



General Assembly

Amendment

January Session, 2015

LCO No. 7387



Offered by:

SEN. LOONEY, 11th Dist.
SEN. DUFF, 25th Dist.
SEN. COLEMAN, 2nd Dist.
SEN. DOYLE, 9th Dist.

SEN. SLOSSBERG, 14th Dist.
SEN. GERRATANA, 6th Dist.
SEN. CRISCO, 17th Dist.

To: Subst. Senate Bill No. 1024

File No. 270

Cal. No. 193

"AN ACT CONCERNING THE SECURITY OF CONSUMER DATA."

1 Strike everything after the enacting clause and substitute the
2 following in lieu thereof:

3 "Section 1. (NEW) (*Effective October 1, 2015*) (a) As used in this
4 section:

5 (1) "Breach of security" has the same meaning as provided in section
6 36a-701b of the general statutes, as amended by this act;

7 (2) "Company" means a health insurer, health care center or other
8 entity licensed to do health insurance business in this state, pharmacy
9 benefits manager, as defined in section 38a-479aaa of the general
10 statutes, third-party administrator, as defined in section 38a-720 of the
11 general statutes, that administers health benefits, and utilization
12 review company, as defined in section 38a-591a of the general statutes;

13 (3) "Encryption" means the rendering of electronic data into a form
14 that is unreadable or unusable without the use of a confidential
15 process or key; and

16 (4) "Personal information" means an individual's first name or first
17 initial and last name in combination with any one or more of the
18 following data: (A) A Social Security number; (B) a driver's license
19 number or a state identification number; (C) protected health
20 information as defined in 45 CFR 160.103, as amended from time to
21 time; (D) a taxpayer identification number; (E) an alien registration
22 number; (F) a government passport number; (G) a demand deposit
23 account number; (H) a savings account number; (I) a credit card
24 number; (J) a debit card number; or (K) unique biometric data such as
25 a fingerprint, a voice print, a retina or an iris image, or other unique
26 physical representations. "Personal information" does not include
27 publicly available information that is lawfully made available to the
28 general public from federal, state or local government records or
29 widely distributed media.

30 (b) (1) Not later than October 1, 2017, each company shall
31 implement and maintain a comprehensive information security
32 program to safeguard the personal information of insureds and
33 enrollees that is compiled or maintained by such company. Such
34 security program shall be in writing and contain administrative,
35 technical and physical safeguards that are appropriate to (A) the size,
36 scope and type of business of such company, (B) the amount of
37 resources available to such company, (C) the amount of data compiled
38 or maintained by such company, and (D) the need for security and
39 confidentiality of such data.

40 (2) Each company shall update such security program as often as
41 necessary and practicable but at least annually and shall include in
42 such security program:

43 (A) Secure computer and Internet user authentication protocols that
44 include, but are not limited to, (i) control of user identifications and

45 other identifiers, (ii) multifactor authentication that includes a
46 reasonably secure method of assigning and selecting a password or the
47 use of unique identifier technologies such as biometrics or security
48 tokens, (iii) control of security passwords to ensure that such
49 passwords are maintained in a location and format that do not
50 compromise the security of personal information, (iv) restriction of
51 access to only active users and active user accounts, and (v) the
52 blocking of access after multiple unsuccessful attempts to gain access
53 to data compiled or maintained by a company;

54 (B) Secure access control measures that include, but are not limited
55 to, (i) restriction of access to personal information to only those
56 individuals who require such data to perform their job duties, (ii)
57 assignment, to each individual with computer and Internet access to
58 data compiled or maintained by such company, of passwords that are
59 not vendor-assigned default passwords and that require resetting not
60 less than every six months and of unique user identifications, that are
61 designed to maintain the integrity of the security of the access controls,
62 (iii) encryption of all personal information while being transmitted on
63 a public Internet network or wirelessly, (iv) encryption of all personal
64 information stored on a laptop computer or other portable device, (v)
65 monitoring of such company's security systems for breaches of
66 security, (vi) for personal information that is stored or accessible on a
67 system that is connected to the Internet, reasonably up-to-date
68 software security protection that can support updates and patches,
69 including, but not limited to, firewall protection, operating system
70 security patches and malicious software protection, and (vii) employee
71 education and training on the proper use of the company's security
72 systems and the importance of the security of personal information;

73 (C) Designation of one or more employees to oversee such security
74 program and the maintenance of such security program;

