

1                   **STATE SECURITY STANDARDS FOR PERSONAL**  
2   **INFORMATION**

3   2013 GENERAL SESSION

4   STATE OF UTAH

5   **Chief Sponsor: Stuart C. Reid**

6   House Sponsor: Paul Ray

---

---

8                   **LONG TITLE**

9                   **General Description:**

10                   This bill amends the Medical Assistance Act to require a health care provider to give a  
11                   patient notice that some personal identifying information about the patient may be  
12                   shared with the state's Medicaid and Children's Health Insurance Program eligibility  
13                   database, and amends provisions in the Utah Technology Governance Act related to  
14                   statewide security standards for personal information stored or transmitted on state  
15                   servers.

16                   **Highlighted Provisions:**

17                   This bill:

- 18                   ▶ beginning July 1, 2013, requires a health care provider who participates in the state  
19                   Medicaid program or the Children's Health Insurance Program to include in the  
20                   health care provider's notice of privacy practices that the health care provider either  
21                   has, or may submit, personally identifiable information about the patient to the  
22                   state's Medicaid and Children's Health Insurance Program eligibility database;
- 23                   ▶ requires the state Medicaid program and Children's Health Insurance Program,  
24                   before giving a provider access to the state's eligibility database, to verify that the  
25                   health care provider's notice of privacy practices complies with federal and state  
26                   law;
- 27                   ▶ gives the Department of Health administrative rulemaking authority to establish  
28                   uniform language for the state requirement regarding notice of privacy practices to  
29                   patients;

- 30           ▶ amends the Utah Technology Governance Act to require the state's chief  
31 information officer to:
- 32           • in coordination with the governor's office, convene a group of experts to identify  
33 industry best practices for data security standards;
  - 34           • incorporate industry best practices for data security standards into the  
35 Department of Technology Services and executive branch agency practices;
  - 36           • modify the state's executive branch information technology strategic plan to  
37 incorporate the industry best practices standards as feasible within the  
38 Department of Technology Services or executive branch agency budgets;
  - 39           • inform the speaker of the House of Representatives and the president of the  
40 Senate if security standards are not adopted due to budget issues; and
  - 41           • conduct an assessment of the Department of Technology Services and executive  
42 branch agency security standards at least once every two years;
- 43           ▶ provides a process in which a state agency that contracts for services from the  
44 Department of Technology Services may enter into an agreement with the  
45 department to audit the security standards implemented by the department; and
- 46           ▶ makes technical and conforming amendments.

47 **Money Appropriated in this Bill:**

48           None

49 **Other Special Clauses:**

50           None

51 **Utah Code Sections Affected:**

52 AMENDS:

53           **63F-1-104**, as last amended by Laws of Utah 2011, Chapter 270

54           **63F-1-202**, as last amended by Laws of Utah 2010, Chapter 286

55           **63F-1-203**, as last amended by Laws of Utah 2011, Chapter 270

56           **63F-1-204**, as last amended by Laws of Utah 2008, Chapter 382

57           **63F-1-604**, as last amended by Laws of Utah 2011, Chapter 270

58 ENACTS:

59 **26-18-17**, Utah Code Annotated 1953



61 *Be it enacted by the Legislature of the state of Utah:*

62 Section 1. Section **26-18-17** is enacted to read:

63 **26-18-17. Patient notice of health care provider privacy practices.**

64 (1) (a) For purposes of this section:

65 (i) "Health care provider" means a health care provider as defined in Section

66 78B-3-403 who:

67 (A) receives payment for medical services from the Medicaid program established in  
68 this chapter, or the Children's Health Insurance Program established in Chapter 40, Utah  
69 Children's Health Insurance Act; and

70 (B) submits a patient's personally identifiable information to the Medicaid eligibility  
71 database or the Children's Health Insurance Program eligibility database.

72 (ii) "HIPAA" means 45 C.F.R. Parts 160, 162, and 164, Health Insurance Portability  
73 and Accountability Act of 1996, as amended.

74 (b) Beginning July 1, 2013, this section applies to the Medicaid program, the  
75 Children's Health Insurance Program created in Chapter 40, Utah Children's Health Insurance  
76 Act, and a health care provider.

77 (2) A health care provider shall, as part of the notice of privacy practices required by  
78 HIPAA, provide notice to the patient or the patient's personal representative that the health care  
79 provider either has, or may submit, personally identifiable information about the patient to the  
80 Medicaid eligibility database and the Children's Health Insurance Program eligibility database.

