PRINTER'S NO. 322

THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 308 Session of 2017

INTRODUCED BY VULAKOVICH, SCARNATI, AUMENT, BREWSTER, BROWNE, COSTA, DiSANTO, FARNESE, FOLMER, GORDNER, GREENLEAF, HAYWOOD, HUGHES, LAUGHLIN, McGARRIGLE, RAFFERTY, RESCHENTHALER, SABATINA, SCAVELLO, SCHWANK, STEFANO, TARTAGLIONE AND WARD, FEBRUARY 15, 2017

REFERRED TO COMMUNICATIONS AND TECHNOLOGY, FEBRUARY 15, 2017

AN ACT

Amending the act of December 22, 2005 (P.L.474, No.94), entitled "An act providing for the notification of residents whose personal information data was or may have been disclosed due to a security system breach; and imposing penalties," further providing for title of act, for definitions and for notification of breach; prohibiting employees of the Commonwealth from using nonsecured Internet connections; and providing for Commonwealth policy and for entities subject to the Health Insurance Portability and Accountability Act of 1996.

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

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

AN ACT

Providing <u>for security of computerized data and</u> for the notification of residents whose personal information data was or may have been disclosed due to a security system breach; and imposing penalties.

Section 2. The definition of "personal information" in section 2 of the act is amended and the section is amended by adding definitions to read:

Section 2. Definitions.

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

* * *

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

* * *

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

* * *

"Personal information."

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

(i) Social Security number.

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

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

individual's financial account.

(iv) Medical information.

(v) Health insurance information.

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

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

* * *

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

Section 3. Notification of breach.

* * *

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

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

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

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

* * *

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

Section 5.1. Encryption required.

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

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

Section 5.2. Commonwealth policy.

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

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

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

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

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

Information Technology for Economic and Clinical Health Act (Public Law 115-5, 123 Stat. 226-279 and 467-496) shall be deemed to be in compliance with the provisions of this act.

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