# Everett School Employee Benefit Trust

# Reportable Breach Notification Policy
# HIPAA HITECH Rules and Washington State Law

***Introduction***

The Everett School Employee Benefit Trust ("Trust") adopts this policy to comply with the Interim Final Rule, Breach Notification for Unsecured Protected Health Information, issued by the Department of Health and Human Services ("HHS"), 45 CFR Part 164, Subpart D, 74 Fed. Reg. 42740 (August 24, 2009) ("HHS Breach Regulations") and applicable Washington state law.

Under the HHS Breach Regulations, the Trust is required to provide notice to the affected individuals, to HHS, and, in certain instances, to the media if a breach of unsecured protected health information of the Trust has occurred, including instances in which the breach occurred regarding the Trust's unsecured protected health information being used or held by Trust's Business Associates. Washington law also requires notification to affected individuals in certain instances where unauthorized individuals may have gained access to personal information held by the Trust.

Prior to January 1, 2012, the Trust provided health benefits to eligible employees of the Everett School through a self-funded health plan. As of January 1, 2012, the Trust provides health benefits through health insurance policies. Almost all of the Protected Health Information ("PHI") of the Trust resides with one or more insurers that issue the health insurance policies ("Insurers"). To the extent that there is a Reportable Breach (as defined below) involving PHI used, held, or maintained by an Insurer, and the Trust receives adequate assurance that the Insurer will comply or has complied with the HHS Breach Regulations and/or applicable Washington state law described in this Policy, the Trust may defer to the Insurer and not duplicate compliance with these rules regarding such a Reportable Breach. To the extent the Insurer is not responsible for the Reportable Breach, or the Insurer does not comply with the HHS Breach Regulations and/or applicable Washington state law, the Trust shall follow this Reportable Breach Notification Policy. The Privacy Officer is responsible for informing the Trust whether additional compliance is required by the Trust after a Reportable Breach of PHI used, held or maintained by an Insurer. All employees and other workforce members of the Trust, the Everett School working on Trust matters, and Business Associates are required to report incidents involving breaches or possible breaches of which they become aware to the Trust's Privacy Officer, even if such incidents are Reportable Breaches which are the responsibility of the Insurer.

***General Procedures***

All breaches of security and/or privacy of information held by or for the Trust need to be analyzed under the following general rules:

- If the information is computerized data that has been encrypted in accordance with NIST standards acceptable under the HIPAA regulations, there are no reportable breaches under either HIPAA or Washington state law unless the breach also involves a compromise of the encryption keys or codes.
- If the information does not involve SSNs, driver's license numbers, or financial account information, Washington state law does not apply.
- For non-encrypted computer information, a breach could trigger a notification requirement under only HIPAA, only under Washington state law, under both, or under neither.
- Washington state law only applies to computer information. HIPAA applies to breaches of both computer and non-computer information.

## I. HIPAA HITECH Rules

*Effective Date*

These procedures apply to breaches discovered on or after September 23, 2009 (note that the date of the discovery of the breach, not the date of the actual breach, controls).

A. **Reportable Breach.** The first step in the HIPAA procedures is to determine whether a Reportable Breach has occurred. If there is not a Reportable Breach, then there is no breach notification requirement ("Notification Requirement"). All employees and other workforce members of the Trust, the Everett School working on Trust matters, and Business Associates are required to report incidents involving breaches or possible breaches to the Trust's Privacy Officer. The Trust's Privacy Officer is responsible for determining if a Reportable Breach has occurred in accordance with the following rules.

1. <u>Reportable Breach.</u> There is a Reportable Breach when all of the following occur:

   a. There is a violation of the HIPAA privacy rule involving "unsecure" PHI.

   b. The violation involved unauthorized access, use, acquisition, or disclosure of unsecure PHI.

   c. The violation resulted in a significant risk of harm to the individual.

   d. One of the exceptions to the Notification Requirement does not apply.

2. <u>Violation of HIPAA Privacy Rule.</u> Was there an impermissible use or disclosure resulting from or in connection with a violation of the HIPAA privacy rule by the Trust or business associate of Trust ("BA")? If not, then there is no Notification Requirement.

a. Was Protected Health Information (PHI) involved? If not, then there is no Notification Requirement.

(1) PHI = Individually identifiable health information

(2) Not PHI if health information has been deidentified (See Appendix A for additional information)

b. Was the PHI secured? If yes, then there is no Notification Requirement**.**

(1) Electronic PHI: must be encrypted to NIST standards to be secured.

(2) Paper PHI: must have been destroyed to be secured.