81 (3) The Medicaid program and the Children's Health Insurance Program may not give a  
82 health care provider access to the Medicaid eligibility database or the Children's Health  
83 Insurance Program eligibility database unless the health care provider's notice of privacy  
84 practices complies with Subsection (2).

85 (4) The department may adopt an administrative rule to establish uniform language for

86 the state requirement regarding notice of privacy practices to patients required under  
87 Subsection (2).

88 Section 2. Section **63F-1-104** is amended to read:

89 **63F-1-104. Purposes.**

90 The department shall:

91 (1) lead state executive branch agency efforts to reengineer the state's information  
92 technology architecture with the goal of coordinating central and individual agency information  
93 technology in a manner that:

94 (a) ensures compliance with the executive branch agency strategic plan; and  
95 (b) ensures that cost-effective, efficient information and communication systems and  
96 resources are being used by agencies to:

97 (i) reduce data, hardware, and software redundancy;  
98 (ii) improve system interoperability and data accessibility between agencies; and  
99 (iii) meet the agency's and user's business and service needs;

100 (2) ~~(a)~~ coordinate an executive branch strategic plan for all agencies;

101 ~~(b)~~ (3) each year, in coordination with the governor's office, convene a group of  
102 public and private sector information technology and data security experts to identify best  
103 practices from agencies and other public and private sector entities~~;~~ and], including best  
104 practices for data and information technology system security standards;

105 ~~(c)~~ (4) develop and implement processes to replicate information technology best  
106 practices and standards identified in Subsection (3), throughout the executive branch;

107 (5) by July 1, 2015, and at least once every two years thereafter:

108 (a) evaluate the adequacy of the department's and the executive branch agencies' data  
109 and information technology system security standards through an independent third party  
110 assessment; and

111 (b) communicate the results of the independent third party assessment to the  
112 appropriate executive branch agencies and to the president of the Senate and the speaker of the  
113 House of Representatives;

114           ~~[(3)]~~ (6) oversee the expanded use and implementation of project and contract  
115 management principles as they relate to information technology projects within the executive  
116 branch;

117           ~~[(4)]~~ (7) serve as general contractor between the state's information technology users  
118 and private sector providers of information technology products and services;

119           ~~[(5)]~~ (8) work toward building stronger partnering relationships with providers;

120           ~~[(6)]~~ (9) develop service level agreements with executive branch departments and  
121 agencies to ensure quality products and services are delivered on schedule and within budget;

122           ~~[(7)]~~ (10) develop standards for application development including a standard  
123 methodology and cost-benefit analysis that all agencies shall utilize for application  
124 development activities;

125           ~~[(8)]~~ (11) determine and implement statewide efforts to standardize data elements and  
126 determine data ownership assignments among executive branch agencies;

127           ~~[(9)]~~ (12) develop systems and methodologies to review, evaluate, and prioritize  
128 existing information technology projects within the executive branch and report to the governor  
129 and the Public Utilities and Technology Interim Committee on a semiannual basis regarding  
130 the status of information technology projects; and

131           ~~[(10)]~~ (13) assist the Governor's Office of Planning and Budget with the development  
132 of information technology budgets for agencies.

133           Section 3. Section **63F-1-202** is amended to read:

134           **63F-1-202. Technology Advisory Board -- Membership -- Duties.**

135           (1) There is created the Technology Advisory Board to the chief information officer.

136           The board shall have seven members as follows:

137           (a) three members appointed by the governor who are individuals actively involved in  
138 business planning for state agencies;

139           (b) one member appointed by the governor who is actively involved in business  
140 planning for higher education or public education;

141           (c) one member appointed by the speaker of the House of Representatives and

142 president of the Senate from the Legislative Automation Committee of the Legislature to  
143 represent the legislative branch;

144 (d) one member appointed by the Judicial Council to represent the judicial branch; and

145 (e) one member appointed by the governor who represents private sector business  
146 needs in the state, but who is not an information technology vendor for the state.

147 (2) (a) The members of the advisory board shall elect a chair from the board by  
148 majority vote.

149 (b) The department shall provide staff to the board.

150 (c) (i) A majority of the members of the board constitutes a quorum.

151 (ii) Action by a majority of a quorum of the board constitutes an action of the board.

