Everett School Employee Benefit Trust

HIPAA Privacy Manual

Implementation Date: April 14, 2003

As prepared by:

Everett School District
Human Resources Department
3715 Oakes Avenue
Everett, WA 98201

Table of Contents

1. Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the US Department of Health and Human Services (HHS) to establish rules to protect the privacy of health information. HHS issued detailed rules (referred to throughout this Manual as the HIPAA Privacy Rule), for health plans, health care providers, and certain other health care entities (known as Covered Entities). Health information covered by the HIPAA Privacy Rule is known as Protected Health Information (PHI).

Words and phrases that are capitalized in this Manual, such as "Covered Entities," have special meanings that are defined in Section 8.

The Board of Trustees sponsors the Everett School Employee Benefit Trust ("Plan") described in Section 10.01. Health plans and other Covered Entities are required to create Policies and Procedures to ensure their compliance with the HIPAA Privacy Rule. This Manual includes the Policies and Procedures for the Plan. Because each Plan is sponsored by Everett School Employee Benefit Trust they collectively comprise an "organized health care arrangement" and the Manual represents the policies and procedures for each Plan. The HIPAA Privacy Rule and this Manual are effective on and after April 14, 2003.

The Manual consists of ten (10) sections.

Section 1, this introduction, describes the purpose of the Manual and its organization.

Section 2 describes the Plan's overall policy for protecting the use and disclosure of health information.

Sections 3 and 4 describe the basic requirements that apply to the Plan's use and disclosure of PHI. The sections also describe the procedures Everett School Employee Benefit Trust will use when handling health information for the Plan.

Section 5 describes certain rights that Plan Participants and their beneficiaries have concerning their own PHI, and the Plan's procedures for administering those rights.

Sections 6 and 7 describe risk management requirements that the Plan must meet and documentation that the Plan must maintain. The sections also describe Everett School Employee Benefit Trust's risk management activities for actions it performs on the Plan's behalf.

Section 8 defines key terms that are used in this Manual. The defined terms are capitalized throughout the Manual. *In general, the term Participant is used to refer to persons who are or*

were eligible for benefits under the Plan. Participant is used to refer to both employee Participants and other beneficiaries, unless the context clearly indicates otherwise.

Section 9 contains the text of the HIPAA Privacy Rule.

Section 10 contains key resources related to the implementation of this Manual. It includes the name of the Privacy Official responsible for the development, coordination, implementation, and management of the Manual. It also includes key contacts (persons or offices) responsible for responding to Participants exercising their rights described in Section 5, for receiving complaints about the Plan's compliance with the Manual or with the HIPAA Privacy Rule, and for processing any specific Authorizations that Participants may be asked to provide concerning the use of their PHI. Finally, it includes the forms and other Plan Documents that the Plan's Administrator will be using to meet the privacy requirements, along with instructions for using those forms.

The Manual will be provided to employees of Everett School District and Board of Trustees who have access to PHI. In this document, we are referring to those health plans covered under HIPAA and Plan's Administrator encompasses both employees of Everett School District and the Board of Trustees. The Plan's Administrator will also receive updates that reflect any changes in law or the Manual's procedures. Employees can obtain more information from the Plan's Privacy Official and other contacts listed in Section 10.

*Health information collected by the Plant pursuant to other laws such as the Family and Medical Leave Act, Americans with Disabilities Act, Occupational Safety and Health Act, or workers' compensation laws, is **not** protected under HIPAA as PHI (although this type of information may be protected under other federal or state laws). Employees should consult Human Resources for District privacy policies governing employee information not connected with the Plan.*

2. Statement of Privacy Policy

The Plan will protect the privacy of Participant and family member health information (known as Protected Health Information or PHI) in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and applicable state law. PHI generally will be used only for health plan Payment activities and operations, and in other limited circumstances such as where required for law enforcement and public health activities. In addition, the Minimum Necessary information will be used except in limited situations specified by law. Other uses and disclosures of PHI will not occur unless the Participant authorizes them. Participants will have the opportunity to inspect, copy, and amend their PHI as required by HIPAA. Participants can exercise the rights granted to them under HIPAA free from any intimidating or retaliatory acts.

When PHI is shared with Business Associates providing services to the Plan, they will be required to agree in writing to maintain procedures that protect the PHI from improper uses and disclosures in conformance with HIPAA.

When the Plan's Administrator receive PHI to assist in Plan administration, it will adhere to its own stringent procedures to protect the information. Among the Procedures in place are:

- Administrative and technical firewalls that limit which groups of employees are entitled to access PHI and the purposes for which they can use it;
- Rules for safeguarding PHI from improper disclosures;
- Processes to limit the disclosure of PHI to the Minimum Necessary;
- A verification process to identify and confirm the authority of persons requesting PHI;
- A training process for relevant staff; and
- Processes for filing privacy complaints.

The Plan may update this Policy and its Procedures at any time. The Plan will also update this Policy and its Procedures to reflect any change required by law. Any changes to this Policy and Procedures will be effective for all PHI that the Plan may maintain. This includes PHI that was previously created or received, not just PHI created or received after the Policy and Procedures are changed.

3. Safeguards

3.01 Overview

3.02 Protection Procedures

3.03 Verification Procedures

3.01 Overview

The Plan will develop and implement administrative, technical, and physical safeguards that will reasonably protect Protected Health Information (PHI) from intentional and unintentional uses or disclosures that violate the HIPAA Privacy Rule. In addition, the Plan will institute procedures to verify the identity of any person or entity requesting PHI and the authority of that person or entity to have access to PHI.

