

THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 1048 Session of 2015

INTRODUCED BY VULAKOVICH, SCARNATI, AUMENT, BROWNE, COSTA, FARNESE, FOLMER, FONTANA, GORDNER, GREENLEAF, HAYWOOD, HUGHES, PILEGGI, RAFFERTY, SCAVELLO, SCHWANK, STEFANO, VOGEL, WARD AND BREWSTER, OCTOBER 26, 2015

SENATOR BROWNE, APPROPRIATIONS, RE-REPORTED AS AMENDED, SEPTEMBER 26, 2016

AN ACT

1 Amending the act of December 22, 2005 (P.L.474, No.94), entitled
2 "An act providing for the notification of residents whose
3 personal information data was or may have been disclosed due
4 to a security system breach; and imposing penalties," further
5 providing for title of act, for definitions and for
6 notification of breach; prohibiting employees of the
7 Commonwealth from using nonsecured Internet connections; and
8 providing for ENCRYPTION REQUIRED, FOR Commonwealth policy <--
9 AND FOR ENTITIES SUBJECT TO THE HEALTH INSURANCE PORTABILITY <--
10 AND ACCOUNTABILITY ACT OF 1996.

11 The General Assembly of the Commonwealth of Pennsylvania
12 hereby enacts as follows:

13 Section 1. The title of the act of December 22, 2005
14 (P.L.474, No.94), known as the Breach of Personal Information
15 Notification Act, is amended to read:

AN ACT

17 Providing for security of computerized data and for the
18 notification of residents whose personal information data was
19 or may have been disclosed due to a security system breach;
20 and imposing penalties.

1 Section 2. The definition of "personal information" in
2 section 2 of the act is amended AND THE SECTION IS AMENDED BY <--
3 ADDING DEFINITIONS to read:

4 Section 2. Definitions.

5 The following words and phrases when used in this act shall
6 have the meanings given to them in this section unless the
7 context clearly indicates otherwise:

8 * * * <--

9 "HEALTH INSURANCE INFORMATION." AN INDIVIDUAL'S HEALTH
10 INSURANCE POLICY NUMBER OR SUBSCRIBER IDENTIFICATION NUMBER OR
11 ANY MEDICAL INFORMATION IN AN INDIVIDUAL'S INSURANCE APPLICATION
12 AND CLAIMS HISTORY, INCLUDING ANY APPEALS RECORDS.

13 * * *

14 "MEDICAL INFORMATION." ANY INDIVIDUALLY IDENTIFIABLE
15 INFORMATION CONTAINED IN OR DERIVED FROM THE INDIVIDUAL'S
16 CURRENT OR HISTORICAL RECORD OF MEDICAL HISTORY OR MEDICAL
17 TREATMENT OR DIAGNOSIS CREATED BY A HEALTH CARE PROFESSIONAL.

18 * * *

19 "Personal information."

20 (1) An individual's first name or first initial and last
21 name in combination with and linked to any one or more of the
22 following data elements when the data elements are not
23 encrypted or redacted:

24 (i) Social Security number.

25 (ii) Driver's license number or a State
26 identification card number issued in lieu of a driver's
27 license.

28 (iii) Financial account number, credit or debit card
29 number, in combination with any required security code,
30 access code or password that would permit access to an

1 individual's financial account.

2 (iv) Medical information.

3 (v) Health insurance information.

4 (vi) A user name or e-mail address, in combination
5 with a password or security question and answer that
6 would permit access to an online account.

7 (2) The term does not include publicly available
8 information that is lawfully made available to the general
9 public from Federal, State or local government records.

10 * * *

11 Section 3. Section 3 of the act is amended by adding
12 subsections to read:

13 Section 3. Notification of breach.

14 * * *

15 (a.1) Notification by State agency.--If a State agency is
16 the subject of a breach of security of the system, the State
17 agency shall provide notice of the breach of security of the
18 system required under subsection (a) within seven days following
19 discovery of the breach. Notification shall be provided to the
20 Office of Attorney General within three business days following
21 discovery of the breach. A State agency under the Governor's
22 jurisdiction shall also provide notice of a breach of security
23 of the system to the Governor's Office of Administration within
24 three business days following the discovery of the breach.
25 Notification shall occur regardless of the existence of
26 procedures and policies under section 7.