3. Unauthorized Access, Use, Acquisition or Disclosure of PHI. Did the violation of the HIPAA rules involve any of the following? If not, then there is no Notification Requirement.

a. Unauthorized access of PHI

b. Unauthorized use of PHI

c. Unauthorized acquisition of PHI

d. Unauthorized disclosure of PHI

4. Significant Risk. Did the violation result in significant risk of harm to the individual? If not, then there is no Notification Requirement. This is a risk assessment/judgment call of the Trust based on various factors.

a. Significant risk means *financial risk*, *reputational risk*, or *other risk*.

b. Some factors for the Trust to consider in its risk assessment:

(1) Was the disclosure to another HIPAA covered entity or to federal agency or other entity subject to privacy rules similar to HIPAA privacy rules? **YES = Probably not significant risk of harm to the individual.**

(2) Can the Trust obtain satisfactory assurance or binding agreement from the recipient that the PHI will be destroyed or not further used or disclosed? **YES = Probably not significant risk of harm to the individual.**

(3) Was the PHI in question returned prior to it being accessed for improper purpose (i.e., return of a computer that was not hacked into)? **YES = Probably not significant risk of harm to the individual.**

(4) What was the amount and extent of PHI disclosed? **The greater the amount/extent of the disclosure, the more likely there is significant risk.**

(a) Mere fact that someone was in general hospital may not be significant risk.

(b) However, disclosure of treatment in substance abuse hospital or oncology unit may be significant risk.

(c) The disclosure of SSN, account number, mother's name and other information that poses a higher risk of identity theft is more likely to be a significant risk.

(5) What is the risk that the person can be identified from the PHI? **The greater the risk of identification, the greater the chance of significant risk.**

c. Documentation that Risk is Not Significant. If the Trust decides that there was not a significant risk of harm to the individual, the Trust must document its decision in writing on why the breach did not result in significant harm, and keep the written document on file.

5. Exceptions to the Rule. Is there no Notification Requirement because an exception applies?

a. Exception 1: There is no Notification Requirement if the breach involved an inadvertent unauthorized access, use, acquisition or disclosure to an employee, volunteer, or other workforce member of the Trust or BA and no further Unauthorized Access, Use, Acquisition, or Disclosure occurred, if the:

(1) The unauthorized access, use, acquisition or disclosure was in good faith; and

(2) The unauthorized access, use, acquisition, or disclosure was in scope of authority of workforce member.

(3) Examples:

(a) Inadvertent email to wrong co-worker: exception may apply

(b) Unauthorized employee looks up PHI of neighbor: exception does not apply.

b. Exception 2: There is no Notification Requirement if the breach involved an inadvertent disclosure from one person authorized by Trust to have

access to PHI to another person authorized by the Trust to have access to PHI.

c. Exception 3: There is no Notification Requirement if the breach involved a disclosure where there is a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI.

(1) Examples:

(a) EOB sent to wrong person, but was returned to the Trust unopened.

(b) A report with PHI is handed to a wrong person, but is immediately pulled back before the person can read it.

B. **A Reportable Breach Has Occurred: Timing Issues.** If it is determined that a Reportable Breach has occurred triggering a Notification Requirement, the second step in the procedures is to determine the Discovery Date of the Reportable Breach in order to determine the timing for giving notice of the Reportable Breach.

1. Trigger: Discovery of Reportable Breach. The deadlines for giving Notices of Reportable Breaches are triggered from the date the discovery of the Reportable Breach occurs ("Discovery Date").

2. Discovery Date of the Reportable Breach. The Discovery Date of the Reportable Breach is the earlier of the two following dates:

a. Actual Knowledge. The date that a workforce member (other than a workforce member who committed the Reportable Breach) knows of the Reportable Breach.

(1) Employees must be trained to notify the Trust's privacy officer or other responsible person immediately so the Trust can meet the deadlines.

b. Deemed Knowledge. The date that a Trust workforce member or agent of the Trust (other than the person who committed the Reportable Breach) would have known of the Reportable Breach if the person was exercising *reasonable due diligence*.

(1) *Reasonable due diligence* is the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

(2) The Trust must have reasonable systems and procedures in place to discover the existence of breaches.

c. Rules for Business Associates. If a BA has a Reportable Breach relating to the Trust's participants, the Trust is responsible for giving Notices of Reportable Breaches (the BA must give notice of the Reportable Breach to the Trust).

(1) The Discovery Date for the Trust is the date that the Trust is informed of the Reportable Breach by the BA.

(2) The Trust must require immediate notification of Reportable Breaches by BAs.

