6. Risk Management Activities

6.01 Overview

6.02 Training

6.03 Complaints

6.04 Sanctions

6.05 Mitigation

6.06 Document Retention

6.01 Overview

The Plan must participate in certain risk management activities to ensure compliance with the HIPAA Privacy Rule including:

- Everett School District employees and Board of Trustees training on the Policies and Procedures for use, disclosure and general treatment of PHI (see Section 6.02);
- Developing a complaint process for individuals to file complaints about the Plan's Policies and Procedures, practices, and compliance with the HIPAA Privacy Rule (see Section 6.03);
- Designing a system of written disciplinary policies and sanctions for Everett School District employees and Board of Trustees who violate the HIPAA Privacy Rule (see Section 6.04);
- Mitigating damages known to the Plan resulting from improper use or disclosure of PHI (see Section 6.05); and
- Retaining copies of its Policies and Procedures, written communications, and actions or designations (see Section 6.06).

Some of these risk management rules require Covered Entities to design processes affecting workforce members under its control. Since the Plan itself has no workforce, it will comply by requiring Business Associates, Insurers, and the Plan's Administrator to implement the required activity. Sections 6.02 through 6.06 describe the Procedures developed by the Plan's Administrator.

6.02 Training

HIPAA generally requires Covered Entities to provide training to all current and future workforce members under their direct control on the use, disclosure, and general treatment of PHI. Since the Plan itself has no workforce members, Everett School District employees and Board of Trustees will be trained to ensure that the Plan meets its obligations under this Manual (including limiting the use, disclosure of PHI as required under Section 4). This training will occur no later than April 14, 2003. The Privacy Official or his or her designee will coordinate the training. Business Associates and Insurers will separately engage in training activities as needed to ensure they meet their responsibilities under the HIPAA Privacy Rule and Business Associate Agreements (as applicable).

a. When Training will Occur

Everett School District employees and Board of Trustees who will have access to PHI will receive privacy training as part of their initial training. Everett School District employees and Board of Trustees who change positions or when a material change in the Plan's Policies and Procedures will receive new privacy training at the time of the change. The retraining will occur within a reasonable period of time after the Plan changes its Policies and Procedures.

b. Contents of Training

Everett School District employees and Board of Trustees will receiving training on the use and disclosure of PHI including the protection, permissible disclosures, and general treatment of PHI.

The following topics are to be covered in the training:

Training topic	Section
The definition of PHI	3.01 and 8.08
The Plan's processes for using and disclosing PHI (include applicable state-specific requirements)	4.01 - 4.06
The Plan's processes for handling Authorizations	4.04 and 7.06
How to respond to requests for PHI from various parties (family members, law enforcement, etc.)	4.05
The Plan's physical safeguard procedures for protecting PHI	3.01 - 3.03
The identification of the Privacy Official and his or her duties and contact information	1 and 10.02
The identification of Business Associates	10.04

Training topic	Section
An explanation of the Plan's internal complaint procedures	6.03
How to respond when a violation of the HIPAA Privacy Rule or the Plan's Policies and/or Procedures occurs	6.05
The possible sanctions if an Everett School District employee or Board of Trustee violates the HIPAA Privacy Rule or the Plan's Policies and Procedures	6.04

c. Documentation

Documentation of privacy training will be maintained by the Privacy Official for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

The documentation of privacy training will include:

Description of documentation	The Plan's specifics	Done
The forum used to train Everett School District employees and Board of Trustees, including information on whether training is through personal instruction, web-based instruction, individual study, etc.	Training done by personal instruction.	Yes
Information on the training presentation, including the name of the training program, its location and date, the workforce groups attending, etc.	• HIPAA Privacy Training on April 10, 2003 from 10:00 a.m. – 12:00 p.m. at the Longfellow Annex. Workforce groups include Human Resources, Finance/Payroll and Information Systems & Technology • HIPAA Privacy Training on April 28, 2003 from 2:00 p.m. to 3:00 p.m. at the Longfellow Annex. Makeup session for workforce groups unable to attend April 10th which are Human Resources and Finance/Payroll • HIPAA Privacy Training on April 28, 2003 at 3:30 p.m. in the Human Resources Conference Room at the Longfellow Building. Training for all Trustees.	Yes
A description and a copy of the training materials.	PowerPoint presentation and distribution/review of the Everett School	Yes

Description of documentation	The Plan's specifics	Done
	Employee Benefit Trust HIPAA Privacy Manual	
Information on the presenter including background, qualifications, contact information, etc.	Presenter: Jill Mehner of Mercer Human Resource Consultant	Yes
Training attendance records, including directions given to each training location on required information for such records	Attendance records kept in a file folder entitled, "HIPAA PHI Privacy Training" along with a copy of correspondence confirming attendance of workforce members.	Yes
Evaluation summaries of the training course, if applicable		

