HOUSE AMENDED

PRIOR PRINTER'S NOS. 775, 793, 1330, 1779

PRINTER'S NO. 2007

THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 696 Session of 2021

INTRODUCED BY LAUGHLIN, BARTOLOTTA, STEFANO, J. WARD, HAYWOOD AND BROOKS, MAY 19, 2021

AS AMENDED ON SECOND CONSIDERATION, HOUSE OF REPRESENTATIVES, OCTOBER 25, 2022

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; providing for ~~Commonwealth~~ DATA STORAGE policy and for entities subject to the Health Insurance Portability and Accountability Act of 1996; and further providing for notice exemption AND FOR APPLICABILITY. <--

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 <u>of the security OF THE system</u>; and imposing penalties. <--

Section 2. The ~~definition of~~ DEFINITIONS OF "NOTICE" AND "personal information" in section 2 of the act ~~is~~ ARE 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:

* * *

"DETERMINATION." A VERIFICATION OR REASONABLE CERTAINTY THAT A BREACH OF THE SECURITY OF THE SYSTEM HAS OCCURRED. <--

"DISCOVERY." THE KNOWLEDGE OF OR REASONABLE SUSPICION THAT A BREACH OF THE SECURITY OF THE SYSTEM HAS OCCURRED.

* * *

"Health insurance information." An individual's health insurance policy number or subscriber identification number in combination with access code or other medical information that permits misuse of an individual's health insurance benefits.

* * *

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

~~* * *~~ <--

"NOTICE." MAY BE PROVIDED BY ANY OF THE FOLLOWING METHODS OF NOTIFICATION: <--

(1) WRITTEN NOTICE TO THE LAST KNOWN HOME ADDRESS FOR THE INDIVIDUAL.

(2) TELEPHONIC NOTICE, IF THE [CUSTOMER] INDIVIDUAL CAN BE REASONABLY EXPECTED TO RECEIVE IT AND THE NOTICE IS GIVEN IN A CLEAR AND CONSPICUOUS MANNER, DESCRIBES THE INCIDENT IN

GENERAL TERMS AND VERIFIES PERSONAL INFORMATION BUT DOES NOT REQUIRE THE [CUSTOMER] INDIVIDUAL TO PROVIDE PERSONAL INFORMATION AND THE [CUSTOMER] INDIVIDUAL IS PROVIDED WITH A TELEPHONE NUMBER TO CALL OR INTERNET WEBSITE TO VISIT FOR FURTHER INFORMATION OR ASSISTANCE.

(3) E-MAIL NOTICE, IF A PRIOR BUSINESS RELATIONSHIP EXISTS AND THE PERSON OR ENTITY HAS A VALID E-MAIL ADDRESS FOR THE INDIVIDUAL.

(3.1) ELECTRONIC NOTICE, IF THE NOTICE DIRECTS THE PERSON WHOSE PERSONAL INFORMATION HAS BEEN MATERIALLY COMPROMISED BY A BREACH OF THE SECURITY OF THE SYSTEM TO PROMPTLY CHANGE THE PERSON'S PASSWORD AND SECURITY QUESTION OR ANSWER, AS APPLICABLE OR TO TAKE OTHER STEPS APPROPRIATE TO PROTECT THE PERSON'S ONLINE ACCOUNT TO THE EXTENT THE ENTITY HAS SUFFICIENT CONTACT INFORMATION FOR THE PERSON.

(4) (I) SUBSTITUTE NOTICE, IF THE ENTITY DEMONSTRATES ONE OF THE FOLLOWING:

(A) THE COST OF PROVIDING NOTICE WOULD EXCEED $100,000.

(B) THE AFFECTED CLASS OF SUBJECT PERSONS TO BE NOTIFIED EXCEEDS 175,000.

(C) THE ENTITY DOES NOT HAVE SUFFICIENT CONTACT INFORMATION.

(II) SUBSTITUTE NOTICE SHALL CONSIST OF ALL OF THE FOLLOWING:

(A) E-MAIL NOTICE WHEN THE ENTITY HAS AN E-MAIL ADDRESS FOR THE SUBJECT PERSONS.

(B) CONSPICUOUS POSTING OF THE NOTICE ON THE ENTITY'S INTERNET WEBSITE IF THE ENTITY MAINTAINS ONE.

(C) NOTIFICATION TO MAJOR STATEWIDE MEDIA.

