236 sold;

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

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

241 (g) A statement that the Consumer Health Data sold pursuant to the valid authorization
242 may be subject to redisclosure by the purchaser and may no longer be protected by this section.

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

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

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

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

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

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

251 (5) The seller and purchaser of Consumer Health Data must retain a copy of all valid
252 authorizations for sale of Consumer Health Data for six years from the date of its signature or the
253 date when it was last in effect, whichever is later.

254 Section 7. Enforcement - Consumer Protection Act.

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

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

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

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

270 Section 8. Exemptions.

271 (1) This chapter does not apply to protected health information collected, used, or
272 disclosed by covered entities and business associates when the protected health information is
273 collected, used, or disclosed in accordance with the federal health insurance portability and
274 accountability act of 1996 and its implementing regulations and afforded all the privacy
275 protections and security safeguards of that federal law. For the purpose of this subsection (1),
276 "protected health information," "covered entity," and "business associate" have the same

277 meaning as in the federal health insurance portability and accountability act of 1996 and its
278 implementing regulations.

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

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