



General Assembly

Amendment

January Session, 2015

LCO No. 8332



Offered by:
SEN. LOONEY, 11th Dist.
SEN. DUFF, 25th Dist.

To: Subst. Senate Bill No. **949** File No. 705 Cal. No. 401

(As Amended by Senate Amendment Schedule "A")

"AN ACT IMPROVING DATA SECURITY AND AGENCY EFFECTIVENESS."

1 After the last section, add the following and renumber sections and
2 internal references accordingly:

3 "Sec. 501. (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 (1) comply with the notice requirements set forth in
129 section 36a-701b of the general statutes, as amended by this act, (2) 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, and
132 (3) offer appropriate identity theft prevention services and, if
133 applicable, identity theft mitigation services, as set forth in
134 subparagraph (B) of subdivision (2) of subsection (b) of section 36a-
135 701b of the general statutes, as amended by this act.

136 (f) The Insurance Commissioner shall enforce the provisions of

137 subsections (b) to (d), inclusive, of this section.

138 Sec. 502. Section 36a-701b of the general statutes is repealed and the
139 following is substituted in lieu thereof (*Effective October 1, 2015*):

140 (a) For purposes of this section, (1) "breach of security" means
141 unauthorized access to or unauthorized acquisition of electronic files,
142 media, databases or computerized data, containing personal
143 information when access to the personal information has not been
144 secured by encryption or by any other method or technology that
145 renders the personal information unreadable or unusable; and (2)
146 "personal information" means an individual's first name or first initial
147 and last name in combination with any one, or more, of the following
148 data: [(1)] (A) Social Security number; [(2)] (B) driver's license number
149 or state identification card number; or [(3)] (C) account number, credit
150 or debit card number, in combination with any required security code,
151 access code or password that would permit access to an individual's
152 financial account. "Personal information" does not include publicly
153 available information that is lawfully made available to the general
154 public from federal, state or local government records or widely
155 distributed media.

156 (b) (1) Any person who conducts business in this state, and who, in
157 the ordinary course of such person's business, owns, licenses or
158 maintains computerized data that includes personal information, shall
159 provide notice of any breach of security following the discovery of the
160 breach to any resident of this state whose personal information was []
161 breached or is reasonably believed to have been [, accessed by an
162 unauthorized person through such breach of security] breached. Such
163 notice shall be made without unreasonable delay but not later than
164 ninety days after the discovery of such breach, unless a shorter time is
165 required under federal law, subject to the provisions of subsection (d)
166 of this section and the completion of an investigation by such person to
167 determine the nature and scope of the incident, to identify the
168 individuals affected, or to restore the reasonable integrity of the data
169 system. Such notification shall not be required if, after an appropriate

170 investigation and consultation with relevant federal, state and local
171 agencies responsible for law enforcement, the person reasonably
172 determines that the breach will not likely result in harm to the
173 individuals whose personal information has been acquired and
174 accessed.

175 (2) If notice of a breach of security is required by subdivision (1) of
176 this subsection: [, the]

177 (A) The person who conducts business in this state, and who, in the
178 ordinary course of such person's business, owns, licenses or maintains
179 computerized data that includes personal information, shall, not later
180 than the time when notice is provided to the resident, also provide
181 notice of the breach of security to the Attorney General; and

182 (B) The person who conducts business in this state, and who, in the
183 ordinary course of such person's business, owns or licenses
184 computerized data that includes personal information, shall offer to
185 each resident whose personal information under subparagraph (A) of
186 subdivision (4) of subsection (a) of section 501 of this act or
187 subparagraph (A) of subdivision (2) of subsection (a) of this section
188 was breached or is reasonably believed to have been breached,
189 appropriate identity theft prevention services and, if applicable,
190 identity theft mitigation services. Such service or services shall be
191 provided at no cost to such resident for a period of not less than twelve
192 months. Such person shall provide all information necessary for such
193 resident to enroll in such service or services and shall include
194 information on how such resident can place a credit freeze on such
195 resident's credit file.

196 (c) Any person that maintains computerized data that includes
197 personal information that the person does not own shall notify the
198 owner or licensee of the information of any breach of the security of
199 the data immediately following its discovery, if the personal
200 information of a resident of this state was [,] breached or is reasonably
201 believed to have been [accessed by an unauthorized person] breached.

202 (d) Any notification required by this section shall be delayed for a
203 reasonable period of time if a law enforcement agency determines that
204 the notification will impede a criminal investigation and such law
205 enforcement agency has made a request that the notification be
206 delayed. Any such delayed notification shall be made after such law
207 enforcement agency determines that notification will not compromise
208 the criminal investigation and so notifies the person of such
209 determination.

210 (e) Any notice to a resident, owner or licensee required by the
211 provisions of this section may be provided by one of the following
212 methods: (1) Written notice; (2) telephone notice; (3) electronic notice,
213 provided such notice is consistent with the provisions regarding
214 electronic records and signatures set forth in 15 USC 7001; (4)
215 substitute notice, provided such person demonstrates that the cost of
216 providing notice in accordance with subdivision (1), (2) or (3) of this
217 subsection would exceed two hundred fifty thousand dollars, that the
218 affected class of subject persons to be notified exceeds five hundred
219 thousand persons or that the person does not have sufficient contact
220 information. Substitute notice shall consist of the following: (A)
221 Electronic mail notice when the person has an electronic mail address
222 for the affected persons; (B) conspicuous posting of the notice on the
223 web site of the person if the person maintains one; and (C) notification
224 to major state-wide media, including newspapers, radio and television.

225 (f) Any person that maintains such person's own security breach
226 procedures as part of an information security policy for the treatment
227 of personal information and otherwise complies with the timing
228 requirements of this section, shall be deemed to be in compliance with
229 the security breach notification requirements of this section, provided
230 such person notifies, as applicable, residents of this state, owners and
231 licensees in accordance with such person's policies in the event of a
232 breach of security and in the case of notice to a resident, such person
233 also notifies the Attorney General not later than the time when notice
234 is provided to the resident. Any person that maintains such a security

235 breach procedure pursuant to the rules, regulations, procedures or
 236 guidelines established by the primary or functional regulator, as
 237 defined in 15 USC 6809(2), shall be deemed to be in compliance with
 238 the security breach notification requirements of this section, provided
 239 (1) such person notifies, as applicable, such residents of this state,
 240 owners, and licensees required to be notified under and in accordance
 241 with the policies or the rules, regulations, procedures or guidelines
 242 established by the primary or functional regulator in the event of a
 243 breach of security, and (2) if notice is given to a resident of this state in
 244 accordance with subdivision (1) of this subsection regarding a breach
 245 of security, such person also notifies the Attorney General not later
 246 than the time when notice is provided to the resident.

247 (g) Failure to comply with the requirements of this section shall
 248 constitute an unfair trade practice for purposes of section 42-110b and
 249 shall be enforced by the Attorney General."

This act shall take effect as follows and shall amend the following sections:		
Sec. 501	October 1, 2015	New section
Sec. 502	October 1, 2015	36a-701b