"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 OR WIDELY DISTRIBUTED MEDIA. <--

* * *

~~"State agency contractor." A person that has a contract with a State agency for goods or services and a third-party subcontractor that provides goods or services for the fulfillment of the contract.~~

~~"STATE AGENCY CONTRACTOR." A PERSON OR BUSINESS THAT HAS A CONTRACT WITH A STATE AGENCY FOR GOODS OR SERVICES AND A THIRD-~~ <--

~~PARTY SUBCONTRACTOR THAT PROVIDES THE GOODS OR SERVICES FOR THE FULFILLMENT OF THE CONTRACT OR A PERSON OR BUSINESS THAT IS A SUBCONTRACTOR PROVIDING GOODS OR SERVICES TO ONE OR MORE STATE AGENCIES, THE PERFORMANCE OF WHICH WILL REQUIRE ACCESS TO PERSONAL INFORMATION.~~

"STATE AGENCY CONTRACTOR." A PERSON, BUSINESS, SUBCONTRACTOR OR THIRD PARTY SUBCONTRACTOR THAT HAS A CONTRACT WITH A STATE AGENCY FOR GOODS OR SERVICES THAT REQUIRES ACCESS TO PERSONAL INFORMATION FOR THE FULFILLMENT OF THE CONTRACT. <--

Section 3. Section ~~3 of the act is amended~~ 3 HEADING, (A) AND (C) OF THE ACT ARE AMENDED AND THE SECTION IS AMENDED by adding subsections to read: <--

Section 3. Notification of THE breach OF THE SECURITY OF THE SYSTEM. <--

~~* * *~~ <--

(A) GENERAL RULE.--AN ENTITY THAT MAINTAINS, STORES OR MANAGES COMPUTERIZED DATA THAT INCLUDES PERSONAL INFORMATION SHALL PROVIDE NOTICE OF ANY BREACH OF THE SECURITY OF THE SYSTEM FOLLOWING [DISCOVERY] DETERMINATION OF THE BREACH OF THE SECURITY OF THE SYSTEM TO ANY RESIDENT OF THIS COMMONWEALTH WHOSE UNENCRYPTED AND UNREDACTED PERSONAL INFORMATION WAS OR IS REASONABLY BELIEVED TO HAVE BEEN ACCESSED AND ACQUIRED BY AN UNAUTHORIZED PERSON. EXCEPT AS PROVIDED IN SECTION 4 OR IN ORDER TO TAKE ANY MEASURES NECESSARY TO DETERMINE THE SCOPE OF THE BREACH AND TO RESTORE THE REASONABLE INTEGRITY OF THE DATA SYSTEM, THE NOTICE SHALL BE MADE WITHOUT UNREASONABLE DELAY. FOR THE PURPOSE OF THIS SECTION, A RESIDENT OF THIS COMMONWEALTH MAY BE DETERMINED TO BE AN INDIVIDUAL WHOSE PRINCIPAL MAILING ADDRESS, AS REFLECTED IN THE COMPUTERIZED DATA WHICH IS MAINTAINED, STORED OR MANAGED BY THE ENTITY, IS IN THIS

COMMONWEALTH.

(a.1) Notification by State agency or State agency contractor.--

~~(1) If a State agency determines that it is the subject of a breach affecting personal information of the Commonwealth maintained by the State or State agency contractor, the State agency shall provide notice of the breach required under subsection (a) within seven days following determination of the breach or notification by a State agency contractor as provided under paragraph (2). Notification shall be provided concurrently to the Office of Attorney General.~~ <--

~~(2) (1)~~ (1) IF A STATE AGENCY DETERMINES THAT IT IS THE SUBJECT OF A BREACH OF THE SECURITY OF THE SYSTEM AFFECTING PERSONAL INFORMATION MAINTAINED BY THE STATE AGENCY OR STATE AGENCY CONTRACTOR, THE STATE AGENCY SHALL PROVIDE NOTICE OF THE BREACH OF THE SECURITY OF THE SYSTEM REQUIRED UNDER SUBSECTION (A) WITHIN SEVEN BUSINESS DAYS FOLLOWING DETERMINATION OF THE BREACH OF THE SECURITY OF THE SYSTEM. NOTIFICATION SHALL BE PROVIDED CONCURRENTLY TO THE OFFICE OF ATTORNEY GENERAL. <--

(2) A State agency contractor shall, UPON DISCOVERY OF THE BREACH OF THE SECURITY OF THE SYSTEM, notify the chief information security officer, or a designee, of the State agency ~~for whom the work is performed of a~~ AFFECTED BY THE STATE AGENCY CONTRACTOR'S breach of the security of the system ~~within seven business days following determination~~ ~~DISCOVERY~~ AS SOON AS REASONABLY PRACTICAL, BUT NO LATER THAN THE TIME PERIOD SPECIFIED IN THE APPLICABLE TERMS OF THE CONTRACT BETWEEN THE STATE AGENCY CONTRACTOR AND THE STATE <-- <-- <--

AGENCY of the breach OF THE SECURITY OF THE SYSTEM. <--

~~(3) (2)~~ (3) A State agency under the Governor's <--
jurisdiction shall also provide notice of a breach of the security of the system to the Governor's Office of Administration ~~AND THE OFFICE OF ATTORNEY GENERAL~~ within <--
three business days following the determination of the breach OF THE SECURITY OF THE SYSTEM. Notification shall occur <--
notwithstanding the existence of procedures and policies under section 7.

