

---

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

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

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

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

17 AN ACT

18 Providing for security of computerized data and for the  
19 notification of residents whose personal information data was  
20 or may have been disclosed due to a [security system] breach  
21 of the security OF THE system; and imposing penalties. <--

1 Section 2. The ~~definition of~~ DEFINITIONS OF "NOTICE" AND <--  
2 "personal information" in section 2 of the act ~~is~~ ARE amended <--  
3 and the section is amended by 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 "DETERMINATION." A VERIFICATION OR REASONABLE CERTAINTY THAT <--  
10 A BREACH OF THE SECURITY OF THE SYSTEM HAS OCCURRED.

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

13 \* \* \*

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

18 \* \* \*

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

23 \* \* \* <--

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

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

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

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

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

9 (3.1) ELECTRONIC NOTICE, IF THE NOTICE DIRECTS THE  
10 PERSON WHOSE PERSONAL INFORMATION HAS BEEN MATERIALLY  
11 COMPROMISED BY A BREACH OF THE SECURITY OF THE SYSTEM TO  
12 PROMPTLY CHANGE THE PERSON'S PASSWORD AND SECURITY QUESTION  
13 OR ANSWER, AS APPLICABLE OR TO TAKE OTHER STEPS APPROPRIATE  
14 TO PROTECT THE PERSON'S ONLINE ACCOUNT TO THE EXTENT THE  
15 ENTITY HAS SUFFICIENT CONTACT INFORMATION FOR THE PERSON.

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

18 (A) THE COST OF PROVIDING NOTICE WOULD EXCEED  
19 \$100,000.

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

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

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

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

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

1 (C) NOTIFICATION TO MAJOR STATEWIDE MEDIA.

2 "Personal information."

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

7 (i) Social Security number.

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

11 (iii) Financial account number, credit or debit card  
12 number, in combination with any required security code,  
13 access code or password that would permit access to an  
14 individual's financial account.

15 (iv) Medical information.

16 (v) Health insurance information.

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

20 (2) The term does not include publicly available  
21 information that is lawfully made available to the general  
22 public from Federal, State or local government records OR <--  
23 WIDELY DISTRIBUTED MEDIA.

24 \* \* \*

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

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

~~1 PARTY SUBCONTRACTOR THAT PROVIDES THE GOODS OR SERVICES FOR THE~~  
~~2 FULFILLMENT OF THE CONTRACT OR A PERSON OR BUSINESS THAT IS A~~  
~~3 SUBCONTRACTOR PROVIDING GOODS OR SERVICES TO ONE OR MORE STATE~~  
~~4 AGENCIES, THE PERFORMANCE OF WHICH WILL REQUIRE ACCESS TO~~  
~~5 PERSONAL INFORMATION.~~

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

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

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

15 \* \* \* <--

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

1 COMMONWEALTH.

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

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

13 ~~(2) (1) IF A STATE AGENCY DETERMINES THAT IT IS THE <--~~  
14 ~~SUBJECT OF A BREACH OF THE SECURITY OF THE SYSTEM AFFECTING~~  
15 ~~PERSONAL INFORMATION MAINTAINED BY THE STATE AGENCY OR STATE~~  
16 ~~AGENCY CONTRACTOR, THE STATE AGENCY SHALL PROVIDE NOTICE OF~~  
17 ~~THE BREACH OF THE SECURITY OF THE SYSTEM REQUIRED UNDER~~  
18 ~~SUBSECTION (A) WITHIN SEVEN BUSINESS DAYS FOLLOWING~~  
19 ~~DETERMINATION OF THE BREACH OF THE SECURITY OF THE SYSTEM.~~  
20 ~~NOTIFICATION SHALL BE PROVIDED CONCURRENTLY TO THE OFFICE OF~~  
21 ~~ATTORNEY GENERAL.~~

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

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

2 ~~(3) (2)~~ (3) A State agency under the Governor's <--

3 jurisdiction shall also provide notice of a breach of the

4 security of the system to the Governor's Office of

5 Administration ~~AND THE OFFICE OF ATTORNEY GENERAL~~ within <--

6 three business days following the determination of the breach

7 OF THE SECURITY OF THE SYSTEM. Notification shall occur <--

8 notwithstanding the existence of procedures and policies

9 under section 7.

10 ~~(4) (3)~~ A State agency that, on the effective date of <--

11 this section, has an existing contract with a State agency

12 contractor shall use reasonable efforts to amend the contract

13 to include provisions relating to the State agency

14 contractor's compliance with this act unless the existing

15 contract already contains breach of the security of the

16 system notification requirements.

17 ~~(5) (4)~~ (4) A State agency that, after the effective <--

18 date of this section, enters into a contract WHICH INVOLVES <--

19 THE USE OF PERSONAL INFORMATION with a State agency

20 contractor shall ensure that the contract includes provisions

21 relating to the State agency contractor's compliance with

22 this act.

