Nazareth Area School District

Title – 815.1 Administrative Regulations – Data Breach Notification

Section - Operations

Adopted – October 13, 2015

Revised

With the increased reliance upon electronic data, and the maintenance of personal information of students, employees and others in electronic and other formats, the Nazareth Area School District ("School District") is concerned about the risk of a breach[1] in the electronic system's security and other possible disclosures of personal information.

Employees, agents, guests, vendors, business associates, and if applicable, students must comply with the Pennsylvania mandated identity theft prevention laws, including the *Breach of Personal Information Notification Act*, the *Confidentiality of Social Security Number* law, the federal *Health Information Technology for Economic and Clinical Health Act ("HITECH Act")*, and accompanying Health and Human Services ("HHS") regulations, the School District's Data Breach Notification Policy # 815.1, this Administrative Regulation, any other accompanying administrative regulations, 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 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, business associates, and if applicable students, are required to protect the sensitive, confidential, and personally identifiable information about students, employees and others from theft, inadvertent, negligent and willful disclosure or breach 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.

[1] See the *Nazareth Area School District Data Breach Notification Policy # 815.1*, Definition section, and footnotes, for the defined terms generally provided in initial capital letters through out that Policy and this Administrative Regulation.

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.

School District administrators must provide appropriate notification of a HITECH Breach of PHI in a manner not permitted under the HIPAA Privacy Rule.

Violation of this Administrative Regulation may result in corrective action up to and including termination as provided in the School District's Data Breach Notification Policy.

Pennsylvania Data Breach Notification for Personal Information[2]

A. If any employee becomes aware of the release of School District data, information, or Records the release must be reported to the Superintendent, or designee, immediately.

B. The Superintendent, or designee, following discovery of the Breach of the System's Security must provide without unreasonable delay notice of breached computerized records to any Pennsylvania resident whose unencrypted and unredacted Personal Information was, or is reasonably believed to have been accessed and acquired by an unauthorized person. Before providing the notice, the Superintendent, or designee, must take any measures necessary to determine the scope of the breach, restore the reasonable integrity of the data system, and carry out subsection E below.

C. The School District must provide notice of the BPINA Breach (a) if the encrypted information is accessed and acquired in an unencrypted form, (b) if the Breach of the System's Security is linked to a breach of the encryption, or (c) if the BPINA Breach involves a person with access to the encryption key.

D. A vendor that maintains, stores or manages computerized data on behalf of the School District must provide notice of any Breach of the System's Security following discovery by the vendor to the School District. The School District is then responsible for making the determinations and discharging any remaining duties pursuant to the *Breach of Personal Information Notification Act*.

E. The School District must report the Breach of the System's Security and any information pertaining to the BPINA Breach to the local, state, or federal law enforcement agency for investigation or handling in advance of the disclosure to any resident, or others. The School District may be required to delay notification if a law enforcement agency determines and provides in writing that the notification will impede a criminal or civil investigation, or will compromise an investigation into national or homeland security.

[2] As a guide for administrators, see *NASD Checklist for Responding to Reported and Suspected Data Security Breaches: Data Breach Notification Laws, pages 9 to 11*. Assistance can also be obtained from the School District's attorney.

F. The School District administration must then determine whether a data breach notification will be issued. Notifications must be provided by at least one (1) of the following methods:

1. Written notice, to last known home address for the individual.

2. Telephone notice, if the individual can be reasonably expected to receive the notice 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 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 School District has a valid e-mail address for the individual.

4. Substitute notice, if the School District demonstrates that the cost of providing the notice exceeds $100,000, the affected individuals exceeds 175,000 persons, or the School District does not have sufficient contact information. Substitute notice must consist of all of the following: an e-mail notice if the School District has an e-mail address for the persons, conspicuous posting of the notice on the School District's website, and notification to major Statewide media.

G. If the School District provides notification under a BPINA Breach to more than 1,000 persons at one (1) time, the School District must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (defined in the Fair Credit Reporting Act) of the timing, distribution and number of notices.