~~(4) (3) A State agency that, on the effective date of this section, has an existing contract with a State agency contractor shall use reasonable efforts to amend the contract to include provisions relating to the State agency contractor's compliance with this act unless the existing contract already contains breach of the security of the system notification requirements.~~ <--

~~(5) (4)~~ (4) A State agency that, after the effective <--
date of this section, enters into a contract WHICH INVOLVES <--
THE USE OF PERSONAL INFORMATION with a State agency contractor shall ensure that the contract includes provisions relating to the State agency contractor's compliance with this act.

(a.2) Notification by county, ~~school district~~ PUBLIC SCHOOL <--
or municipality.--If a county, ~~school district~~ PUBLIC SCHOOL or <--
municipality is the subject of a breach of the security of the system, the county, ~~school district~~ PUBLIC SCHOOL or <--
municipality shall provide notice of the breach of the security of the system required under subsection (a) within seven BUSINESS days following determination of the breach OF THE <--
SECURITY OF THE SYSTEM. Notification shall be provided to the

district attorney in the county where the breach OF THE SECURITY OF THE SYSTEM occurred within three business days following determination of the breach OF THE SECURITY OF THE SYSTEM. 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 for 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, the ~~State agency, county, school district PUBLIC SCHOOL or municipality~~ ENTITY, to the extent that it has sufficient contact information for the person, may comply with this section by providing the breach of the security of the system notification in electronic or other form that directs the person whose personal information has been ~~breached~~ MATERIALLY COMPROMISED BY THE BREACH OF THE SECURITY OF THE SYSTEM 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 ~~State agency, county, school district PUBLIC SCHOOL or municipality~~ ENTITY and other online accounts for which the person whose personal information has been ~~breached~~ MATERIALLY COMPROMISED BY THE BREACH OF THE SECURITY OF THE SYSTEM uses the same user name or e-mail address and password or security question or answer.

(a.4) Affected individuals.--In the case of a breach of the security of the system involving personal information ~~for a user~~ OF AN INDIVIDUAL'S USER name or e-mail address in combination with a password or security question and answer that would permit access to an online account, the State agency contractor may comply with this section by providing a list of affected

residents of this Commonwealth AND THEIR VALID E-MAIL ADDRESSES, <-- if known, to the State agency subject of the breach of the security of the system.

* * *

(C) VENDOR NOTIFICATION.--A VENDOR THAT MAINTAINS, STORES OR <-- MANAGES COMPUTERIZED DATA ON BEHALF OF ANOTHER ENTITY SHALL PROVIDE NOTICE OF ANY BREACH OF THE SECURITY OF THE SYSTEM FOLLOWING DISCOVERY BY THE VENDOR TO THE ENTITY ON WHOSE BEHALF THE VENDOR MAINTAINS, STORES OR MANAGES THE DATA. THE ENTITY SHALL BE RESPONSIBLE FOR MAKING THE DETERMINATIONS AND DISCHARGING ANY REMAINING DUTIES UNDER THIS ACT.

(D) DEFINITIONS.--AS USED IN THIS SECTION, THE TERM "PUBLIC <-- SCHOOL" MEANS ANY SCHOOL DISTRICT, INTERMEDIATE UNIT, CHARTER SCHOOL, CYBER CHARTER SCHOOL OR AREA CAREER AND TECHNICAL SCHOOL.

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

Section 5.1. Encryption required.

~~(a) General rule. State employees and State agency contractor employees shall, while working with personal information on behalf of the Commonwealth or otherwise conducting official business on behalf of the Commonwealth, utilize encryption, OR OTHER APPROPRIATE SECURITY MEASURES, to protect the transmission of personal information over the Internet from being viewed or modified by an unauthorized third party IN ACCORDANCE WITH THE GOVERNOR'S OFFICE OF ADMINISTRATION POLICY UNDER SUBSECTION (B).~~ <--

~~(b) Transmission policy. The Governor's Office of Administration shall develop and maintain a policy to govern the proper encryption and transmission OF DATA, WHICH INCLUDES PERSONAL INFORMATION, by State agencies under the Governor's~~ <--

~~jurisdiction of data which includes personal information.~~ <--

~~(C) CONSIDERATIONS.--IN DEVELOPING THE POLICY, THE~~ <--
~~GOVERNOR'S OFFICE OF ADMINISTRATION SHALL CONSIDER SIMILAR~~
~~EXISTING FEDERAL AND OTHER POLICIES IN OTHER STATES, BEST~~
~~PRACTICES IDENTIFIED BY OTHER STATES AND RELEVANT STUDIES AND~~
~~OTHER SOURCES AS APPROPRIATE.~~

