



# House of Representatives

General Assembly

**File No. 485**

February Session, 2016

Substitute House Bill No. 5346

*House of Representatives, April 6, 2016*

The Committee on Public Health reported through REP. RITTER of the 1st Dist., Chairperson of the Committee on the part of the House, that the substitute bill ought to pass.

***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 any  
32 such 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 information breach and eliminate or  
40 reduce such vulnerabilities; (2) identify the occurrence of any  
41 confidential information breach; (3) classify the severity of a  
42 confidential information breach; (4) limit or contain the disclosure of  
43 confidential information in the event of a confidential information  
44 breach; (5) document each incident of a confidential information  
45 breach; and (6) notify affected parties in the event of a confidential  
46 information breach. Not later than December 31, 2016, the  
47 Commissioner of Public Health shall submit a copy of such policies to  
48 the joint standing committee of the General Assembly having

49 cognizance of matters relating to public 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 any such revision.



The following Fiscal Impact Statement and Bill Analysis are prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and do not represent the intent of the General Assembly or either chamber thereof for any purpose. In general, fiscal impacts are based upon a variety of informational sources, including the analyst's professional knowledge. Whenever applicable, agency data is consulted as part of the analysis, however final products do not necessarily reflect an assessment from any specific department.

***OFA Fiscal Note******State Impact:*** None***Municipal Impact:*** None***Explanation***

The bill, which concerns confidentiality procedures within the Departments of Public Health and Consumer Protection, results in no state fiscal impact as it is procedural in nature.

***The Out Years******State Impact:*** None***Municipal Impact:*** None

**OLR Bill Analysis**

**sHB 5346**

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

**SUMMARY:**

This bill requires the Department of Public Health (DPH) and Department of Consumer Protection (DCP) commissioners, by October 1, 2016, to each develop and implement the use of a confidentiality pledge for their departments' employees concerning the use and disclosure of confidential information.

It also requires the DPH and DCP commissioners to each develop and implement internal department policies to protect against a breach of confidential information the departments obtain or generate. Each commissioner must do so by December 1, 2016, and in consultation with the Office of Policy and Management secretary. The bill requires the commissioners, by December 31, 2016, to submit a copy of their policies to the Public Health and General Law committees, respectively.

EFFECTIVE DATE: Upon passage

**CONFIDENTIALITY PLEDGE**

Under the bill, the required confidentiality pledges must notify DPH or DCP employees of their responsibilities concerning the use and disclosure of confidential information and potential consequences for its misuse under applicable statutes, regulations, and department policies. The commissioners must ensure that their departments' employees each receive and sign the pledge (1) by January 1, 2017 or (2) if hired after that date, on the first day of the individual's employment.

Each commissioner must review and revise his department's confidentiality pledge as he deems necessary. If the commissioner revises the pledge, the department's employees must receive and sign the revised form within 15 days.

### **POLICIES TO PROTECT AGAINST CONFIDENTIAL INFORMATION BREACH**

The bill's required policies must include processes to (1) identify features of the department's computer system that are vulnerable to a confidential information breach and (2) eliminate or reduce these vulnerabilities. They must also include processes to do the following in the event of a breach:

1. identify and document when a breach occurs,
2. classify its severity,
3. limit or contain the disclosure of confidential information, and
4. notify affected parties.

### **DEFINITIONS**

By law and under the bill, "confidential information" is:

1. a person's name, date of birth, or mother's maiden name;
2. specified identification numbers (e.g., Social Security or credit or debit card numbers);
3. unique biometric data (e.g., fingerprints);
4. "personally identifiable information" and "protected health information," as defined in federal education and patient data privacy regulations, respectively; or
5. information that a state contracting agency tells the contractor is confidential.

The term does not include information that may be lawfully

obtained from public sources or from federal, state, or local government records lawfully made available to the general public (CGS § 4e-70).

Under the bill, a “confidential information breach” is an instance where an unauthorized person or entity accesses confidential information. This includes instances in which:

1. confidential information not encrypted or secured by any method or technology that makes the information unreadable or unusable is misplaced, lost, stolen, or subject to unauthorized access;
2. a third party, without prior written state authorization, accesses or takes control or possession of (a) unencrypted or unprotected confidential information or (b) encrypted or protected confidential information along with the confidential process or key capable of compromising its integrity; or
3. there is a substantial risk of identity theft or fraud.

**COMMITTEE ACTION**

Program Review and Investigations Committee

Joint Favorable Substitute Change of Reference  
Yea 10 Nay 0 (03/07/2016)

Public Health Committee

Joint Favorable  
Yea 28 Nay 0 (03/21/2016)