
THE GENERAL ASSEMBLY OF PENNSYLVANIA

SENATE BILL

No. 608 Session of
2021

INTRODUCED BY PHILLIPS-HILL, LAUGHLIN, MARTIN, J. WARD AND
MENSCH, APRIL 27, 2021

REFERRED TO COMMUNICATIONS AND TECHNOLOGY, APRIL 27, 2021

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 definitions and for notification of breach; and
6 providing for contents and nature of notice and for storage
7 policies.

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

10 Section 1. The definitions of "notice" and "personal
11 information" in section 2 of the act of December 22, 2005
12 (P.L.474, No.94), known as the Breach of Personal Information
13 Notification Act, are amended and the section is amended by
14 adding definitions to read:

15 Section 2. Definitions.

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

19 * * *

20 "Health insurance information." Any of the following

1 regarding an individual:

2 (1) The individual's health insurance policy number or
3 subscriber identification number.

4 (2) A unique identifier used by a health insurer to
5 identify the individual.

6 (3) Information in the individual's application and
7 claims history, including any appeals records.

8 * * *

9 "Medical information." Information regarding an individual's
10 medical history, mental or physical condition, or medical
11 treatment or diagnosis by a health care professional.

12 "Notice." May be provided by any of the following methods of
13 notification:

14 (1) Written notice to the last known home address for
15 the individual.

16 (2) Telephonic notice, if the customer can be reasonably
17 expected to receive it and the notice is given in a clear and
18 conspicuous manner, describes the incident in general terms
19 and verifies personal information but does not require the
20 customer to provide personal information and the customer is
21 provided with a telephone number to call or Internet website
22 to visit for further information or assistance.

23 (3) E-mail notice, if a prior business relationship
24 exists and the person or entity has a valid e-mail address
25 for the individual.

26 (4) (i) Substitute notice, if the entity demonstrates
27 one of the following:

28 (A) The cost of providing notice would exceed
29 \$100,000.

30 (B) The affected class of subject persons to be

1 notified exceeds 175,000.

2 (C) The entity does not have sufficient contact
3 information.

4 (ii) Substitute notice shall consist of all of the
5 following:

6 (A) E-mail notice when the entity has an e-mail
7 address for the subject persons.

8 (B) Conspicuous posting of the notice on the
9 entity's publicly accessible Internet website if the
10 entity maintains one. The posting shall occur for a
11 minimum of 30 days and provide a link to the notice
12 on the home page of the website or on the first
13 significant page after entering the website.

14 (C) Notification to major Statewide media.

15 "Personal information." As follows:

16 (1) [An] The term includes an individual's first name
17 or first initial and last name in combination with and linked
18 to any one or more of the following data elements when the
19 data elements are not encrypted or redacted:

20 (i) Social Security number.

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

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

28 (1.1) The term also includes any of the following:

29 (i) Health insurance information.

30 (ii) Medical information.

- 1 (iii) Educational records.
- 2 (iv) Income or other socioeconomic information.
- 3 (v) Religious information or information regarding
4 other beliefs.
- 5 (vi) Information regarding food purchases.
- 6 (vii) Unique biometric data generated from
7 measurements or technical analyses of human body
8 characteristics, including, but not limited to, a
9 fingerprint, voice print, retinal or iris image or any
10 other unique physical representation or digital
11 representation of biometric data.
- 12 (viii) Geolocation data.
- 13 (ix) Information or data collected through the use
14 or operation of an automated license plate recognition
15 system.
- 16 (x) A user name or e-mail address, in combination
17 with a password or security question and answer that
18 would permit access to an online account.

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

22 * * *

23 Section 2. Section 3(a) of the act is amended and the
24 section is amended by adding a subsection to read:

25 Section 3. Notification of breach.

26 (a) General rule.--

27 (1) An entity that maintains, stores or manages
28 computerized data that includes personal information shall
29 provide notice of any breach of the security of the system
30 following discovery of the breach of the security of the

1 system to any resident of this Commonwealth whose unencrypted
2 and unredacted personal information was or is reasonably
3 believed to have been accessed and acquired by an
4 unauthorized person.

5 (2) Except as provided in subsection (d) or section 4 or
6 in order to take any measures necessary to determine the
7 scope of the breach and to restore the reasonable integrity
8 of the data system, the notice shall be made without
9 unreasonable delay.

10 (3) For the purpose of this section, a resident of this
11 Commonwealth may be determined to be an individual whose
12 principal mailing address, as reflected in the computerized
13 data which is maintained, stored or managed by the entity, is
14 in this Commonwealth.

15 * * *

16 (d) Notification by specific entities.--

17 (1) If a State agency is the subject of the breach of
18 the security of the system, the State agency shall notify the
19 following:

20 (i) The head of the State agency within two hours of
21 the detection of the breach of the security of the
22 system.