(3) In the Business Associates Agreements with BAs, the Trust shall require that (1) the BAs report incidents involving breaches or possible breaches to the Trust's Privacy Officer immediately upon discovery; (2) the BAs provide any and all information to the Trust as requested by the Trust regarding the Reportable Breach, including, but not limited to, the information described in D.1. below; and (3) the BAs have procedures and policies in place to comply with the HHS Breach Regulations, including appropriate workforce training regarding the procedures, policies, and the HHS Breach Regulations. In addition the Trust may require the BAs to pay some or all of the costs relating to Reportable Breaches of unsecured PHI by the BAs, including, but not limited to, the costs of developing and providing notice(s) under the HHS Breach Regulations and mitigating the effects of such Reportable Breaches.

3. Deadlines for Notices

a. Notices must be given "without unreasonable delay" but in no event later than 60 calendar days after the "Discovery Date".

(1) This means that the investigation of whether there is a Reportable Breach and if so, to whom the Reportable Breach applies, must be done in a reasonable amount of time.

(2) Examples:

(a) Investigation is completed fifteen days after the Discovery Date. Notices must be given shortly thereafter (20-25 days after the Discovery Date) because waiting until day 55 would be an unreasonable delay.

(b) Investigation is undertaken immediately and completed 57 days after the Discovery Date. Notice must be given by 60 calendar days after the discovery date.

b. There is an exception to these rules if a law enforcement official requests that the Trust delay giving the Notices.

c. Urgent Notices (see D. 3.) must be given sooner.

C. **Types of Required Notices of the Reportable Breach; Responsibility for Notices**

1. Notices to Individual (See Section D)

a. Actual Notice

b. Substitute Notice

c. Urgent Notice

2. Notice to Prominent Media Outlets. (if the Reportable Breach involved 501 or more residents of a State or other jurisdiction) (See Section E)

3. Notice to HHS (See Section F)

a. The Reportable Breach involved 500 or more affected persons: immediate notice to HHS.

b. Annual report to HHS of Reportable Breaches with less than 500 affected individuals.

4. Privacy Officer Responsible for Notices. The Trust's Privacy Officer is responsible for the content of the Notices and for delivering the Notices in a timely manner in accordance with rules set forth below.

D. **Notice to Individuals.** The Notice to Individuals is always required and must be written in plain language.

1. Required Contents of Notice to Individuals. The Notice to Individuals must contain all of the following:

a. A brief description of incident.

b. If known, the date of the Reportable Breach and Discovery Date.

c. Description of PHI involved in the Reportable Breach (for example, full name, SSN, address, diagnosis, date of birth, account number disability code, or other).

d. The steps individuals should take to protect themselves. Examples:

(1) Contact credit card company

(2) Contact credit bureaus

(3) Obtain credit monitoring services

e. A description of what the Trust is doing to investigate the Reportable Breach. Example:

(1) Filing police report

(2) Reviewing security logs or tapes

f. A description of what the Trust is doing to mitigate harm to individuals.

g. A description of what measures the Trust is taking to protect against further breaches. Examples:

(1) Sanctions imposed on workforce members involved in the Reportable Breach

(2) Encryption

(3) Installing new firewalls

h. Contact information where individuals can learn more about the Reportable Breach or ask other questions, which must include one of the following:

(1) Toll-free phone number

(2) Email address

(3) Website

(4) Postal address

2. Forms of Notices to Individuals

a. Actual Notice (see D.1 for required contents)

(1) Sent first class mail to last known address of the individual(s).

(2) Can be sent via email if the individual has agreed to receive electronic notices.

(3) Sent to the parent of minor child

(4) Sent to next-of-kin or personal representative of deceased person

b. Substitute Notice. The Substitute Notice must have the same contents as Actual Notice (see D.1. for required contents).

(1) If the Trust has insufficient or out-of-date addresses, then Substitute Notice is required.

(2) If addresses of fewer than 10 living individuals are insufficient or out-of-date, Substitute notice can be given in the following manner:

(a) Telephone notice

(b) Notice in person

(c) Email notice

(3) If addresses of 10 or more living individuals are insufficient or out-of-date, Substitute Notice must be given in one of the two following manners:

(a) Website. Conspicuous posting on home page of the Trust website for 90 days, including toll-free number which can be called to obtain information about the Reportable Breach

(i) Contents of the Notice (see D.1.) can be provided directly on website or via hyperlink.

(b) Media. Conspicuous notice in major print or broadcast media in the geographic areas where the individuals affected by the Reportable Breach likely reside, including toll-free number which can be called to obtain information about the Reportable Breach.