PHI is individually identifiable health information created or received by a Covered Entity or employer. Information is "individually identifiable" if it identifies the individual or there is a reasonable basis to believe components of the information could be used to identify the individual. Information is protected whether it is in writing, in an electronic medium, or communicated orally. "Health information" means information, whether oral or recorded in any form or medium, that (i) is created or received by a health care provider, health plan, employer, life Insurer, public health authority, health care clearinghouse or school or university; and (ii) relates to the past, present, or future physical or mental health or condition of a person, the provision of health care to a person, or the past, present, or future Payment for health care.

Sections 3.02 and 3.03 describe the Procedures the Plan's Administrator will use to establish safeguards and to verify identification and authority when using PHI. Insurers and Business Associates of the Plan will also adopt procedures that meet the requirements of the HIPAA Privacy Rule.

3.02 Protection Procedures

The Plan's Administrator will apply the following Procedures to protect PHI:

Protected information	Protection procedures
Printed/hard copy documentation	• Funnel incoming mail through distinct channels to limit the number of people with access to PHI. • Limit the number of photocopies made of PHI. • Implement a "clean desk" practice. PHI will be put away if the employee is away from his or her desk throughout the day and PHI will be placed in closed and locked drawers or cabinets when the employee is not in the office. • PHI that the Plan is required to retain for lengthy time frames will be kept in off-site storage areas, with access limited to designated personnel. • PHI in paper format will be destroyed when it is obsolete or is not required to be retained for storage purposes, with shredding the preferred method of destruction.
E-mail and electronic storage (LAN/hard drive/diskettes)	• Destroy electronic PHI that is no longer needed, including cutting or destroying CDs or diskettes so that they are not readable. • Limit the use of PHI in e-mails to the Minimum Necessary (e.g., refrain from forwarding strings of e-mail messages containing PHI. Instead, prepare a new message, with only the Minimum Necessary information.) • Encrypt e-mail information as needed. • Require password entry each time an employee accesses the e-mail system. • Use "locking" screensavers to limit access. • Maintain and periodically update network monitoring software, including intrusion detection and reporting. • Maintain and periodically update systems for backing up data and contingency plans for data recovery in the event of a disaster.

Protected information	Protection procedures
	• Maintain and periodically update systems for tracking access and changes to data. • Periodically review the process for handling system maintenance and the hardware/software acquisition process. • Maintain and periodically update virus software and protection processes. • Maintain and periodically review procedures for ending data access for staff (e.g., after they terminate employment). • Follow other District IT guidelines regarding electronic data. • Limit remote access to systems to secure methods
Facsimiles	• Ensure that designated fax machines are not located in publicly accessible areas. • Develop fax coversheet including confidentiality statement and warning about releasing data. • Limit faxing of PHI to urgent information. • Notify the receiver that the Plan's Administrator is sending a fax so he or she can retrieve it immediately. • Check confirmation sheets to verify that outgoing faxes were received by the correct number.

Protected information	Protection procedures
Oral conversations/ Telephone calls/ voicemail	• Limit the content of PHI in conversations (e.g., with vendors and other staff) to the Minimum Necessary. • Verify the identity of individuals on the telephone. • Implement reasonable measures to prevent other individuals from overhearing conversations, e.g., using speakerphone only when in a closed office. • Limit voicemail messages, or messages left for other individuals, to high-level information to ensure no one else could over hear PHI.

3.03 Verification Procedures

In performing administration activities for the Plan, the Plan's Administrator will implement the following verification procedures to reasonably ensure the accurate identification and authority of any person or entity requesting PHI. Note that documentation of these verifications should be retained as provided in Section 6.06. Insurers and Business Associates will also institute verification procedures for disclosures of PHI.

Who makes the request	Procedure
Participants, Beneficiaries, and others acting on their behalf	The Plan's Administrator may obtain photo identification, a letter or oral Authorization, marriage certificate, birth certificate, enrollment information, identifying number, and/or claim number.
Health plans, providers, and other Covered Entities	The Plan's Administrator may obtain identifying information about the entity and the purpose of the request, including the identity of a person, place of business, address, phone number, and/or fax number known to the Plan.
Public officials	For in-person requests, obtain agency identification, official credentials or identification, or other proof of government status. For written requests, verify they are on the appropriate government letterhead. Also obtain a written (or, if impracticable, oral) statement of the legal authority under which the information is requested.*
Person acting on behalf of a public official	Obtain a written statement on appropriate government letterhead or other evidence or documentation of agency (such as a contract for services, memorandum of understanding, or purchase order) that establishes that the person is acting on behalf of the public official.
Person acting through legal process	Obtain a copy of the applicable warrant, subpoena, order, or other legal process issued by a grand jury or judicial or administrative tribunal.
Person needing information based on health or safety threats	Consult with Privacy Official. Disclosure is permitted if, in the exercise of professional judgment, the Plan's Administrator concludes the disclosure is necessary to avert or lessen an imminent threat to health or safety, and that the person to whom the PHI is disclosed can avert or lessen that threat.

*The Plan's Administrator will rely on the statements and documents of public officials unless such reliance is unreasonable in the context of the particular situation.

a. Citations

45 CFR § 164.514(h)