75 (D) (i) Identification and assessment of reasonably foreseeable
76 internal and external risks to the security, confidentiality or integrity of
77 any electronic, paper or other records that contain personal

78 information, (ii) evaluation and improvement where necessary of the
79 effectiveness of the current safeguards for limiting such risks,
80 including, but not limited to, (I) ongoing employee training, (II)
81 employee compliance with security policies and procedures, and (III)
82 means for detecting and preventing security system failures, and (iii)
83 the upgrade of safeguards as necessary to limit risks;

84 (E) Development of employee security policies and procedures for
85 the storage of, access to, transport of and transmittal of personal
86 information off-premises;

87 (F) Imposition of disciplinary measures on employees for violating
88 security policies or procedures or other provisions of the
89 comprehensive information security program;

90 (G) Prevention of terminated, inactive or retired employees from
91 accessing personal information;

92 (H) Oversight of third parties with which such company enters into
93 contracts or agreements that have or will have access to personal
94 information compiled or maintained by the company, by (i) selecting
95 third parties that are capable of maintaining appropriate safeguards
96 consistent with this subsection to protect such personal information,
97 and (ii) requiring such third parties by contract or agreement to
98 implement and maintain such safeguards;

99 (I) Reasonable restrictions on physical access to personal
100 information in paper format and storage of such data in locked
101 facilities, storage areas or containers;

102 (J) Review of the scope of the secure access control measures at least
103 annually or whenever there is a material change in the company's
104 business practices that may affect the security, confidentiality or
105 integrity of personal information;

106 (K) Mandatory post-incident review by the company following any
107 actual or suspected breach of security, and documentation of actions

108 the company takes in response to such breach, including any changes
109 the company makes to its business practices relating to the
110 safeguarding of personal information; and

111 (L) Any other safeguards the company believes will enhance its
112 comprehensive information security program.

113 (c) On or after October 1, 2017, each company shall certify annually
114 to the Insurance Department, under penalty of perjury, that it
115 maintains a comprehensive information security program that
116 complies with the requirements of subsection (b) of this section.

117 (d) Upon request by the Insurance Commissioner or by the Attorney
118 General, each company shall provide to the commissioner or the
119 Attorney General a copy of its comprehensive information security
120 program. If the commissioner or the Attorney General determines that
121 such security program does not conform to the requirements set forth
122 in subsection (b) of this section, the commissioner or the Attorney
123 General shall notify the company of such determination and such
124 company shall make changes as necessary to bring such security
125 program into conformance to the commissioner's or the Attorney
126 General's satisfaction.

127 (e) Each company that discovers an actual or suspected breach of
128 security shall comply with the notice requirements set forth in section
129 36a-701b of the general statutes, as amended by this act, and shall be
130 subject to the penalty set forth in subsection (g) of section 36a-701b of
131 the general statutes, as amended by this act, for failure to comply.

132 (f) The Insurance Commissioner shall enforce the provisions of
133 subsections (b) to (d), inclusive, of this section.

134 Sec. 2. Section 36a-701b of the general statutes is repealed and the
135 following is substituted in lieu thereof (*Effective October 1, 2015*):

136 (a) For purposes of this section, (1) "breach of security" means
137 unauthorized access to or unauthorized acquisition of electronic files,

138 media, databases or computerized data, containing personal
139 information when access to the personal information has not been
140 secured by encryption or by any other method or technology that
141 renders the personal information unreadable or unusable; and (2)
142 "personal information" means (A) any information or combination of
143 information capable of being used to access, open, use or misuse any
144 credit account of an individual or to commit identity theft, as defined
145 in section 53a-129a, or (B) an individual's first name or first initial and
146 last name in combination with any one, or more, of the following data:
147 [(1)] (i) Social Security number; [(2)] (ii) driver's license number or state
148 identification card number; or [(3)] (iii) account number, credit or debit
149 card number, in combination with any required security code, access
150 code or password that would permit access to an individual's financial
151 account. "Personal information" does not include publicly available
152 information that is lawfully made available to the general public from
153 federal, state or local government records or widely distributed media.