23 (a.2) Notification by county, ~~school district~~ PUBLIC SCHOOL <--

24 or municipality.--If a county, ~~school district~~ PUBLIC SCHOOL or <--

25 municipality is the subject of a breach of the security of the

26 system, the county, ~~school district~~ PUBLIC SCHOOL or <--

27 municipality shall provide notice of the breach of the security

28 of the system required under subsection (a) within seven

29 BUSINESS days following determination of the breach OF THE <--

30 SECURITY OF THE SYSTEM. Notification shall be provided to the

1 district attorney in the county where the breach OF THE SECURITY <--  
2 OF THE SYSTEM occurred within three business days following  
3 determination of the breach OF THE SECURITY OF THE SYSTEM. <--  
4 Notification shall occur notwithstanding the existence of  
5 procedures and policies under section 7.

6 (a.3) Electronic notification.--In the case of a breach of  
7 the security of the system involving personal information for a  
8 user name or e-mail address in combination with a password or  
9 security question and answer that would permit access to an  
10 online account, the State agency, county, school district PUBLIC <--  
11 SCHOOL or municipality ENTITY, to the extent that it has <--  
12 sufficient contact information for the person, may comply with  
13 this section by providing the breach of the security of the  
14 system notification in electronic or other form that directs the  
15 person whose personal information has been breached MATERIALLY <--  
16 COMPROMISED BY THE BREACH OF THE SECURITY OF THE SYSTEM to  
17 promptly change the person's password and security question or  
18 answer, as applicable or to take other steps appropriate to  
19 protect the online account with the State agency, county, school <--  
20 district PUBLIC SCHOOL or municipality ENTITY and other online <--  
21 accounts for which the person whose personal information has  
22 been breached MATERIALLY COMPROMISED BY THE BREACH OF THE <--  
23 SECURITY OF THE SYSTEM uses the same user name or e-mail address  
24 and password or security question or answer.

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



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

4 \* \* \*

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

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

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

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

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

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

2 ~~(C) CONSIDERATIONS. IN DEVELOPING THE POLICY, THE~~ <--

3 ~~GOVERNOR'S OFFICE OF ADMINISTRATION SHALL CONSIDER SIMILAR~~

4 ~~EXISTING FEDERAL AND OTHER POLICIES IN OTHER STATES, BEST~~

5 ~~PRACTICES IDENTIFIED BY OTHER STATES AND RELEVANT STUDIES AND~~

6 ~~OTHER SOURCES AS APPROPRIATE.~~

7 ~~(D) REVIEW AND UPDATE. THE POLICY SHALL BE REVIEWED AT~~

8 ~~LEAST ANNUALLY AND UPDATED AS NECESSARY.~~

9 ~~Section 5.2. Commonwealth policy.~~

10 ~~(a) Storage policy. The Governor's Office of Administration~~ <--

11 ~~shall develop a policy to govern the proper storage by State~~

12 ~~agencies under the Governor's jurisdiction of data which~~

13 ~~includes personal information. The policy shall address~~

14 ~~identifying, collecting, maintaining, displaying and~~

15 ~~transferring personal information, using personal information in~~

16 ~~test environments, remediating personal information stored on~~

17 ~~legacy systems and other relevant issues. A goal of the policy~~

18 ~~shall be to reduce the risk of future breaches of the security~~

19 ~~of the system.~~

20 ~~(b) Considerations. In developing the policy, the~~ <--

21 ~~Governor's Office of Administration shall consider similar~~

22 ~~existing Federal and other policies in other states, best~~

23 ~~practices identified by other states and relevant studies and~~

24 ~~other sources as appropriate.~~

25 ~~(c) Review and update. The policy shall be reviewed at~~

26 ~~least annually and updated as necessary.~~

27 ~~(A) GENERAL RULE.--AN ENTITY THAT MAINTAINS, STORES OR~~ <--

28 ~~MANAGES COMPUTERIZED DATA ON BEHALF OF THE COMMONWEALTH THAT~~

29 ~~CONSTITUTES PERSONAL INFORMATION SHALL UTILIZE ENCRYPTION, OR~~

30 ~~OTHER APPROPRIATE SECURITY MEASURES, TO REASONABLY PROTECT THE~~

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

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

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

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

16 SECTION 5.2. DATA STORAGE POLICY.

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

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

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

1 Section 5.3. Entities subject to the Health Insurance  
2 Portability and Accountability Act of 1996.  
3 Any covered entity or business associate that is subject to  
4 and in compliance with the privacy and security standards for  
5 the protection of electronic personal health information  
6 established under the Health Insurance Portability and  
7 Accountability Act of 1996 (Public Law 104-191, 110 Stat. 1936)  
8 and the Health Information Technology for Economic and Clinical  
9 Health Act (Public Law 111-5, 123 Stat. 226-279 and 467-496)  
10 shall be deemed to be in compliance with the provisions of this  
11 act.

12 Section 5. ~~Section 7(b)(2) of the act is amended to read:--~~ <--  
13 SECTIONS 7(B)(2) AND 29 OF THE ACT ARE AMENDED TO READ: <--

14 Section 7. Notice exemption.

15 \* \* \*

16 (b) Compliance with Federal requirements.--

17 \* \* \*

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

26 SECTION 29. APPLICABILITY. <--

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

1 Section 6. This act shall take effect in ~~120~~ 180 days.

<--