LUZERNE INTERMEDIATE UNIT #18

SECTION: OPERATIONS

TITLE: DATA BREACH NOTIFICATION

ADOPTED: NOVEMBER 18, 2015

	830. Data Breach Notification
1. Purpose	The Luzerne Intermediate Unit ("Intermediate Unit") recognizes that information, data, and records are primary assets of and necessary to the operation, educational programs, and mission of the Intermediate Unit. Intermediate Unit 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 Intermediate Unit 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 Person 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 Intermediate Unit as part of the database of Personal Information regarding multiple individuals and that causes or the Intermediate Unit reasonable believes has caused or will cause loss or injury to any Pennsylvania resident. Good faith acquisition of Personal Information by an employee or agent of the Intermediate Unit for the purposes of the Intermediate Unit 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 Intermediate Unit and is not subject to further unauthorized disclosure. [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 Bread 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).

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. 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.
45 C.F.R. Part 164, §164.402; 45 C.F.R. subpart E; LIU HIPAA Plan	2. Under the federal Health Information Technology for Economic and Clinical Health Act ("HITECH Act") the subsequent words have the following meanings. **Breach** [4] – Breach under the HITECH Act means the acquisition, access, use or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule, which Compromises the Security or Privacy of the Protected Health Information. Compromises the Security or Privacy of the Protected Health Information means poses a significant risk of financial, reputational, or other harm to the individual.
45 C.F.R. § 164.514 (e) (2)	A use or disclosure of protected health information that does not include the identifiers listed at § 164.514 (e)(2) (Implementation Specification for the Limited Date Set standard), date of birth, and zip code does not Compromise the Security or Privacy of the Protected Health Information. Breach **excludes:** (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the Intermediate Unit or a business associate, in such acquisition, access, or use was made in

[4] Breach relevant to the HITECH Act may also be referred to as "HITECH breach"

	Good faith and within the scope of authority and does not result in further use of 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 at the Intermediate Unit or business associate to another person authorized to access protected health information at the Intermediate Unit or business associate, or organized health care arrangement in which the Intermediate Unit 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 where the Intermediate Unit 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 obtain such information. **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 in guidance issued under the American Recovery and Reinvestment Act of 2009 (ARRA), §13402(h)(2).
47 C.F.R. § 164.304	**Access** – means ability to read, write, modify, or communicate data/information or otherwise use any system resource.
3. Delegation of Responsibility	Employees, agents, guests, vendors, business associates, and if applicable, students must comply with the Pennsylvania mandated identity theft prevention laws, including the Breach of Person Information Notification Act [5], the Confidentiality of Social Security Number law, the HITECH Act, and accompanying Health and Human Services ("HHS") regulations, this Policy and its accompanying administrative regulations(s), procedures, and rules, and the Intermediate Unit's additional relevant policies, administrative regulations, procedures, and rules, including the Student Records Policy and the Student Records Plan. Employees, agents, guests, vendors, 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 information, data or records when they are under the supervision or control of the [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 Intermediate Unit's attorney. [6]The work "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.

	Intermediate Unit, and when they are not under the supervision or control of the Intermediate Unit, for example, but not limited to, working at home, on vacation, or elsewhere. Intermediate Unit 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. Intermediate Unit administrators must provide appropriate notification of a HITECH Breach of protected health information in a manner not permitted under the HIPAA Privacy Rule, which compromises the Security or Privacy of the Protected Health Information. The Executive Director, 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, the HITECH Act, the Confidentiality of Social Security Number law, and the destruction of records.
4. Guidelines	This Policy, it's accompanying administrative regulations(s), procedures and rules apply to all Intermediate Unit environments, whether the data, information, or records are used on Intermediate Unit property, or beyond Intermediate Unit property, in applications, systems, networks that the Intermediate Unit owns or that are operated by Intermediate Unit 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 identify, authenticated, and authorized individuals and entities. The Executive Director, 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 it's accompanying administrative regulations(s), procedures and rules. Violations of this Policy, it's administrative regulation(s), or other Intermediate Unit 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), and/or legal proceedings on a case-by-case basis. This Policy incorporates all other relevant Intermediate Unit 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 (PA) – 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 Information Technology for Economic and Clinical Health 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