



AN ACT IMPROVING DATA SECURITY AND AGENCY EFFECTIVENESS.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

1 Section 1. (NEW) (*Effective July 1, 2015*) (a) As used in this section
2 and section 2 of this act:

3 (1) "Contractor" means an individual, business or other entity that is
4 receiving confidential information from a state contracting agency or
5 agent of the state pursuant to a written agreement to perform services
6 for the state.

7 (2) "State agency" means any agency with a department head, as
8 defined in section 4-5 of the general statutes.

9 (3) "State contracting agency" means any state agency disclosing
10 confidential information to a contractor pursuant to a written
11 agreement with such contractor for the performance of services for the
12 state.

13 (4) "Confidential information" means information capable of being
14 associated with a particular individual through one or more
15 identifiers, including, but not limited to, an individual's name, date of
16 birth, mother's maiden name, motor vehicle operator's license number,
17 Social Security number, employee identification number, employer or

18 taxpayer identification number, alien registration number, government
19 passport number, health insurance identification number, demand
20 deposit account number, savings account number, credit card number,
21 debit card number or unique biometric data such as fingerprint, voice
22 print, retina or iris image, or other unique physical representation. In
23 addition, "confidential information" includes any information that a
24 state agency identifies as confidential to the contractor. "Confidential
25 information" does not include information that may be lawfully
26 obtained from publicly available sources or from federal, state, or local
27 government records that are lawfully made available to the general
28 public.

29 (5) "Confidential information breach" means an instance where an
30 unauthorized person or entity accesses or may have accessed
31 confidential information in any manner, including, but not limited to,
32 the following occurrences: (A) Any confidential information that is not
33 encrypted or secured by any other method or technology that renders
34 the personal information unreadable or unusable is misplaced, lost,
35 stolen or in any way compromised; (B) one or more third parties have
36 had access to, or taken control or possession of, without prior written
37 authorization from the state, (i) any confidential information that is not
38 encrypted or protected, or (ii) any encrypted or protected confidential
39 information together with the confidential process or key that is
40 capable of compromising the integrity of the confidential information;
41 or (C) there is a substantial risk of identity theft or fraud of the client of
42 the state contracting agency, the contractor, the state contracting
43 agency or the state.

44 (b) Except as provided in section 2 of this act, every agreement that
45 requires a state contracting agency to share confidential information
46 with a contractor shall require the contractor to, at a minimum, do the
47 following:

48 (1) At its own expense, protect from a confidential information
49 breach any and all confidential information that it comes to possess or
50 control, wherever and however stored or maintained;

51 (2) Implement and maintain a comprehensive data-security
52 program for the protection of confidential information. The safeguards
53 contained in such program shall be consistent with and comply with
54 the safeguards for protection of confidential information as set forth in
55 all applicable federal and state law and written policies of the state
56 contained in the agreement. Such data-security program shall include,
57 but not be limited to, the following: (A) A security policy for contractor
58 employees related to the storage, access and transportation of data
59 containing confidential information; (B) reasonable restrictions on
60 access to records containing confidential information, including the
61 area where such records are kept and secure passwords for
62 electronically stored records; (C) a process for reviewing policies and
63 security measures at least annually; and (D) an active and ongoing
64 employee security awareness program that is mandatory for all
65 employees who may have access to confidential information provided
66 by the state contracting agency that, at a minimum, advises such
67 employees of the confidentiality of the information, the safeguards
68 required to protect the information and any applicable civil and
69 criminal penalties for noncompliance pursuant to state and federal
70 law;

71 (3) Limit access to confidential information to authorized contractor
72 employees and their authorized agents, for authorized purposes as
73 necessary for the completion of the contracted services;

74 (4) Maintain all electronic data obtained from state contracting
75 agencies: (A) In a secure server; (B) on secure drives; (C) behind
76 multilevel firewall protections and monitored by intrusion detection
77 software; and (D) in a manner where access is restricted to authorized
78 employees and their authorized agents; and

79 (5) Enter into and maintain an appropriate confidentiality
80 agreement with each employee and authorized agent who has access
81 to confidential information.

82 (c) Except as specifically provided for in the agreement, a contractor

83 shall not:

84 (1) Store data on stand-alone computer or notebook hard disks or
85 portable storage devices such as external or removable hard drives,
86 flash cards, flash drives, compact disks or digital video disks; or

87 (2) Copy, reproduce or transmit data except as necessary for the
88 completion of the contracted services.

89 (d) All copies of data of any type, including, but not limited to, any
90 modifications or additions to data that contain confidential
91 information, are subject to the provisions of this section in the same
92 manner as the original data.