Federal Data Breach Notification for PHI[3]

A. The School District must protect the privacy and security of HIPAA PHI. Unless the PHI is encrypted or destroyed pursuant to the U.S. Department of Health and Human services ("HHS") standards and considered secure health information the School District must comply with the HITECH Breach notification rules.

B. The HITECH Breach Notification Rule requires School Districts to notify each individual whose Unsecured PHI has been, or is reasonably believed to have been Accessed, acquired, used, or disclosed following a Breach of that Unsecured PHI. The Rule also requires a business associate to notify the School District of a Breach of unsecured PHI.

C. HHS sets forth the following three-step process for the School District to follow in determining whether a HITECH Breach has occurred for which notification must be given:

[3] As a guide for administrators, see *NASD Checklist for Responding to Reported and Suspected Data Security Breaches: Data Breach Notification Laws, pages 4 to 8.* Assistance can also be obtained from the School District's attorney.

1. Determine whether there has been an impermissible use or disclosure of PHI under the HIPAA Privacy Rule;

2. Determine, and document, whether the impermissible use or disclosure compromises the privacy or security of the PHI; and

3. Determine whether the incident is excluded from the definition of HITECH "Breach" because it is:

- An unintentional acquisition, Access, or use of PHI by a workforce member or person acting under the authority of the School District or 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;

- An inadvertent disclosure of PHI 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 disclosed in a manner not permitted under the HIPAA Privacy Rule; or

- A disclosure of PHI where the School District or business associate has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI.

Except as provided in paragraph (a) 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 business associate, as applicable, demonstrates that there is a low probability that the protected health information 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.

D. Once the breach has been established, the Rule requires notice of a HITECH Breach of Unsecured PHI to be provided as follows:

1. The School District must notify each individual whose Unsecured PHI has been, or is reasonably believed by the School District to have been accessed, acquired, or disclosed as a result of a breach.

2. A business associate of the School District must notify the School District of the business associate's breach. The notice must include the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the business associate to have been accessed, acquired, or disclosed during the breach.

3. A HITECH breach must be treated as discovered as of the first day on which the breach is known by the School District or by the covered entity, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or agent of the School District or business associate, respectively) or should reasonably have been known to the School District or business associate (or person) to have occurred.

4. **Timeliness of Notification** Subject to section 7 below, all notifications must be made "without unreasonable delay" but no later than 60 calendar days after discovery of the HITECH Breach by the School District (or business associate involved in the case of a notification required in section D.2 above).

5. **Methods of Notifications**

- ***Notifications to Individuals*** – Written notification must be sent promptly to the individual's last known address by first-class mail, or email if the individual has specified a preference for the notification to be sent by email and has not withdrawn the email preference. Written notifications may be sent in one or more mailings.

  If the contact information for less than 10 individuals is outdated or insufficient, substitute notice may be provided by an alternative written notice, by telephone, or by other means. If the contact information for 10 or more individuals is found to be outdated or insufficient, the School District must provide substitute notice in one of the following forms:

  (1) Conspicuous posting on the home page of the School District's website for a period of not less than 90 days; or

  (2) In major print or broadcast media, including in the geographic areas where the affected individuals likely reside.

  (3) In addition, the substitute notice on the website or in print or broadcast media must include a toll-free telephone number that will remain active for 90 days where individuals can learn whether their unsecured PHI was included in the breach.

  If the School District deems an urgency of imminent misuse of the Unsecured PHI, the School District may provide information to the individuals by telephone

or other means, as appropriate, in addition to the written notice required in section 5(a) above.

If the individual is deceased, the School District must send the notification to the last known address of the individual or next of kin, or personal representative.

•. ***Notification to Media*** – If the HITECH Breach affects more than 500 or more residents of a particular state or jurisdiction, the School District also must notify "prominent media outlets" serving the state or jurisdiction of the HITECH Breach without unreasonable delay, but no later than 60 calendar days after discovery of the HITECH Breach.

