EAST STROUDSBURG AREA SCHOOL DISTRICT

SECTION: OPERATIONS
TITLE: DATA BREACH NOTIFICATION

ADOPTED: July 16, 2007

REVISED: May 16, 2011
September 15, 2014
May 21, 2018

RENUMBERED: August 15, 2022
September 19, 2022

REVISED: 2023

	# 830.2 DATA BREACH NOTIFICATION
1. Purpose	The East Stroudsburg Area School District ("School District") recognizes that data, information, and records[1] must be protected in all ~~of~~ their forms, on all ~~of~~ their media, and during all ~~of~~ the phases of their life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction. With the increased reliance upon electronic data, and the maintenance of personal information of students, employees, and others in electronic and other formats, the School District is concerned about the risk of a breach in the electronic system's security and other possible disclosures of personal information. This policy addresses the manner in which the School District will respond to unauthorized access and acquisition of computerized data that compromises the security and confidentially of personal information.
2. Authority **73 P.S. § 2301 et seq.**	District administrators shall provide appropriate notification of any computerized system security breach to any Commonwealth resident whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed or acquired by unauthorized persons.

[1] ~~"Records" (with an initial capital letter) refers to the defined terms of Pennsylvania's *Breach of Personal Information Notification Act*, whereas "records" (without an initial capital letter) refers to records generally.~~

~~2~~3. Definitions 73 P.S. § 2302	~~1.~~ Under *Pennsylvania's Breach of Personal Information Notification Act* the subsequent words have the following meanings. **Breach of the System's Security**[2] – means unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of p~~P~~ersonal i~~I~~nformation[3] maintained by the School District as part of a~~the~~ database of p~~P~~ersonal i~~I~~nformation regarding multiple individuals and that causes, or the School District reasonably believes has caused or will cause loss or injury to any ~~Pennsylvania~~ resident of the~~is~~ Commonwealth of Pennsylvania. Good faith acquisition of p~~P~~ersonal ~~I~~nformation by an employee or agent acting in good faith on behalf of the School District for the purposes of the School District is not a b~~B~~reach of the s~~S~~ystem's s~~S~~ecurity if the p~~P~~ersonal i~~I~~nformation is not used for a purpose other than the lawful purpose of the School District and is not subject to further unauthorized disclosure. **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. **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. **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** – Notice may be provided by any of the following methods of notification:

~~[2] *Breach of the System's Security* relevant to Pennsylvania's *Breach of Personal Information Notification Act* may also be referred to as "BPINA Breach".~~

~~[3] See Definition section for the defined terms generally provided in initial capital letters throughout this Policy and the accompanying administrative regulation(s).~~

	(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.
73 P.S. § 2302	**Personal Information** – Personal Information ~~i~~ncludes 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: (1) Social Security number (2) Driver's license number or a State identification card number issued in lieu of a driver's license. (3) 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.

	(4) Health information. (5) Health insurance information. (6) 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.
73 P.S. § 2302 Policy 801	The term~~Personal information~~ does not include publicly available information that is lawfully made available to the general public from federal, S~~s~~tate or local government records or widely distributed media.
73 P.S. §2302	**Records –** ~~pursuant to the *Breach of Personal Information Notification Act,*~~ Records mean any material, regardless of its physical form, on which information is recorded or preserved by any means, including 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** – Redact 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. ~~2. The Health Insurance Portability and Accountability Act, as Amended, and its implementing Regulations.~~
~~45 C.F.R. Part 164, § 164.402; 45 C.F.R. subpart E If relevant, the School District HIPAA Privacy Policy and HIPAA Manual~~	~~The Health Insurance Portability and Accountability Act, as Amended, and its implementing Regulations (collectively ("HIPAA") *may or may not apply* to the School District. If HIPAA *is not* applicable to the School District, the following section(s) and the HIPAA requirements in this Policy, and any accompanying, regulation(s), procedures and rules should be disregarded. If HIPAA is applicable to the School District, then the following section(s) and reference to the HIPAA in this Policy, and any other accompanying regulation(s), procedure(s) and rule(s) *must be observed*. The Superintendent, or designee, will make this determination. Under the HIPAA the subsequent words have the following meanings.~~ ~~**Breach**[4] – Breach under the HIPAA means the acquisition, access, use, or~~

[4] ~~*Breach* relevant to the *HITECH Act* may also be referred to as "HITECH Breach".~~

45 C.F.R. § 164.514(e)(2)	disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the PHI. The School District may use or disclose a limited data set that meets the requirements of the HITECH regulations § 164.514(e)(2) (*Implementation Specification: Limited Data Set) and §164.514(e)(3) (Implementation Specifications: Permitted Purposes for Use and Disclosures), if the School District enters into a data use agreement with the limited data set recipient, and the agreement contains the requirements of the HITECH Act § 164.414(e)(4).*
45 C.F.R. § 164.402	Breach *excludes*: (i) Any unintentional acquisition, Access, or use of PHI by a workforce member or person acting under the authority of the School District or a business associate, if such acquisition, Access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule. (ii) Any inadvertent disclosure by a person who is authorized to Access PHI at the School District or business associate to another person authorized to Access PHI at the School District or business associate, or organized health care arrangement in which the School District participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule. (iii) A disclosure of PHI where the School District or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. Except as provided in paragraph (i) of this definition, an acquisition, Access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless the School District or the covered entity, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors: (i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the PHI or to whom the disclosure was made; (iii) Whether the PHI was actually acquired or viewed; and