93 (e) In the case of a confidential information breach or suspected
94 confidential information breach a contractor shall:

95 (1) Notify the state contracting agency and the Attorney General as
96 soon as practical, but not later than twenty-four hours after the
97 contractor becomes aware of or has reason to believe that any
98 confidential information that the contractor possesses or controls has
99 been subject to a confidential information breach or suspected
100 confidential information breach;

101 (2) Immediately cease all use of the data provided by the state
102 contracting agency or developed internally by the contractor if so
103 directed by the state contracting agency;

104 (3) Not later than three business days after the notification, submit
105 to the office of the Attorney General and the state contracting agency
106 either (A) a report detailing the breach, or (B) a report detailing why,
107 upon further investigation, the contractor believes no breach has
108 occurred; and

109 (4) Not later than six days after the notification, submit to the office
110 of the Attorney General and the state contracting agency a plan to
111 mitigate the effects of the breach and specifying the steps taken to

112 ensure future breaches do not occur, except that no such plan is
113 required of a contractor who has reported that no breach has occurred
114 under subdivision (3) of this subsection.

115 (f) Based on the report and, if applicable, the plan provided, the
116 state contracting agency shall decide, in its sole discretion, whether to
117 permit any contractor who has been directed to cease use of data
118 under subdivision (2) of subsection (e) of this section, to recommence
119 use of the data or whether to cancel the agreement.

120 (g) The Attorney General may investigate any violation of this
121 section. If the Attorney General finds that a contractor has violated or
122 is violating any provision of this section, the Attorney General may
123 bring a civil action in the superior court for the judicial district of
124 Hartford under this section in the name of the state against such
125 contractor.

126 (h) If the confidential information or personally identifiable
127 information, as defined in 34 CFR 99.3, that has been subject to a
128 confidential information breach consists of education records, the
129 contractor may be subject to a five-year ban from receiving access to
130 such information imposed by the Department of Education.

131 (i) The requirements of this section shall be in addition to the
132 requirements of section 36a-701b of the general statutes, and nothing in
133 this section shall be construed to supersede a contractor's obligations
134 pursuant to the Health Insurance Portability and Accountability Act of
135 1996 P.L. 104-191 (HIPAA), the Family Educational Rights and Privacy
136 Act of 1974, 20 USC 1232g, (FERPA) or any other applicable federal or
137 state law.

138 Sec. 2. (NEW) (*Effective July 1, 2015*) The Secretary of the Office of
139 Policy and Management, or the secretary's designee, may require
140 additional protections or alternate measures of security assurance for
141 any requirement of section 1 of this act where the facts and
142 circumstances warrant such additional requirement or alternate

143 measure after taking into consideration, among other factors, (1) the
144 type of confidential information being shared, (2) the amount of
145 confidential information being shared, (3) the purpose for which the
146 information is being shared, and (4) the types of services being
147 contracted for.

148 Sec. 3. Section 4-66 of the general statutes is repealed and the
149 following is substituted in lieu thereof (*Effective from passage*):

150 The Secretary of the Office of Policy and Management shall have the
151 following functions and powers:

152 (1) To keep on file information concerning the state's general
153 accounts;

154 (2) [to] To furnish all accounting statements relating to the financial
155 condition of the state as a whole, to the condition and operation of
156 state funds, to appropriations, to reserves and to costs of operations;

157 (3) [to] To furnish such statements as and when they are required
158 for administrative purposes and, at the end of each fiscal period, to
159 prepare and publish such financial statements and data as will convey
160 to the General Assembly the essential facts as to the financial
161 condition, the revenues and expenditures and the costs of operations
162 of the state government;

163 (4) [to] To furnish to the State Comptroller on or before the
164 twentieth day of each month cumulative monthly statements of
165 revenues and expenditures to the end of the last-completed month
166 together with [(1)] (A) a statement of estimated revenue by source to
167 the end of the fiscal year, at least in the same detail as appears in the
168 budget act, and [(2)] (B) a statement of appropriation requirements of
169 the state's General Fund to the end of the fiscal year itemized as far as
170 practicable for each budgeted agency, including estimates of lapsing
171 appropriations, unallocated lapsing balances and unallocated
172 appropriation requirements;

173 (5) [to] To transmit to the Office of Fiscal Analysis a copy of monthly
174 position data and monthly bond project run;

175 (6) [to] To inquire into the operation of, and make or recommend
176 improvement in, the methods employed in the preparation of the
177 budget and the procedure followed in determining whether the funds
178 expended by the departments, boards, commissions and institutions
179 supported in whole or in part by the state are wisely, judiciously and
180 economically expended and to submit such findings and
181 recommendations to the General Assembly at each regular session,
182 together with drafts of proposed legislation, if any;

183 (7) [to] To examine each department, state college, state hospital,
184 state-aided hospital, reformatory and prison and each other institution
185 or other agency supported in whole or in part by the state, except
186 public schools, for the purpose of determining the effectiveness of its
187 policies, management, internal organization and operating procedures
188 and the character, amount, quality and cost of the service rendered by
189 each such department, institution or agency;

190 (8) [to] To recommend, and to assist any such department,
191 institution or agency to effect, improvements in organization,
192 management methods and procedures and to report its findings and
193 recommendations and submit drafts of proposed legislation, if any, to
194 the General Assembly at each regular session;