~~(D) REVIEW AND UPDATE.--THE POLICY SHALL BE REVIEWED AT~~
~~LEAST ANNUALLY AND UPDATED AS NECESSARY.~~

~~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 personal information, using personal information in~~
~~test environments, remediating personal information stored on~~
~~legacy systems and other relevant issues. A goal of the policy~~
~~shall be to reduce the risk of future breaches of the security~~
~~of the system.~~

~~(b) Considerations.--In developing the policy, the~~ <--
~~Governor's Office of Administration shall consider similar~~
~~existing Federal and other 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.~~

(A) GENERAL RULE.--AN ENTITY THAT MAINTAINS, STORES OR <--
MANAGES COMPUTERIZED DATA ON BEHALF OF THE COMMONWEALTH THAT
CONSTITUTES PERSONAL INFORMATION SHALL UTILIZE ENCRYPTION, OR
OTHER APPROPRIATE SECURITY MEASURES, TO REASONABLY PROTECT THE

TRANSMISSION OF PERSONAL INFORMATION OVER THE INTERNET FROM BEING VIEWED OR MODIFIED BY AN UNAUTHORIZED THIRD PARTY.

(B) TRANSMISSION POLICY.--AN ENTITY THAT MAINTAINS, STORES OR MANAGES COMPUTERIZED DATA ON BEHALF OF THE COMMONWEALTH THAT CONSTITUTES PERSONAL INFORMATION SHALL DEVELOP AND MAINTAIN A POLICY TO GOVERN THE PROPER ENCRYPTION OR OTHER APPROPRIATE SECURITY MEASURES AND TRANSMISSION OF DATA BY STATE AGENCIES.

(C) CONSIDERATIONS.--IN DEVELOPING THE POLICY, AN ENTITY SHALL REASONABLY CONSIDER SIMILAR EXISTING FEDERAL POLICIES AND OTHER POLICIES, BEST PRACTICES IDENTIFIED BY OTHER STATES AND RELEVANT STUDIES AND OTHER SOURCES AS APPROPRIATE IN ACCORDANCE WITH BEST PRACTICES AS ESTABLISHED BY THE FEDERAL GOVERNMENT AND THE COMMONWEALTH.

(D) REVIEW AND UPDATE.--THE POLICY SHALL BE REVIEWED AT LEAST ANNUALLY AND UPDATED AS NECESSARY.

SECTION 5.2. DATA STORAGE POLICY.

(A) STORAGE POLICY.--AN ENTITY THAT MAINTAINS, STORES OR MANAGES COMPUTERIZED DATA ON BEHALF OF THE COMMONWEALTH THAT CONSTITUTES PERSONAL INFORMATION SHALL DEVELOP A POLICY TO GOVERN REASONABLY PROPER STORAGE OF THE PERSONAL INFORMATION. A GOAL OF THE POLICY SHALL BE TO REDUCE THE RISK OF FUTURE BREACHES OF THE SECURITY OF THE SYSTEM.

(B) CONSIDERATIONS.--IN DEVELOPING THE POLICY, AN ENTITY SHALL REASONABLY CONSIDER SIMILAR EXISTING FEDERAL POLICIES AND OTHER POLICIES, BEST PRACTICES IDENTIFIED BY OTHER STATES AND RELEVANT STUDIES AND OTHER SOURCES AS APPROPRIATE IN ACCORDANCE WITH BEST PRACTICES AS ESTABLISHED BY THE FEDERAL GOVERNMENT AND THE COMMONWEALTH.

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

Section 5. ~~Section 7(b)(2) of the act is amended to read:~~ <--

SECTIONS 7(B)(2) AND 29 OF THE ACT ARE AMENDED TO READ: <--

Section 7. Notice exemption.

* * *

(b) Compliance with Federal requirements.--

* * *

(2) An entity, a State agency ~~or State agency contractor~~ <--
OR A STATE AGENCY'S CONTRACTOR, that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the entity's ~~State agency or State agency contractor's~~, STATE <--
AGENCY'S OR STATE AGENCY'S CONTRACTOR'S primary STATE or <--
functional Federal regulator, shall be in compliance with <--
this act.

SECTION 29. APPLICABILITY. <--

THIS ACT SHALL APPLY TO THE [DISCOVERY] DETERMINATION OR NOTIFICATION OF A BREACH [IN] OF THE SECURITY OF [PERSONAL INFORMATION DATA] THE SYSTEM THAT OCCURS ON OR AFTER THE EFFECTIVE DATE OF THIS SECTION.

Section 6. This act shall take effect in ~~120~~ 180 days. **<--**