	~~(iv) The extent to which the risk to the PHI has been mitigated.~~
	~~**Health Information** – Health information means any information, including genetic information, whether oral or recorded in any form or medium, that:~~
34 C.F.R. §160.103	~~(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and~~
	~~(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.~~
	~~**Individually Identifiable Health Information** – Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:~~
34 C.F.R. §160.103	~~(1) Is creative or received by a health care provider, health plan, employer, or health are clearinghouse; and~~
	~~(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and~~
	~~(i) That identifies the individual; or~~
	~~(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.~~
34 C.F.R. §160.103	~~**Protected Health Information (PHI)** – means individually identifiable health information:~~
	~~(i) Except as excluded below, that is:~~
	~~(ii) Transmitted by electronic media;~~
	~~(iii) Maintained in electronic media; or~~
	~~(iv) Transmitted or maintained in any other form or medium.~~
	~~PHI *excludes* individually identifiable health information:~~
20 U.S.C. § 1232g	~~(i) In educational records covered by the Family Educational Rights~~

	~~and Privacy Act ("FERPA");~~
20 U.S.C. §1232g (4)(B)(iv)	~~(ii) In records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice.~~ ~~(iii) In employment records held by the School District in its role as employer; and~~ ~~(iv) Regarding a person who has been deceased for more than 50 years.~~ ~~**Unsecured Protected Health Information** - means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under the American Recovery and Reinvestment Act of 2009 (ARRA), §13402(h)(2).~~
47 C.F.R. § 164.304	~~**Access** - relevant to security standards for the protection of electronic PHI (47 C.F.R. § 164.3000 through 316), means ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource.~~
4~~3~~. Delegation of Responsibility ~~ARRA, §13402(h)(2)~~ 73 P.S. §2301 et seq.	Employees, agents, guests, vendors, ~~business associates,~~ and students must comply with the Pennsylvania mandated identity theft prevention laws, including the *Breach of Personal Information Notification Act*~~,~~[5] and the *Confidentiality of Social Security Number* law, ~~if applicable, HIPAA, and accompanying Health and Human Services ("HHS") regulations,~~ In addition, compliance is required with: (1) This Policy and its accompanying administrative regulation(s), procedures, and rules, and

[5] ~~If the data breach notification law of another state and Pennsylvania's *Breach of Personal Information Notification Act* apply to a matter consult the School District's attorney.~~

	(2) The School District's additional relevant policies, administrative regulations, procedures, and rules (including the Student Records Policy, the Privacy and Security of Student Electronic ~~Records~~ and Digital Information Policy, ~~and~~ the Student Records Plan, and the Information Protection Policy), ~~and~~ (3) The relevant agreements that the School District has entered into with vendors to protect student, employee, and other School District data, information, and records from unauthorized disclosure and/or breach of the security of the system, and (4) Any similar requirement to protect computerized data as part of a database that would materially compromise the security or confidentiality of personal information maintained by the School District that causes, or the School District reasonably believes has caused or will cause loss or injury to any resident of the Commonwealth. Employees, agents, guests, vendors, ~~and if applicable, business associates,~~ and students, are required to protect the sensitive, confidential, personally identifiable information about students, employees and others from theft, inadvertent, negligent and willful disclosure or breach[6] of such data, information, or records when they are under the supervision or control of the School District, and when they are not under the supervision or control of the School District, for example, but not limited to, working at home, on vacation, or elsewhere. School District administrators must provide ~~appropriate~~ notification as required by law of any ~~BPINA b~~B~~r~~each of the system's security to any resident whose unencrypted, unredacted, and unsecure Personal Information protected by Pennsylvania's *Breach of Personal Information Notification Act* was or is reasonably believed to have been accessed or acquired by unauthorized persons. ~~If HIPAA is applicable to the School District, School District administrators must provide appropriate notifications of a HIPAA Breach of PHI in a manner permitted under the HIPAA Privacy Rule.~~ The Superintendent, and/or designee, in collaboration with appropriate administrators shall ~~is hereby granted the authority to~~ create and enforce additional administrative regulations, procedures, and rules to ~~carry out~~implement ~~the purpose of~~ this Policy. The administrative regulation(s), procedures, and rules accompanying this Policy must include among other items:

[6] ~~The word "breach" refers collectively to all breaches whether it is a *BPINA Breach*, a HITECH Breach, or any breach of data, information, or record and/or under any law.~~