23 (ii) The Governor's Office of Administration and the
24 office of Attorney General within four hours of the
25 detection of the breach of the security of the system.

26 (2) If a political subdivision of the Commonwealth is
27 the subject of the breach of the security of the system, the
28 political subdivision shall notify the following:

29 (i) The head of the political subdivision of the
30 Commonwealth within two hours of the detection of the

1 breach of the security of the system.

2 (ii) The district attorney of the county in which
3 the political subdivision is located within three
4 business days of the detection of the breach of the
5 security of the system.

6 (3) If an individual or a business doing business in
7 this Commonwealth is the subject of the breach of the
8 security of the system, the individual or business shall
9 notify the following:

10 (i) The district attorney of the county in which the
11 business is located within three business days of the
12 detection of the breach of the security of the system.

13 (ii) Individuals affected by the breach of the
14 security of the system within 14 days of the detection of
15 the breach of the security of the system.

16 (4) Notification under this subsection shall occur
17 regardless of whether the notice exemption applies under
18 section 7.

19 Section 3. The act is amended by adding sections to read:

20 Section 3.1. Contents and nature of notice.

21 (a) Mandatory contents.--Each written, e-mail or website
22 notice under this act shall include, at a minimum, the
23 following:

24 (1) The name and contact information of the entity
25 providing the notice.

26 (2) The date of the notice.

27 (3) A list of the types of personal information that
28 were or are reasonably believed to have been the subject of
29 the breach of the security of the system.

30 (4) If possible to determine at the time the notice is

1 provided, all of the following:

2 (i) The date of the breach of the security of the
3 system.

4 (ii) The estimated date of the breach of the
5 security of the system.

6 (iii) The date range within which the breach of the
7 security of the system occurred.

8 (5) A general description of the breach incident, if
9 that information is possible to determine at the time the
10 notice is provided.

11 (6) A statement regarding whether notice was delayed as
12 a result of a law enforcement investigation, if that
13 information is possible to determine at the time the notice
14 is provided.

15 (7) The toll-free telephone numbers and addresses of the
16 major credit reporting agencies if the breach of the security
17 of the system exposed an individual's Social Security number,
18 driver's license number or State identification card number
19 issued in lieu of a driver's license.

20 (8) Information regarding the steps taken to protect the
21 individuals whose personal information is the subject of the
22 breach of the security of the system.

23 (9) An offer by the entity providing the notice to
24 provide free credit reports, credit protection and identity
25 theft protection for 12 months to each individual affected by
26 the breach of the security of the system.

27 (10) Advice on steps that the individual affected by the
28 breach of the security of the system may take to protect the
29 individual.

30 (b) Mandatory format.--Each written, e-mail or website

1 notice under this act shall:

2 (1) Be written in plain language.

3 (2) Be titled "Notice of Data Breach."

4 (3) Present the information under the following

5 headings:

6 (i) "What Happened."

7 (ii) "What Information Was Involved."

8 (iii) "What We Are Doing."

9 (iv) "What You Can Do."

10 (v) "For More Information."

11 (4) Provide for the possibility of additional
12 information to be provided as a supplement to the notice.

13 (5) Be designed to call attention to the nature and
14 significance of the information contained in the notice.

15 (6) Display the title, headings and text of the notice
16 in a clear and conspicuous manner.

17 (7) Provide that the text of the notice and any other
18 written notification provided under this section be no
19 smaller than 10-point type.

20 Section 9. Storage policies.

21 (a) Development.--The head of each State agency, whether or
22 not under the Governor's jurisdiction, the Court Administrator
23 of Pennsylvania and the administrators of the legislative
24 caucuses of the Senate and the House of Representatives shall
25 develop policies for the offices under their jurisdiction to
26 govern the safe and proper storage of computerized data
27 containing personal information and other sensitive personally
28 identifiable information. A goal of the policies shall be to
29 reduce the risk of future breaches of the security of the
30 system.

1 (b) Subject matter.--As permitted by Federal or State law or
2 regulation, the policies developed under subsection (a) shall
3 address:

4 (1) identifying, collecting, maintaining, displaying,
5 restoring, protecting and transferring personally
6 identifiable information;

7 (2) using personally identifiable information in test
8 environments;

9 (3) remediating the negative effects concerning the
10 breach or corruption of personally identifiable information
11 stored on legacy systems; and

12 (4) other relevant issues.

13 (c) Considerations.--In developing the policies under
14 subsection (a), consideration shall be given to Federal and
15 State law and regulations, similar existing policies in other
16 states, best practices identified by other states, relevant
17 studies and other sources as appropriate.

18 (d) Review.--The policies developed under this section shall
19 be reviewed at least annually and updated as necessary.

20 Section 4. This act shall take effect in 120 days.