195 (9) [to] To consider and devise ways and means whereby
196 comprehensive plans and designs to meet the needs of the several
197 departments and institutions with respect to physical plant and
198 equipment and whereby financial plans and programs for the capital
199 expenditures involved may be made in advance and to make or assist
200 in making such plans;

201 (10) [to] To devise and prescribe the form of operating reports that
202 shall be periodically required from the several departments, boards,
203 commissions, institutions and agencies supported in whole or in part

204 by the state;

205 (11) [to] To require the several departments, boards, commissions,
206 institutions and agencies to make such reports for such periods as said
207 secretary may determine; and

208 (12) [to] To verify the correctness of, and to analyze, all such reports
209 and to take such action as may be deemed necessary to remedy
210 unsatisfactory conditions disclosed by such reports.

211 Sec. 4. (NEW) (*Effective July 1, 2015*) (a) For purposes of this section:

212 (1) "Data" means statistical or factual information that: (A) is
213 reflected in a list, table, graph, chart, or other nonnarrative form that
214 can be digitally transmitted or processed; (B) is regularly created and
215 maintained by or on behalf of an executive agency; and (C) records a
216 measurement, transaction or determination related to the mission of
217 the executive agency or is provided to such agency by any third party
218 as required by any provision of law. "Data" does not include return
219 and return information, as defined in section 12-15 of the general
220 statutes;

221 (2) "Executive agency" means any agency with a department head,
222 as defined in section 4-5 of the general statutes, a constituent unit of
223 higher education, as defined in section 10a-1 of the general statutes, or
224 the Office of Higher Education, established by section 10a-1d of the
225 general statutes; and

226 (3) "State agency" means any office, department, board, council,
227 commission, institution, constituent unit of the state system of higher
228 education, technical high school or other agency in the executive,
229 legislative or judicial branch of state government.

230 (b) The Secretary of the Office of Policy and Management shall
231 develop a program to access, link, analyze and share data maintained
232 by executive agencies and to respond to queries from any state agency,
233 and from any private entity or person that would otherwise require

234 access to data maintained by two or more executive agencies. The
235 secretary shall give priority to queries that seek to measure outcomes
236 for state-funded programs or that may facilitate the development of
237 policies to promote the effective, efficient and best use of state
238 resources.

239 (c) The secretary shall establish policies and procedures to:

240 (1) Review and respond to queries to ensure (A) a response is
241 permitted under state and federal law; (B) the privacy and
242 confidentiality of protected data can be assured; and (C) the query is
243 based on sound research design principles; and

244 (2) Protect and ensure the security, privacy, confidentiality and
245 administrative value of data collected and maintained by executive
246 agencies.

247 (d) The secretary shall, in consultation with the Chief Information
248 Officer, develop and implement a secure information technology
249 solution to link data across executive agencies and to develop and
250 implement a detailed data security and safeguarding plan for the data
251 accessed or shared through such solution.

252 (e) The secretary shall request from, and execute a memorandum of
253 agreement with, each executive agency detailing data-sharing between
254 the agency and the Office of Policy and Management. Each such
255 agreement shall authorize the Office of Policy and Management to act
256 on behalf of the executive agency that is a party to such agreement for
257 purposes of data access, matching and sharing and shall include
258 provisions to ensure the proper use, security and confidentiality of the
259 data shared. Any executive agency that is requested by the secretary to
260 execute such an agreement shall comply with such request.

261 (f) The secretary shall notify the applicable executive agency when
262 data within such agency's custody has been requested under
263 subsection (b) of this section.

264 (g) The Office of Policy and Management shall be an authorized
 265 representative of the Labor Commissioner or administrator of
 266 unemployment compensation under chapter 567 of the general statutes
 267 and shall receive upon request by the secretary any information in the
 268 Labor Commissioner's possession relating to employment records that
 269 may include, but need not be limited to: Employee name, Social
 270 Security number, current residential address, name and address of the
 271 employer, employer North American Industry Classification System
 272 code and wages.

273 (h) For the purposes of the Freedom of Information Act, as defined
 274 in section 1-200 of the general statutes, the Office of Policy and
 275 Management shall not be considered the agency with custody or
 276 control of any public records or files that are made accessible to said
 277 office pursuant to this section, but shall be considered the agency with
 278 custody and control of any public records or files created by the Office
 279 of Policy and Management, including, but not limited to, all reports
 280 generated by said office in response to queries posed under subsection
 281 (b) of this section.

This act shall take effect as follows and shall amend the following sections:		
Section 1	<i>July 1, 2015</i>	New section
Sec. 2	<i>July 1, 2015</i>	New section
Sec. 3	<i>from passage</i>	4-66
Sec. 4	<i>July 1, 2015</i>	New section

GAE *Joint Favorable Subst.*

INS *Joint Favorable*

JUD *Joint Favorable*