# BREACH OF PERSONAL INFORMATION NOTIFICATION ACT

**Act of Dec. 22, 2005, P.L. 474, No. 94 Cl. 12**

AN ACT

Providing for security of computerized data and for the notification of residents whose personal information data was or may have been disclosed due to a breach of the security of the system; and imposing penalties. (Title amended Nov. 3, 2022, P.L.2139, No.151)

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

Section 1. Short title.

This act shall be known and may be cited as the Breach of Personal Information Notification Act.

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:

"Breach of the security of the system." The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth. Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.

"Business." A sole proprietorship, partnership, corporation, association or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered or holding a license or authorization certificate under the laws of this Commonwealth, any other state, the United States or any other country, or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records.

"Determination." A verification or reasonable certainty that a breach of the security of the system has occurred. (Def. added Nov. 3, 2022, P.L.2139, No.151)

"Discovery." The knowledge of or reasonable suspicion that a breach of the security of the system has occurred. (Def. added Nov. 3, 2022, P.L.2139, No.151)

"Encryption." The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

"Entity." A State agency, a political subdivision of the Commonwealth or an individual or a business doing business in this Commonwealth.

"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. (Def. added Nov. 3, 2022, P.L.2139, No.151)

"Individual." A natural person.

"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. (Def. added Nov. 3, 2022, P.L.2139, No.151)

"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 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 individual to provide personal information and the 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.

(Def. amended Nov. 3, 2022, P.L.2139, No.151)

"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 in the possession of a State agency or State agency contractor.

(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.

(Def. amended June 28, 2024, P.L.427, No.33)

"Records." Any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed or electromagnetically transmitted. The term does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.

"Redact." The term includes, but is not limited to, alteration or truncation such that no more than the last four digits of a Social Security number, driver's license number, State identification card number or account number is accessible as part of the data.

"State agency." Any agency, board, commission, authority or department of the Commonwealth and the General Assembly.

"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. (Def. added Nov. 3, 2022, P.L.2139, No.151)

Section 3. Notification of the breach of the security of the system. (Hdg. amended Nov. 3, 2022, P.L.2139, No.151)

(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 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) amended Nov. 3, 2022, P.L.2139, No.151)

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

(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 affected by the State agency contractor's breach of the security of the system 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) 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 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) 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.1) added Nov. 3, 2022, P.L.2139, No.151)

(a.2) Notification by county, public school or municipality.--If a county, public school or municipality is the subject of a breach of the security of the system, the county, 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.2) added Nov. 3, 2022, P.L.2139, No.151)

(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 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 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 entity and other online accounts for which the person whose personal information has been 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.3) added Nov. 3, 2022, P.L.2139, No.151)

(a.4) Affected individuals.--In the case of a breach of the security of the system involving personal information 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. ((a.4) added Nov. 3, 2022, P.L.2139, No.151)

(b) Encrypted information.--An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

(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. ((c) amended Nov. 3, 2022, P.L.2139, No.151)

(c.1) Notice to Attorney General.--When notice of the breach of the security of the system under this section must be given to more than 500 affected individuals in this Commonwealth, notice shall be made concurrently to the Office of Attorney General. Notice to the Attorney General shall include the following information to the extent known by the notifying entity:

(1) The organization name and location.

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

(3) A summary of the breach incident of the security of the system.

(4) An estimated total number of individuals affected by the breach of the security of the system.

(5) An estimated total number of individuals in this Commonwealth affected by the breach of the security of the system.

((c.1) added June 28, 2024, P.L.427, No.33)

(c.2) Exemption.--An entity subject to the requirements of 40 Pa.C.S. Ch. 45 (relating to insurance data security) shall be exempt from the notice requirements under subsection (c.1). ((c.2) added June 28, 2024, P.L.427, No.33)

(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. ((d) added Nov. 3, 2022, P.L.2139, No.151)

Section 4. Exceptions.

The notification required by this act may be delayed if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation. The notification required by this act shall be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security.

Section 5. Notification of consumer reporting agencies.

When an entity provides notification under this act to more than 500 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in section 603 of the Fair Credit Reporting Act (Public Law 91-508, 15 U.S.C. § 1681a), of the timing, distribution and number of notices.

(5 amended June 28, 2024, P.L.427, No.33)

Section 5.1. Encryption required.

(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.

(5.1 added Nov. 3, 2022, P.L.2139, No.151)

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.

(5.2 added Nov. 3, 2022, P.L.2139, No.151)

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.

(5.3 added Nov. 3, 2022, P.L.2139, No.151)

Section 5.4. Credit reporting and monitoring.

(a) Assumption of costs.--An entity that provides notification under section 5 and meets the requirements of subsection (b) shall assume all costs and fees in providing the affected individuals:

(1) Access to one independent credit report from a consumer reporting agency if the individual is not eligible to obtain an independent credit report from a consumer reporting agency for free under 15 U.S.C. § 1681 (relating to congressional findings and statement of purpose).

(2) Access to credit monitoring services for a period of 12 months following notification. An entity may satisfy the requirements of this paragraph by providing notice to the individual of the availability of monitoring services for a period of 12 months at no cost to the individual.

(b) Data subject to credit reporting and monitoring.--Notwithstanding any other provision of law, an entity shall be subject to the requirements of this section if that entity makes a determination that a breach of the security of the system has occurred and reasonably believes that an individual's first name and last name or an individual's first initial and last name, in combination with any of the following information, has been accessed:

(1) Social Security number.

(2) Bank account number.

(3) Driver's license or State ID number.

(c) Notice.--The entity shall inform the affected individual of the availability of no-cost services under subsection (a) upon notification in compliance with this act.

(5.4 added June 28, 2024, P.L.427, No.33)

Section 6. Preemption.

This act deals with subject matter that is of Statewide concern, and it is the intent of the General Assembly that this act shall supersede and preempt all rules, regulations, codes, statutes or ordinances of all cities, counties, municipalities and other local agencies within this Commonwealth regarding the matters expressly set forth in this act.

Section 7. Notice exemption.

(a) Information privacy or security policy.--An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and is consistent with the notice requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(b) Compliance with Federal requirements.--

(1) A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this act.

(2) An entity, a State agency 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's or State agency's contractor's primary State or functional Federal regulator, shall be in compliance with this act.

((2) amended Nov. 3, 2022, P.L.2139, No.151)

Section 8. Civil relief.

A violation of this act shall be deemed to be an unfair or deceptive act or practice in violation of the act of December 17, 1968 (P.L.1224, No.387), known as the Unfair Trade Practices and Consumer Protection Law. The Office of Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act.

Section 29. Applicability.

This act shall apply to the determination or notification of a breach of the security of the system that occurs on or after the effective date of this section.

(29 amended Nov. 3, 2022, P.L.2139, No.151)

Section 30. Effective date.

This act shall take effect in 180 days.