154 (b) (1) Any person who conducts business in this state, and who, in
155 the ordinary course of such person's business, owns, licenses or
156 maintains computerized data that includes personal information, shall
157 provide notice of any breach of security following the discovery of the
158 breach to any resident of this state whose personal information was, or
159 is reasonably believed to have been, accessed by an unauthorized
160 person through such breach of security. Such notice shall be [made]
161 provided without unreasonable delay but not later than thirty days
162 after such breach of security is discovered, subject to the provisions of
163 subsection (d) of this section and the completion of an investigation by
164 such person to determine the nature and scope of the incident, to
165 identify the individuals affected, or to restore the reasonable integrity
166 of the data system. Such [notification] notice shall not be required if,
167 after an appropriate investigation and consultation with relevant
168 federal, state and local agencies responsible for law enforcement, the
169 person reasonably determines that the breach will not likely result in
170 harm to the individuals whose personal information has been acquired
171 and accessed.

172 (2) If notice of a breach of security is required by subdivision (1) of
173 this subsection; [, the] (A) The person who conducts business in this
174 state, and who, in the ordinary course of such person's business, owns,
175 licenses or maintains computerized data that includes personal
176 information, shall, not later than the time when notice is provided to
177 the resident, also provide notice of the breach of security to the
178 Attorney General; and (B) concurrent with the provision of such notice
179 to a resident, the person providing such notice shall offer to such
180 resident free credit monitoring for a period of not less than one year.
181 Such credit monitoring shall include, at a minimum, a periodic review
182 of the resident's credit report at more than one credit rating agency for
183 accuracy and changes that could be indicative of fraudulent activity.
184 Such offer shall include clear instructions explaining how such
185 resident may enroll in the free credit monitoring program.

186 (c) Any person that maintains computerized data that includes
187 personal information that the person does not own shall notify the
188 owner or licensee of the information of any breach of the security of
189 the data immediately following its discovery, if the personal
190 information of a resident of this state was, or is reasonably believed to
191 have been accessed by an unauthorized person.

192 (d) Any notification required by this section shall be delayed for a
193 reasonable period of time if a law enforcement agency determines that
194 the notification will impede a criminal investigation and such law
195 enforcement agency has made a request that the notification be
196 delayed. Any such delayed notification shall be made after such law
197 enforcement agency determines that notification will not compromise
198 the criminal investigation and so notifies the person of such
199 determination.

200 (e) Any notice to a resident, owner or licensee required by the
201 provisions of this section may be provided by one of the following
202 methods: (1) Written notice; (2) telephone notice; (3) electronic notice,
203 provided such notice is consistent with the provisions regarding
204 electronic records and signatures set forth in 15 USC 7001; (4)

205 substitute notice, provided such person demonstrates that the cost of
206 providing notice in accordance with subdivision (1), (2) or (3) of this
207 subsection would exceed two hundred fifty thousand dollars, that the
208 affected class of subject persons to be notified exceeds five hundred
209 thousand persons or that the person does not have sufficient contact
210 information. Substitute notice shall consist of the following: (A)
211 Electronic mail notice when the person has an electronic mail address
212 for the affected persons; (B) conspicuous posting of the notice on the
213 web site of the person if the person maintains one; and (C) notification
214 to major state-wide media, including newspapers, radio and television.

215 (f) Any person that maintains such person's own security breach
216 procedures as part of an information security policy for the treatment
217 of personal information and otherwise complies with the timing
218 requirements of this section, shall be deemed to be in compliance with
219 the security breach notification requirements of this section, provided
220 such person notifies, as applicable, residents of this state, owners and
221 licensees in accordance with such person's policies in the event of a
222 breach of security and in the case of notice to a resident, such person
223 also notifies the Attorney General not later than the time when notice
224 is provided to the resident. Any person that maintains such a security
225 breach procedure pursuant to the rules, regulations, procedures or
226 guidelines established by the primary or functional regulator, as
227 defined in 15 USC 6809(2), shall be deemed to be in compliance with
228 the security breach notification requirements of this section, provided
229 (1) such person notifies, as applicable, such residents of this state,
230 owners, and licensees required to be notified under and in accordance
231 with the policies or the rules, regulations, procedures or guidelines
232 established by the primary or functional regulator in the event of a
233 breach of security, and (2) if notice is given to a resident of this state in
234 accordance with subdivision (1) of this subsection regarding a breach
235 of security, such person also notifies the Attorney General not later
236 than the time when notice is provided to the resident.

237 (g) Failure to comply with the requirements of this section shall

238 constitute an unfair trade practice for purposes of section 42-110b and
239 shall be enforced by the Attorney General."

This act shall take effect as follows and shall amend the following sections:		
Section 1	<i>October 1, 2015</i>	New section
Sec. 2	<i>October 1, 2015</i>	36a-701b