	(1) Internal procedures following discovery of a breach, including procedures for the determination of a breach and whether notification is required, as well as details regarding timelines, who must be notified and the authorized methods of notification (2) guidance in implementing the Pennsylvania *Data Breach Notification for Personal Information Act*, ~~if applicable, HIPAA,~~ the *Confidentiality of Social Security Number* law, ~~and~~ the Information Protection Policy, and the destruction of data, information, and records.
54. Guidelines	This Policy, its accompanying administrative regulation(s), procedures, and rules apply to all School District environments, whether the data, information, or records are used on School District property, or beyond School District property, in applications, systems, networks that the School District owns or that are operated by School District employees, agents, guests, vendors, business associates, or students. Other than data defined as public, all data, information, and records and processing resources are only accessible on a need-to-know basis to specifically identified, authenticated, and authorized individuals and entities. **Notification Requirements**
73 P.S. §2303(a.2)	Upon determination of a breach, the School District is required to provide notice within seven (7) business days to any resident of the Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed or acquired by unauthorized persons. In addition, the district attorney in the county where the breach occurred is required to be notified within three (3) days following the determination of the breach.
73 P.S. §2303(b)	The School District must provide notice of the Breach if the encrypted information is accessed and acquired in the unencrypted form, if the security breach is linked to a breach of the security of the the encryption, or if the security breach involves a person with access to the encryption key.
73 P.S. §2305a	To the extent required by law, the School District must use encryption, or other reasonable security measures, to protect the transmission of personal information over the Internet from being viewed or modified by an unauthorized third party.
15 U.S.C. §1681(a); 73 P.S. § 2305	If the School District must provide notification to more than 1,000 persons at one time, the School District shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a

	nationwide basis, as defined in the Fair Credit Reporting Act of the timing, distribution, and number of notices.
73 P.S. §2303(c)	A vendor that maintains, stores, or manages computerized data on behalf of the School District shall provide notice of any breach of the security of the system following discovery by the vendor to the School District on whose behalf the vendor maintains, stores, or manages the data. the School District must be responsible for making any determinations and discharging any remaining duties as required by this policy.
73 P.S. § 2304	The notice is required to be made without unreasonable delay unless: (1) A law enforcement agency determines that the notice would impede a criminal or civil investigation and provides the school entity with written notice specifically citing to 73 P.S. 2304. (2) It is necessary to take measures to determine the scope of the breach and to restore the reasonable integrity of the data system. **Training** The Superintendent, or designee, must provide training for employees, and if relevant, instructional sessions for students to assist them in knowing the importance of and how to protect sensitive, confidential, and personal data, information, and records, and how to comply with the data, information, and records requirements of this Policy and its accompanying administrative regulation(s), procedures, and rules. **Consequences for Inappropriate, Unauthorized, and Illegal Violations** Violations of this Policy, its administrative regulation(s), or other School District policies, administrative regulations, rules, and procedures, as well as statutes, regulations and laws may result in a variety of disciplinary actions, including but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, student suspensions, employee suspensions (with or without pay), dismissals, expulsions, breaches of contract, penalties provided in statutes, regulations, and other laws (including but not limited to penalties under Pennsylvania's *Data Breach Notification for Personal Information Act*, ~~and *the HIPAA, if applicable),*~~ and/or legal proceedings on a case-by-case basis. This Policy incorporates all other relevant School District policies, such as, but not limited to, the student and professional employee discipline policies, the Code of Student Conduct, the Acceptable Use Policy, ~~and~~ the Vendor Access Policy, and Information Protection Policy.

73 P.S. §2305a(d)	This Policy must be reviewed at least annually and updated as necessary. References: ~~*American Recovery and Reinvestment Act of 2009* (ARRA), §13402(h)(2).~~ *Breach of Personal Information Notification Act* ~~–~~ – 73 P.S. § 2301 et seq. *Fair Credit Reporting Act* – 15 U.S.C. § 1681a *Family Educational Rights and Privacy Act* – 20 U.S.C. § 1232g, 34 C.F.R. Part 99 ~~*Health Insurance Portability and Accessibility Act of 996 (HIPAA)* – Pub L. 104-191; 110 Stat. 1936~~ ~~*Health Information Technology for Economic and Clinical Health HITECH Act* – 45 C.F.R. Part 160 and 164~~ Identity Theft Laws (PA) – 18 Pa. C.S. § 4120; 42 Pa. C.S. § 9720.1 Pennsylvania Student Records Law – 22 Pa. Code § 12.31 - § 12.32 *Confidentiality of Social Security Number* Law – 74 P.S. § 201 ESASD Board Policies, Administrative Regulations, Procedures, and Rules ~~The~~ *ESASD Student Records Plan for the Collection, Maintenance, and Dissemination of Student Records*~~,~~ ~~*ESASD HIPAA Plan*~~ *ESASD Checklist for Responding to Reported and Suspected Data Security Breaches: Data Breach Notification Laws*~~.~~