

**Proposed Substitute
Bill No. 5346**

LCO No. 2573

**AN ACT CONCERNING STATE AGENCY CONFIDENTIALITY BASED
ON A PROGRAM REVIEW AND INVESTIGATIONS COMMITTEE
STUDY.**

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

1 Section 1. (NEW) (*Effective from passage*) (a) For purposes of this
2 section: (1) "Confidential information" has the same meaning as
3 provided in section 4e-70 of the general statutes; and (2) "confidential
4 information breach" means an instance where an unauthorized person
5 or entity accesses confidential information in any manner, including,
6 but not limited to, the following occurrences: (A) Any confidential
7 information that is not encrypted or secured by any other method or
8 technology that renders the confidential information unreadable or
9 unusable is misplaced, lost, stolen or subject to unauthorized access;
10 (B) one or more third parties have accessed, or taken control or
11 possession of, without prior written authorization from the state, (i)
12 any confidential information that is not encrypted or protected, or (ii)
13 any encrypted or protected confidential information together with the
14 confidential process or key that is capable of compromising the
15 integrity of the confidential information; or (C) there is a substantial
16 risk of identity theft or fraud.

17 (b) Not later than October 1, 2016, the Commissioner of Public
18 Health shall develop and implement the use of a confidentiality pledge

19 for employees of the Department of Public Health concerning the use
20 and disclosure of confidential information. The confidentiality pledge
21 shall notify each employee of his or her responsibilities concerning the
22 use and disclosure of confidential information and potential
23 consequences for the misuse of such information or data under
24 applicable statutes, regulations and department policies. The
25 commissioner shall ensure that each employee of the department
26 receives and signs the confidentiality pledge on or before January 1,
27 2017, or, if hired after said date, on the first day of such employee's
28 employment with the department. The commissioner shall review and
29 revise the confidentiality pledge as the commissioner deems necessary.
30 Each employee of the department shall receive and sign any revised
31 confidentiality pledge not later than fifteen days after the date of such
32 revision.

33 (c) Not later than December 1, 2016, the Commissioner of Public
34 Health, in consultation with the Secretary of the Office of Policy and
35 Management, shall develop and implement internal policies to protect
36 confidential information obtained or generated by the department
37 from a confidential information breach. Such policies shall include, but
38 need not be limited to, processes to: (1) Identify computer system
39 vulnerabilities to a confidential data breach and eliminate or reduce
40 such vulnerabilities; (2) identify the occurrence of any confidential
41 information breach; (3) classify the severity of a confidential
42 information breach; (4) limit or contain the disclosure of confidential
43 information in the event of a confidential information breach; (5)
44 document each incident of a confidential information breach; and (6)
45 notify affected parties in the event of a confidential information breach.
46 Not later than December 31, 2016, the Commissioner of Public Health
47 shall submit a copy of such policies to the joint standing committee of
48 the General Assembly having cognizance of matters relating to public
49 health.

50 Sec. 2. (NEW) (*Effective from passage*) (a) For purposes of this section:
51 (1) "Confidential information" has the same meaning as provided in
52 section 4e-70 of the general statutes; and (2) "confidential information

53 breach" means an instance where an unauthorized person or entity
54 accesses confidential information in any manner, including, but not
55 limited to, the following occurrences: (A) Any confidential information
56 that is not encrypted or secured by any other method or technology
57 that renders the confidential information unreadable or unusable is
58 misplaced, lost, stolen or subject to unauthorized access; (B) one or
59 more third parties have accessed, or taken control or possession of,
60 without prior written authorization from the state, (i) any confidential
61 information that is not encrypted or protected, or (ii) any encrypted or
62 protected confidential information together with the confidential
63 process or key that is capable of compromising the integrity of the
64 confidential information; or (C) there is a substantial risk of identity
65 theft or fraud.

66 (b) Not later than October 1, 2016, the Commissioner of Consumer
67 Protection shall develop and implement the use of a confidentiality
68 pledge for employees of the Department of Consumer Protection
69 concerning the use and disclosure of confidential information. The
70 confidentiality pledge shall notify each employee of his or her
71 responsibilities concerning the use and disclosure of confidential
72 information and potential consequences for the misuse of such
73 information or data under applicable statutes, regulations and
74 department policies. The commissioner shall ensure that each
75 employee of the department receives and signs the confidentiality
76 pledge on or before January 1, 2017, or, if hired after said date, on the
77 first day of such employee's employment with the department. The
78 commissioner shall review and revise the confidentiality pledge as the
79 commissioner deems necessary. Each employee of the department
80 shall receive and sign any revised confidentiality pledge not later than
81 fifteen days after the date of such revision.

82 (c) Not later than December 1, 2016, the Commissioner of Consumer
83 Protection, in consultation with the Secretary of the Office of Policy
84 and Management, shall develop and implement internal policies to
85 protect confidential information obtained or generated by the
86 department from a confidential information breach. Such policies shall

87 include, but need not be limited to, processes to: (1) Identify computer
88 system vulnerabilities to a confidential data breach and eliminate or
89 reduce such vulnerabilities; (2) identify the occurrence of any
90 confidential information breach; (3) classify the severity of a
91 confidential information breach; (4) limit or contain the disclosure of
92 confidential information in the event of a confidential information
93 breach; (5) document each incident of a confidential information
94 breach; and (6) notify affected parties in the event of a confidential
95 information breach. Not later than December 31, 2016, the
96 Commissioner of Consumer Protection shall submit a copy of such
97 policies to the joint standing committee of the General Assembly
98 having cognizance of matters relating to general law.

This act shall take effect as follows and shall amend the following sections:		
Section 1	<i>from passage</i>	New section
Sec. 2	<i>from passage</i>	New section