(i) May have to give notice in both local media outlet(s) and state-wide media outlet(s)

(4) Substitute Notice is only required for living persons.

3. Urgent Notice

a. The Urgent Notice is required where possible imminent misuse of unsecured PHI may occur.

b. The Urgent Notice must be given by telephone or other appropriate means.

c. The Urgent Notice is required in addition to the other Notices that are required. Example:

(1) Urgent Notice is given to Trust participant by telephone call. The Trust must also send Individual Notice via first class mail to the Trust participant.

E. **Notice to Media (Press Release)**

1. The Notice to Media is required where the Reportable Breach involves more than 500 residents of Washington (or 500 residents of any one State or jurisdiction). Examples:

   a. Reportable Breach involves 600 residents of Washington: Notice to Media required

   b. Reportable Breach involves 450 residents of Washington and 60 residents of Oregon. Notice to Media not required.

2. The Notice to Media must be given to prominent media outlets serving the State or jurisdiction.

   a. If the Reportable Breach involves residents of one city, the prominent media outlet would be the city's newspaper or TV station.

   b. If the Reportable Breach involves residents of various parts of the state, the prominent media outlet would be state-wide newspaper or TV station.

3. The Notice to Media must contain the required items listed in D.1.

4. Like other Notices, the Notice to Media must be given without unreasonable delay, and at least within 60 calendar days of the discovery of the Reportable Breach.

F. **Notification to HHS Secretary**

1. **Immediate Notice**. This Notice is required where the Reportable Breach involves 500 or more individuals, regardless of where the individuals reside. Example:

   a. Reportable Breach involves 450 residents of Washington and 60 residents of Oregon: Notice to HHS required.

   b. Like other Notices, this Notice must be given without unreasonable delay, and at least within 60 calendar days of the discovery of the Reportable Breach.

   c. Notice will be given to HHS as directed on the HHS website.

2. **Yearly Report of Reportable Breaches**. If the Reportable Breach involves less than 500 individuals, the Trust must keep a log of the Reportable Breaches and submit a report on the Reportable Breaches to HHS every year by the last day in February (60 calendar days after January 1st) covering the Reportable Breaches which occurred in the preceding calendar year. The reports will be given to HHS

as directed on the HHS website. The Trust's Privacy Officer is responsible for filing such reports.

G. **Training**

1. The Trust's Privacy Officer shall cause appropriate workforce members of the Trust and/or Trust Sponsor to receive training in the rules described in these procedures.

## II. WASHINGTON STATE BREACH NOTIFICATION RULES

A. **Requirements for Reportable Breach under Washington State Law.** There is a Reportable Breach under Washington law if the breach involves the following:

1. **Breach Involves Name Plus SSN, Driver's License, or Financial Account Information.** Washington state law only applies if the breach of involves the **first name or initial and last name** together with one or more of the following:

   a. SSN

   b. Driver's license number or Washington identification card number

   c. Account number or credit or debit card number in combination with any required security code, access code r password that would permit access to the person's financial account

2. **Breach Involves Security of a Computer System**. Washington state law only applies if there has been an unauthorized acquisition by an unauthorized person of unencrypted computerized data that compromises the security, confidentiality, or integrity of the information described in A.1.

3. **Exception.** Notice is not required for technical breach of a security system that does not seem reasonably likely to subject the person to a risk of criminal activity.

B. **Notice Requirement.** If a Reportable Breach has occurred under Washington law, the Trust must disclose the breach to the individual "in the most expedient time possible and without unreasonable delay." Written notice (presumably sent to the person's address) is the method to provide notice. Substitute notice provisions apply if (1) the cost of providing written notice would exceed $250,000; (2) the number of persons is more than 500,000; or (3) there is insufficient contact information for the person. Substitute notice can be provided by email, by conspicuous posting on the Trust's website, or notification to major statewide media.

## APPENDIX

**Deidentified Information**

Health information is considered to be deidentified if the following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

C. Names;

D. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes.

E. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

F. Telephone numbers;

G. Fax numbers;

H. Electronic mail addresses;

I. Social security numbers;

J. Medical record numbers;

K. Health plan beneficiary numbers;

L. Account numbers;

M. Certificate/license numbers;

N. Vehicle identifiers and serial numbers, including license plate numbers;

O. Device identifiers and serial numbers;

P. Web Universal Resource Locators (URLs);

Q. Internet Protocol (IP) address numbers;

R. Biometric identifiers, including finger and voice prints;

S. Full face photographic images and any comparable images; and

T. Any other unique identifying number, characteristic, or code, and the Trust does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.