The Privacy Official may document the above information separately for different offices, locations, or workforce groups, as necessary.

d. Citations

45 CFR § 164.530(b)

6.03 Complaints

The Plan is required to create a process for persons to file complaints about the Plan's Policies and Procedures, practices, and compliance with the HIPAA Privacy Rule. This Section describes the complaint process for self-funded Plan benefits. Insurers will develop procedures to process complaints about insured benefits as required under the HIPAA Privacy Rule.

a. Filing Complaints

Complaints should be filed by completing the Complaint Form including a description of the nature of the particular complaint and sending the completed Complaint Form to the Complaint Manager.

b. Processing Complaints and Complaint Resolution

Complaint Manager will review the complaint, address the situation, consult with the proper individuals (if necessary), and attempt to come to an appropriate resolution of the complaint.

The resolution will depend on the particular facts and circumstances of the complaint. Examples of complaint resolution include:

- Educating the individual about the Plan's Policies and Procedures or practices;
- Implementing changes in the Plan's Policies and Procedures or practices;
- Providing additional training for Everett School District employees and Board of Trustees on the Plan's Policies and Procedures, the HIPAA Privacy Rule, or other applicable laws or regulations;
- Discussing a complaint with the relevant parties and, if necessary, imposing sanctions on individuals who violate the Plan's Policies and Procedures or the HIPAA Privacy Rule; and
- Issuing new workforce communication materials or a revised Privacy Notice regarding the Plan's Policies and Procedures.

If, at any time, an individual wants to know the status of his or her complaint, he or she should contact Complaint Manager.

Once Complaint Manager has resolved a complaint, he or she will send a written or electronic communication to the individual who filed the complaint explaining the resolution.

c. Documentation

The Plan's Administrator will maintain a record of the complaints and a brief explanation of their resolution, if any, for a period of six (6) years.

d. Citations

45 CFR § 164.530(d)

6.04 Sanctions

Covered Entities are required to design a system of written disciplinary policies and sanctions for workforce members who violate the HIPAA Privacy Rule. Since the Plan itself has no workforce members, the Plan Administrator will implement procedures to apply sanctions against its workforce members who violate the Plan's Policies and Procedures or the HIPAA Privacy Rule. Business Associates and Insurers will take whatever steps are required to ensure their compliance with the HIPAA Privacy Rule and Business Associate Agreements (as applicable).

a. Determining Sanctions

The Plan's Administrator will determine a sanction at the time of a violation and will base the sanction on the nature of the violation. Factors taken into account will include the severity of the violation, whether it was intentional or unintentional, and whether it indicated a pattern or practice of improper use or disclosure of PHI. Examples of possible sanctions include:

- Retraining and review of policies and procedures;
- Verbal warnings;
- Written warnings;
- Probationary periods; and
- Termination of employment.

The Plan's Administrator will not apply sanctions against Everett School District employees and Board of Trustees who refuse to follow a Policy or Procedure that they believe, in good faith, violates the HIPAA Privacy Rule, if the refusal is reasonable and does not involve a disclosure of PHI. In addition, the Plan's Administrator will not apply sanctions against Everett School District employees and Board of Trustees who file a complaint with any entity about a privacy violation.

b. Documentation

The Plan's Administrator will document in writing (or in an electronic medium) all sanctions it applies. The Plan's Administrator will retain the documentation of any sanctions it applies for six (6) years.

c. Citations

45 CFR § 164.530(e)

6.05 Mitigation

The Plan is required to mitigate any harmful effects that it knows have resulted from improper use or disclosure of PHI by Everett School District employees, Board of Trustees or Business Associates in violation of the Plan's Policies and Procedures or the HIPAA Privacy Rule. To meet this obligation, the Plan will require Business Associates to mitigate, to the extent practicable, any harmful effects from improper uses and disclosures of PHI known to them. Insurers are also required to mitigate such harmful effects under the HIPAA Privacy Rule.

a. Mitigation Steps

If the Plan's Administrator knows of harmful effects resulting from its own improper use or disclosure of PHI, the Privacy Official will consider a variety of steps, including:

- Investigating the facts and circumstances of the use or disclosure of PHI;
- Contacting the affected parties;
- Reviewing the PHI in question;
- Assisting the affected parties, and
- Contacting the workforce member(s) or the Business Associate(s) involved in the situation.

The Privacy Official will conduct the mitigation activities.

In addition, the Privacy Official may apply sanctions (see Section 6.04) against Everett School District employees or Board of Trustees who violate the Plan's Policies and Procedures or the HIPAA Privacy Rule.

b. Citations

45 CFR § 164.530(f)