EAST STROUDSBURG AREA SCHOOL DISTRICT

SECTION: OPERATIONS
TITLE: DATA BREACH NOTIFICATION

ADOPTED: July 16, 2007

REVISED: May 16, 2011
September 15, 2014
2018

830. DATA BREACH NOTIFICATION

1. Purpose

The East Stroudsburg Area School District ("School District") recognizes that data, information, and records are primary assets of and necessary to the operation, educational programs, and mission of the School District. School District 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.

2. 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 Personal Information[3] maintained by the School District as part of the database of Personal Information regarding multiple individuals and that causes or the School District reasonably believes has caused or will cause loss or injury to any Pennsylvania resident.

[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] *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).

	Good faith acquisition of Personal Information by an employee or agent of the School District for the purposes of the School District is not a Breach of the System's Security if the Personal Information is not used for a purpose other than the lawful purpose of the School District and is not subject to further unauthorized disclosure.
73 P.S. § 2302	**Personal Information** – includes an individual's first name or first initial and last name in combination with and linked to any one or more of the following, when not encrypted or redacted: • Social Security number • Driver's license number or a State identification card number issued in lieu of a driver's license. • 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.
73 P.S. § 2302 Policy 801	Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
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.
	2. ~~Under the *HITECH Act* the subsequent words have the following meanings.~~ 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 ~~ESASD HIPAA Plan~~	The Health Insurance Portability and Accountability Act, as amended, and 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), procedure(s) and rule(s) 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 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 ~~*HITECH Act*~~ *HIPAA*~~*Act*~~ means the acquisition, Access, use, or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule, which ~~C~~ccompromises the ~~S~~ssecurity or ~~P~~pprivacy of the ~~Protected Health Information~~PHI.
45 C.F.R. § 164.514(e)(1)	The School District may use or disclose a limited data set that meets the requirements of the ~~HITECH Act~~HIPAA 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).*.
	Breach *excludes*:
45 C.F.R. § 164.402	(i) Any unintentional acquisition, Access, or use of ~~protected health information~~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 ~~protected health information~~PHI at the School District or business associate to another person authorized to Access ~~protected health information~~ 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 ~~protected health information~~ 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 ~~protected health information~~ PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless the School District or ~~business associate~~the covered entity, as applicable, demonstrates that there is a low probability that the ~~protected health information~~PHI has been compromised based on a risk assessment of at least the following factors:

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

	(i) The nature and extent of the ~~protected health information~~PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the ~~protected health information~~PHI or to whom the disclosure was made; (iii) Whether the ~~protected health information~~ PHI was actually acquired or viewed; and (iv) The extent to which the risk to the ~~protected health information~~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 created or received by a health care provider, health plan, employer, 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; 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. **Protected Health Information (PHI)** – means individually identifiable health information:
34 C.F.R. § 160.103	(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: (i) In educational records covered by the Family Educational Rights and Privacy Act ('FERPA"); (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.
20 U.S.C. § 1232g 20 U.S.C. § 1232g (a)(4)(B)(iv)	
	(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~~PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized ~~individuals~~persons 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). **Access** – relevant to security standards for the protection of electronic PHI (45 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.
47 C.F.R. § 164.304	
3. Delegation of Responsibility ARRA, §13402(h)(2)	Employees, agents, guests, vendors, and if applicable, business associates~~,~~ and ~~if applicable,~~ students must comply with the Pennsylvania mandated identity theft prevention laws, including the *Breach of Personal Information Notification Act*,[5] the *Confidentiality of Social Security Number* law, if applicable, HIPAA, ~~the federal *Health Information Technology for Economic and Clinical Health Act*~~

[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.

	~~*("HITECH Act"),*~~ and accompanying Health and Human Services ("HHS") regulations, this Policy and its accompanying administrative regulation(s), procedures, and rules, and the School District's additional relevant policies, administrative regulations, procedures, and rules (including the Student Records Policy, the ~~Student Electronic~~ Privacy and Security of Student Electronic Records and Digital Information Policy, and the Student Records Plan), and relevant agreements that the School District has entered into with vendors to protect student, employee, and School District data, information, and records from unauthorized disclosure. Employees, agents, guests, vendors, and if applicable, business associates, and ~~if applicable~~ 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 of any BPINA Breach 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 notification of a ~~HITECH~~HIPAA Breach of ~~protected health information~~PHI in a manner permitted under the HIPAA Privacy Rule The Superintendent, and/or designee, is hereby granted the authority to create and enforce additional administrative regulations, procedures, and rules to carry out the purpose of this Policy. The administrative regulation(s), procedures, and rules accompanying this Policy must include among other items guidance in implementing the Pennsylvania *Data Breach Notification for Personal Information Act*, if applicable HIPAA and *the HITECH Act*, the *Confidentiality of Social Security Number* law, and the destruction of data, information, and records.
4. 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.

[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.

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.

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.

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, breach 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 ~~HITECH Act~~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.

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 Accountability Act of 1996 (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 ~~– 801, 801A, 815 and accompanying attachments, 815.1 and accompanying attachment, 830-AR. The~~
- *ESASD Student Records Plan for the Collection, Maintenance, and Dissemination of Student Records~~, the~~

	-*ESASD HIPAA Plan*~~, and the~~ -*ESASD Checklist for Responding to Reported and Suspected Data Security Breaches: Data Breach Notification Laws*.