152 (3) The board shall meet as necessary to advise the chief information officer and assist  
153 the chief information officer and executive branch agencies in coming to consensus on:

154 (a) the development and implementation of the state's information technology strategic  
155 plan;

156 (b) critical information technology initiatives for the state;

157 (c) the development of standards for state information architecture;

158 (d) identification of the business and technical needs of state agencies;

159 (e) the department's performance measures for service agreements with executive  
160 branch agencies and subscribers of services, including a process in which an executive branch  
161 agency may review the department's implementation of and compliance with an executive  
162 branch agency's data security requirements; and

163 (f) the efficient and effective operation of the department.

164 (4) A member may not receive compensation or benefits for the member's service, but  
165 may receive per diem and travel expenses in accordance with:

166 (a) Section 63A-3-106;

167 (b) Section 63A-3-107; and

168 (c) rules made by the Division of Finance pursuant to Sections 63A-3-106 and  
169 63A-3-107.

170 Section 4. Section **63F-1-203** is amended to read:

171 **63F-1-203. Executive branch information technology strategic plan.**

172 (1) In accordance with this section, the chief information officer shall prepare an  
173 executive branch information technology strategic plan:

174 (a) that complies with this chapter; and

175 (b) which shall include:

176 (i) a strategic plan for the:

177 (A) interchange of information related to information technology between executive  
178 branch agencies;

179 (B) coordination between executive branch agencies in the development and  
180 maintenance of information technology and information systems, including the coordination of  
181 agency information technology plans described in Section 63F-1-204; and

182 (C) protection of the privacy of individuals who use state information technology or  
183 information systems, including the implementation of industry best practices for data and  
184 system security that are identified in Subsection 63F-1-104(3);

185 (ii) priorities for the development and implementation of information technology or  
186 information systems including priorities determined on the basis of:

187 (A) the importance of the information technology or information system; and

188 (B) the time sequencing of the information technology or information system; and

189 (iii) maximizing the use of existing state information technology resources.

190 (2) In the development of the executive branch strategic plan, the chief information  
191 officer shall consult with:

192 (a) all cabinet level officials [and];

193 (b) the advisory board created in Section 63F-1-202[-]; and

194 (c) the group convened in accordance with Subsection 63F-1-104(3).

195 (3) (a) Unless withdrawn by the chief information officer or the governor in accordance  
196 with Subsection (3)(b), the executive branch strategic plan takes effect 30 days after the day on  
197 which the executive branch strategic plan is submitted to:

198 (i) the governor; and  
199 (ii) the Public Utilities and Technology Interim Committee.  
200 (b) The chief information officer or the governor may withdraw the executive branch  
201 strategic plan submitted under Subsection (3)(a) if the governor or chief information officer  
202 determines that the executive branch strategic plan:

203 (i) should be modified; or  
204 (ii) for any other reason should not take effect.

205 (c) The Public Utilities and Technology Interim Committee may make  
206 recommendations to the governor and to the chief information officer if the commission  
207 determines that the executive branch strategic plan should be modified or for any other reason  
208 should not take effect.

209 (d) Modifications adopted by the chief information officer shall be resubmitted to the  
210 governor and the Public Utilities and Technology Interim Committee for their review or  
211 approval as provided in Subsections (3)(a) and (b).

212 (4) (a) The chief information officer shall, on or before January 1, 2014, and each year  
213 thereafter, modify the executive branch information technology strategic plan to incorporate  
214 security standards that:

215 (i) are identified as industry best practices in accordance with Subsections  
216 63F-1-104(3) and (4); and

217 (ii) can be implemented within the budget of the department or the executive branch  
218 agencies.

219 (b) The chief information officer shall inform the speaker of the House of  
220 Representatives and the president of the Senate on or before January 1 of each year if best  
221 practices identified in Subsection (4)(a)(i) are not adopted due to budget issues considered  
222 under Subsection (4)(a)(ii).

223 [~~4~~] (5) The executive branch strategic plan is to be implemented by executive branch  
224 agencies through each executive branch agency adopting an agency information technology  
225 plan in accordance with Section 63F-1-204.

226 Section 5. Section **63F-1-204** is amended to read:

227 **63F-1-204. Agency information technology plans.**

228 (1) (a) By July 1 of each year, each executive branch agency shall submit an agency  
229 information technology plan to the chief information officer at the department level, unless the  
230 governor or the chief information officer request an information technology plan be submitted  
231 by a subunit of a department, or by an executive branch agency other than a department.

