

SENATE No. 184

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:	
<i>Robyn K. Kennedy</i>	<i>First Worcester</i>	
<i>Jacob R. Oliveira</i>	<i>Hampden, Hampshire and Worcester</i>	<i>2/3/2023</i>
<i>Jason M. Lewis</i>	<i>Fifth Middlesex</i>	<i>2/9/2023</i>
<i>Lindsay N. Sabadosa</i>	<i>1st Hampshire</i>	<i>2/13/2023</i>
<i>Steven Owens</i>	<i>29th Middlesex</i>	<i>3/14/2023</i>
<i>Jack Patrick Lewis</i>	<i>7th Middlesex</i>	<i>10/4/2023</i>
<i>Paul W. Mark</i>	<i>Berkshire, Hampden, Franklin and Hampshire</i>	<i>1/2/2024</i>

SENATE No. 184

By Ms. Kennedy, a petition (accompanied by bill, Senate, No. 184) of Robyn K. Kennedy, Jacob R. Oliveira, Jason M. Lewis and Lindsay N. Sabadosa for legislation 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:

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

18 (a) An individual’s deoxyribonucleic acid (DNA);

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

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

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

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

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

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

32 (iii) A consumer’s agreement obtained through the use of deceptive designs, including by
33 the use of pre-checked or pre-selected options.

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

39 “Consumer Health Data,” personal information relating to the past, present, or future
40 physical or mental health of a consumer, including any personal information relating to:

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

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

43 (iii) Health related surgeries or procedures;

44 (iv) Use or purchase of medication;

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

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

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

48 (viii) Location information that could reasonably indicate a consumer’s attempt to
49 acquire or receive health services or supplies; and

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

53 (b) Consumer Health Data does not include:

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

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

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

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

70 “Personal Information,” information that identifies, relates to, describes, is reasonably
71 capable of being associated with, or linked, directly or indirectly, with a particular consumer.
72 Personal information does not include publicly available information. For purposes of this
73 paragraph, “publicly available” means information that is lawfully made available from federal,
74 state, or local government records. Any biometric data collected about a consumer by a business
75 without the consumer's knowledge is not publicly available information.

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

80 “Sell” or “Sale,” the sharing of Consumer Health Data for monetary or other valuable
81 consideration. Sell or Sale does not include the sharing of Consumer Health Data for monetary or
82 other valuable consideration to:

83 (i) A third party as an asset that is part of a merger, acquisition, bankruptcy, or other
84 transaction in which the third party assumes control of all or part of the Regulated Entity’s assets
85 that shall comply with the requirements and obligations in this chapter;

86 (ii) A third party at the direction of a consumer; or

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

91 “Share” or “Sharing,” to release, disclose, disseminate, divulge, make available, provide
92 access to, license, or otherwise communicate orally, in writing, or by electronic or other means,
93 Consumer Health Data by a Regulated Entity to a third party where the Regulated Entity
94 maintains control and/or ownership of the Consumer Health Data. The term share or sharing
95 does not include:

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

101 (ii) The disclosure of Consumer Health Data to a third party with whom the consumer has
102 a direct relationship for purposes of providing a product or service requested by the consumer
103 when the Regulated Entity maintains control and ownership of the data and the third party only
104 uses the Consumer Health Data at direction from the Regulated Entity and consistent with the
105 purpose for which it was collected and disclosed to the consumer; or

106 (iii) The disclosure or transfer of personal data to a third party as an asset that is part of a
107 merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of
108 all or part of the Regulated Entity’s assets and shall comply with the requirements and
109 obligations in this chapter.

110 Section 2. Consumer Health Data Privacy Policy.

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

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

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

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

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

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

121 (2) A Regulated Entity shall prominently publish its Consumer Health Privacy Policy on
122 its homepage.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

153 Section 4. Consumer Health Data Rights.

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

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

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

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

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

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

167 (b) All affiliates, service providers, contractors, other third parties that receive notice of a
168 consumer's deletion request shall honor the consumer's deletion request and delete the
169 Consumer Health Data from its records, including from all parts of its network or backup
170 systems.

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

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

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

177 (c) In the case of collecting Consumer Health Data concerning a consumer subject to
178 guardianship, conservatorship, or other protective arrangement under the Consumer Protection
179 Act, the guardian or the conservator of the consumer may exercise the rights of this chapter on
180 the consumer's behalf.

181 Section 5. Consumer Health Data Security and Minimization.

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

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

190 (3) A Regulated Entity shall document the measures used to ensure compliance and shall
191 make this documentation publicly available.

192 Section 6. Unlawful to Sell Consumer Health Data.

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

194 Section 7. Enforcement - Consumer Protection Act.

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

200 Section 8. Exemptions.

201 (1) This chapter does not apply to protected health information collected, used, or
202 disclosed by covered entities and business associates when the protected health information is
203 collected, used, or disclosed in accordance with the federal health insurance portability and
204 accountability act of 1996 and its implementing regulations and afforded all the privacy
205 protections and security safeguards of that federal law. For the purpose of this subsection (1),
206 “protected health information,” “covered entity,” and “business associate” have the same
207 meaning as in the federal health insurance portability and accountability act of 1996 and its
208 implementing regulations.

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

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