27 (a.2) Notification by county, school district or
28 municipality.--If a county, school district or municipality is
29 the subject of a breach of security of the system, the county,
30 school district or municipality shall provide notice of the

1 breach of security of the system required under subsection (a)
2 within seven days following discovery of the breach.
3 Notification shall be provided to the district attorney in the
4 county in which the breach occurred within three business days
5 following discovery of the breach. Notification shall occur
6 regardless of the existence of procedures and policies under
7 section 7.

8 (A.3) ELECTRONIC NOTIFICATION.--IN THE CASE OF A BREACH OF <--
9 THE SECURITY OF THE SYSTEM INVOLVING PERSONAL INFORMATION
10 DEFINED IN SECTION 2 FOR A USERNAME OR E-MAIL ADDRESS IN
11 COMBINATION WITH A PASSWORD OR SECURITY QUESTION AND ANSWER THAT
12 WOULD PERMIT ACCESS TO AN ONLINE ACCOUNT, THE PERSON OR BUSINESS
13 MAY COMPLY WITH THIS SECTION BY PROVIDING THE SECURITY BREACH
14 NOTIFICATION IN ELECTRONIC OR OTHER FORM THAT DIRECTS THE PERSON
15 WHOSE PERSONAL INFORMATION HAS BEEN BREACHED TO PROMPTLY CHANGE
16 THE PERSON'S PASSWORD AND SECURITY QUESTION OR ANSWER, AS
17 APPLICABLE, OR TO TAKE OTHER STEPS APPROPRIATE TO PROTECT THE
18 ONLINE ACCOUNT WITH THE PERSON OR BUSINESS AND ALL OTHER ONLINE
19 ACCOUNTS FOR WHICH THE PERSON WHOSE PERSONAL INFORMATION HAS
20 BEEN BREACHED USES THE SAME USERNAME OR E-MAIL ADDRESS AND
21 PASSWORD OR SECURITY QUESTION OR ANSWER.

22 * * *

23 Section 4. The act is amended by adding sections to read:
24 Section 5.1. Encryption required.

25 (a) General rule.--Employees and contractors of the
26 Commonwealth shall, while performing the employee's or <--
27 contractor's duties WORKING WITH PERSONAL INFORMATION ON BEHALF <--
28 OF THE COMMONWEALTH or otherwise conducting official business on
29 behalf of the Commonwealth, utilize encryption to protect the
30 transmission of personal information over the Internet from

1 being viewed or modified by a third party.

2 (b) Transmission policy.--The Governor's Office of
3 Administration shall develop and maintain a policy to govern the
4 proper encryption and transmission by State agencies under the
5 Governor's jurisdiction of data which includes personal
6 information.

7 Section 5.2. Commonwealth policy.

8 (a) Storage policy.--The Governor's Office of Administration
9 shall develop a policy to govern the proper storage by State
10 agencies under the Governor's jurisdiction of data which
11 includes personal information. The policy shall address
12 identifying, collecting, maintaining, displaying and
13 transferring personally identifiable information, using
14 personally identifiable information in test environments,
15 remediating personally identifiable information stored on legacy
16 systems and other relevant issues. A goal of the policy shall be
17 to reduce the risk of future breaches of security of the system.

18 (b) Considerations.--In developing the policy, the
19 Governor's Office of Administration shall consider similar
20 existing policies in other states, best practices identified by
21 other states and relevant studies and other sources as
22 appropriate.

23 (c) Review and update.--The policy shall be reviewed at
24 least annually and updated as necessary.

25 SECTION 5.3. ENTITIES SUBJECT TO THE HEALTH INSURANCE

<--

26 PORTABILITY AND ACCOUNTABILITY ACT OF 1996.

27 ANY COVERED ENTITY OR BUSINESS ASSOCIATE THAT IS SUBJECT TO
28 AND IN COMPLIANCE WITH THE PRIVACY AND SECURITY STANDARDS FOR
29 THE PROTECTION OF ELECTRONIC HEALTH INFORMATION ESTABLISHED
30 UNDER THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF

1 1996 (PUBLIC LAW 104-191, 110 STAT. 1936) AND THE HEALTH
2 INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT
3 (PUBLIC LAW 115-5, 123 STAT. 226-279 AND 467-496) SHALL BE
4 DEEMED TO BE IN COMPLIANCE WITH THE PROVISIONS OF THIS ACT.

5 Section 5. This act shall take effect in 60 days.