
THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 487 Session of
2019

INTRODUCED BY LAUGHLIN, STEFANO, GORDNER, BREWSTER, FOLMER,
K. WARD, BARTOLOTTA, SCARNATI, COSTA, MENSCH, J. WARD, BROWNE
AND HAYWOOD, MARCH 28, 2019

REFERRED TO COMMUNICATIONS AND TECHNOLOGY, MARCH 28, 2019

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 Commonwealth policy and for entities subject to
9 the Health Insurance Portability and Accountability Act of
10 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:

16 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.

21 Section 2. The definition of "personal information" in

1 section 2 of the act is amended and the section is amended by
2 adding definitions to read:

3 Section 2. Definitions.

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

7 * * *

8 "Health insurance information." An individual's health
9 insurance policy number or subscriber identification number or
10 any medical information in an individual's insurance application
11 and claims history, including any appeals records.

12 * * *

13 "Medical information." Any individually identifiable
14 information contained in or derived from the individual's
15 current or historical record of medical history or medical
16 treatment or diagnosis created by a health care professional.

17 * * *

18 "Personal information."

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

23 (i) Social Security number.

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

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

- 1 (iv) Medical information.
2 (v) Health insurance information.
3 (vi) A user name or e-mail address, in combination
4 with a password or security question and answer that
5 would permit access to an online account.

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

9 * * *

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

12 Section 3. Notification of breach.

13 * * *

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

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

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

7 (a.3) Electronic notification.--In the case of a breach of
8 the security of the system involving personal information
9 defined in section 2 for a user name or e-mail address in
10 combination with a password or security question and answer that
11 would permit access to an online account, the person or business
12 may comply with this section by providing the security breach
13 notification in electronic or other form that directs the person
14 whose personal information has been breached to promptly change
15 the person's password and security question or answer, as
16 applicable, or to take other steps appropriate to protect the
17 online account with the person or business and all other online
18 accounts for which the person whose personal information has
19 been breached uses the same user name or e-mail address and
20 password or security question or answer.

21 * * *

22 Section 4. The act is amended by adding sections to read:

23 Section 5.1. Encryption required.

24 (a) General rule.--Employees and contractors of the
25 Commonwealth shall, while working with personal information on
26 behalf of the Commonwealth or otherwise conducting official
27 business on behalf of the Commonwealth, utilize encryption to
28 protect the transmission of personal information over the
29 Internet from being viewed or modified by a third party.

30 (b) Transmission policy.--The Governor's Office of

1 Administration shall develop and maintain a policy to govern the
2 proper encryption and transmission by State agencies under the
3 Governor's jurisdiction of data which includes personal
4 information.

5 Section 5.2. Commonwealth policy.

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

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

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

23 Section 5.3. Entities subject to the Health Insurance
24 Portability and Accountability Act of 1996.

25 Any covered entity or business associate that is subject to
26 and in compliance with the privacy and security standards for
27 the protection of electronic health information established
28 under the Health Insurance Portability and Accountability Act of
29 1996 (Public Law 104-191, 110 Stat. 1936) and the Health
30 Information Technology for Economic and Clinical Health Act

1 (Public Law 111-5, 123 Stat. 226-279 and 467-496) shall be
2 deemed to be in compliance with the provisions of this act.

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