232 (b) The information technology plans required by this section shall be in the form and  
233 level of detail required by the chief information officer, by administrative rule adopted in  
234 accordance with Section 63F-1-206, and shall include, at least:

- 235 (i) the information technology objectives of the agency;
- 236 (ii) any performance measures used by the agency for implementing the agency's  
237 information technology objectives;
- 238 (iii) any planned expenditures related to information technology;
- 239 (iv) the agency's need for appropriations for information technology;
- 240 (v) how the agency's development of information technology coordinates with other  
241 state and local governmental entities;
- 242 (vi) any efforts the agency has taken to develop public and private partnerships to  
243 accomplish the information technology objectives of the agency; [~~and~~]
- 244 (vii) the efforts the executive branch agency has taken to conduct transactions  
245 electronically in compliance with Section 46-4-503[-]; and
- 246 (viii) the executive branch agency's plan for the timing and method of verifying the  
247 department's security standards, if an agency intends to verify the department's security  
248 standards for the data that the agency maintains or transmits through the department's servers.

249 (2) (a) Except as provided in Subsection (2)(b), an agency information technology plan  
250 described in Subsection (1) shall comply with the executive branch strategic plan established in  
251 accordance with Section 63F-1-203.

252 (b) If the executive branch agency submitting the agency information technology plan  
253 justifies the need to depart from the executive branch strategic plan, an agency information

254 technology plan may depart from the executive branch strategic plan to the extent approved by  
255 the chief information officer.

256 (3) (a) On receipt of a state agency information technology plan, the chief information  
257 officer shall forward a complete copy of the agency information technology plan to the  
258 Division of Enterprise Technology created in Section 63F-1-401 and the Division of Integrated  
259 Technology created in Section 63F-1-501.

260 (b) The divisions shall provide the chief information officer a written analysis of each  
261 agency plan submitted in accordance with ~~[Sections]~~ Subsections 63F-1-404(14) and  
262 63F-1-504(3).

263 (4) (a) The chief information officer shall review each agency plan to determine:

264 (i) (A) whether the agency plan complies with the executive branch strategic plan and  
265 state information architecture; or

266 (B) to the extent that the agency plan does not comply with the executive branch  
267 strategic plan or state information architecture, whether the executive branch entity is justified  
268 in departing from the executive branch strategic plan, or state information architecture; and

269 (ii) whether the agency plan meets the information technology and other needs of:

270 (A) the executive branch agency submitting the plan; and

271 (B) the state.

272 (b) In conducting the review required by Subsection (4)(a), the chief information  
273 officer shall consider the analysis submitted by the divisions under Subsection (3).

274 (5) After the chief information officer conducts the review described in Subsection (4)  
275 of an agency information technology plan, the chief information officer may:

276 (a) approve the agency information technology plan;

277 (b) disapprove the agency information technology plan; or

278 (c) recommend modifications to the agency information technology plan.

279 (6) An executive branch agency or the department may not submit a request for  
280 appropriation related to information technology or an information technology system to the  
281 governor in accordance with Section 63J-1-201 until after the executive branch agency's

282 information technology plan is approved by the chief information officer.

283 Section 6. Section **63F-1-604** is amended to read:

284 **63F-1-604. Duties of the division.**

285 The division shall:

286 (1) be responsible for providing support to executive branch agencies for an agency's  
287 information technology assets and functions that are unique to the executive branch agency and  
288 are mission critical functions of the agency;

289 (2) conduct audits of an executive branch agency when requested under the provisions  
290 of Section 63F-1-208;

291 (3) conduct cost-benefit analysis of delegating a department function to an agency in  
292 accordance with Section 63F-1-208;

293 (4) provide in-house information technology staff support to executive branch  
294 agencies;

295 (5) establish accountability and performance measures for the division to assure that  
296 the division is;

297 (a) meeting the business and service needs of the state and individual executive branch  
298 agencies; and

299 (b) implementing security standards in accordance with Subsection 63F-1-203(4);

300 (6) establish a committee composed of agency user groups for the purpose of  
301 coordinating department services with agency needs;

302 (7) assist executive branch agencies in complying with the requirements of any rule  
303 adopted by the chief information officer; and

304 (8) by July 1, [~~2006~~] 2013, and each July 1 thereafter, report to the Public Utilities and  
305 Technology Interim Committee on the performance measures used by the division under  
306 Subsection (5) and the results.