•. ***Notification to HHS*** – If the HITECH Breach affects more than 500 individuals, notice must be made to HHS contemporaneously with the notification to the affected individuals. If fewer than 500 individuals are affected, the School District must maintain a log of any such HITECH Breaches, and submit the log annually to HHS no later than 60 days following the end of the calendar year.

• ***Posting on HHS Public Website*** – HHS is required to make available on its website a list identifying each entity involved in a breach that the Unsecured PHI of more than 500 individuals is acquired or disclosed.

6. **Content of Notification** – Regardless of the method of notification of the Breach provided to individuals it must be "in plain language" and include the following:

• A brief description of what happened, including the date of the HITECH Breach and the date of discovery of the HITECH Breach, if known;

• A description of the types of Unsecured PHI that were involved in the HITECH Breach;

• Steps individuals should take to protect themselves from potential harm resulting from the HITECH Breach;

• A brief description of the steps the School District is taking to investigate the HITECH Breach, to mitigate harm to the individuals, and to protect against future HITECH Breaches; and

• Contact procedures for individuals to ask questions or obtain additional information, including a toll-free telephone number, an email address, website, or postal address.

7. If a law enforcement official determines that a notification, notice, or posting required would impede a criminal investigation or cause damage to national security, the notification, notice, or posting must be delayed for the time specified by the official and as provided in the HITECH Act.

Student Records

Breach of student information must be reported to the Superintendent, or designee, who must determine whether such disclosure is a reportable matter to the parents and/or student, and if so, how reporting will be done.

Destruction of School District Records

All records of the School District must be destroyed pursuant to the School District Records Retention and Records Destruction Policies, Records Retention and Destruction Schedule and other School District records requirements and procedures. Destruction means shredding, clearing, purging, erasing, or modifying the information in and of the records to make the records unusable, unreadable, indecipherable or non-reconstructionable (redaction does not satisfy the requirement) to unauthorized persons through generally available means.

For Protected Health Information, the media on which the PHI is stored or recorded, including discarded paper records or recycled electronic media, must be destroyed in one of the following ways:

1. Discarded paper, film, or other hard copy media must be shredded or destroyed so that the PHI cannot be read or otherwise cannot be reconstructed; or

2. Electronic media must be cleared, purged, or destroyed consistent with the National Institute of Standards and Technology ("NIST") security standards such that the PHI cannot be retrieved (for example, see NIST Special Publication 800-88, Guidelines for Media Sanitation, Revision 1 (December 2014).

Social Security Number Requirement

A. Unless otherwise permitted by law, School District employees must protect the privacy of Social Security numbers.

B. The School District may not do any of the following:

1. Publicly post or publicly display in any manner an individual's Social Security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise make available the Social Security number to the general public.

2. Print an individual's Social Security number on any card required for the individual to access products or services provided by the School District.

3. Require an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted.

4. Require an individual to use his or her Social Security number to access an Internet website unless a password or unique personal identification number or other authentication device is also required to access the website.

5. Print an individual's Social Security number on any materials that are mailed to the individual unless federal or state law requires the Social Security number to be on the document to be mailed. However, Social Security numbers may be included in

applications and forms sent by mail, including documents sent as part of an application or enrollment process or to establish, amend or terminate an account, contract or policy or to confirm the accuracy of the Social Security number. A Social Security number that is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.

6. Disclose in any manner the Social Security number of an individual who applies for a recreational license (i.e., a fish or game license).

C. The School District may collect, use, or release a Social Security number as required by federal or state law or may use the Social Security number for internal verification, administrative purposes or for law enforcement investigations.

D. This requirement does not apply to a document that:

1. Originated with or is filed with, recorded in or is maintained by any court component or part of the unified judicial system; or

2. Is required by law to be open to the public, and originates with, or is filed, recorded or maintained by any government agency, instrumentality, or taxing authority.

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
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
NASD Board Policies, Administrative Regulations, Procedures, and Rules
NASD Student Records Plan for the Collection, Maintenance, and Dissemination of Student Records
NASD HIPAA Plan
NASD Checklist for Responding to Reported and Suspected Data Security Breaches: Data Breach Notification Laws