HIPAA PRIVACY POLICY

Everett School Employee Benefit Trust

January 1, 2012

HIPAA PRIVACY POLICY

I. INTRODUCTION

The Everett School Employee Benefit Trust ("Trust") provides group health plan benefits (collectively the "Group Health Plan") for eligible employees of the Everett School District ("District"). The Group Health Plan is sponsored by the District and the Everett Education Association (collectively the "Plan Sponsor"). The Group Health Plan is subject to the privacy rules of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations ("Privacy Rules").

It is the Trust's and the Plan Sponsor's policy that the Group Health Plan complies with HIPAA's requirements for the privacy of protected health information ("PHI"). Thus, all members of the Trust's workforce who have access to PHI relating to the Group Health Plan must comply with this Policy. For purposes of this Policy, the Trust's workforce ("Workforce") includes all individuals who would be considered part of the workforce under HIPAA, including Trustees of the Trust and employees of the District with access to PHI of the Group Health Plan.

Members of Workforce may have access to PHI of employees, dependents and other persons participating in the Group Health Plan ("Participants"):

- on behalf of the Group Health Plan; or
- on behalf of the Trust, for administrative functions of the Group Health Plan and other purposes permitted by the Privacy Rules.

HIPAA restricts the ability of the Group Health Plan and the Trust to use and disclose PHI.

For purposes of this Policy, PHI means information that is created or received by the Group Health Plan that identifies an individual (or for which there is a reasonable basis to believe the information can be used to identify the individual) and relates to:

- the past, present, or future physical or mental health or condition of an individual;
- the provision of health care to an individual; or
- the past, present, or future payment for the provision of health care to an individual.

PHI includes information of persons living or deceased. PHI includes information relating to such things as health status, medical condition, claims experience, receipt of health care, payment for health care, medical history, genetic information, and evidence of insurability. PHI does not include health information received from sources other than the Group Health Plan.

Almost all of the Group Health Plan's benefits are provided pursuant to insurance policies issued by insurance companies. The companies issuing health insurance coverage ("Health Insurance Issuers") are also subject to HIPAA and the Privacy Rules, and this Policy is complementary and supplementary to the HIPAA privacy policies of the Health Insurance Issuers. To the extent that PHI of the Group Health Plan is under the control of a Health Insurance Issuer, and has not been

disclosed or released to any member of the Workforce, the Health Insurance Issuer has primary responsibility for compliance with the Privacy Rules of HIPAA.

No third party rights (including, but not limited to, rights of Participants or Business Associates of the Group Health Plan) are created by or intended to be created by this Policy. The Trust reserves the right to amend or change this Policy at any time (even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy is aspirational and is not legally binding upon the Group Health Plan or the Trust. This Policy does not address requirements under other federal laws or under state laws. To the extent this Policy is in conflict with the HIPAA Privacy Rules, the HIPAA Privacy Rules shall govern.

II. PLAN'S RESPONSIBILITIES AS A COVERED ENTITY

A. Privacy Official and Contact Person

Molly Ringo, or such other person so designated by the Trust as her successor, is the privacy official for the Group Health Plan ("Privacy Official"). The Privacy Official is responsible for the development and implementation of policies and procedures relating to privacy of the PHI of the Group Health Plan, including this Policy. The Privacy Official of the Trust or a Privacy Official of the Health Insurance Issuer may serve as the contact person for Participants who have questions, concerns, or complaints about the privacy of their PHI.

The Privacy Official is also responsible for ensuring that the Group Health Plan is in compliance with the provisions of the Privacy Rules regarding Business Associates, including the requirement that the Group Health Plan have a HIPAA-compliant Business Associate Agreement in place with all Business Associates. The Privacy Official shall monitor compliance by all Business Associates with the Privacy Rules and this Policy.

B. Workforce Training

The Trust will provide training to members of the Workforce who have access to PHI of the Group Health Plan in HIPAA and this Policy. The Privacy Official is charged with developing training schedules and programs so that Workforce members with access to PHI receive the training necessary and appropriate to permit them to carry out their functions relating to the Group Health Plan in compliance with HIPAA.

C. Safeguards and Firewall

Appropriate administrative, technical, and physical safeguards have been established to help prevent PHI use or disclosure (intentional or unintentional) in violation of HIPAA's requirements. Administrative safeguards include implementing procedures for use and disclosure of PHI. Technical safeguards include limiting access to information by creating computer-firewalls. Firewalls ensure that only authorized Workforce members have access to PHI, that they have access to only the minimum amount of PHI necessary, and that they do not

further use or disclose PHI in violation of the Privacy Rules. Physical safeguards include locking doors or filing cabinets containing PHI.

D. Privacy Notice

The Privacy Official is responsible for assuring that the Group Health Plan has a notice of the privacy practices ("Privacy Notice") that describes:

- the uses and disclosures of PHI that may be made by the Group Health Plan;
- the rights of individuals under the Privacy Rules;
- the legal duties of the Group Health Plan with respect to the PHI; and
- other information as required by the Privacy Rules.

The Privacy Official may rely on Privacy Notice of the Health Insurance Issuers or may develop and utilize a separate Privacy Notice for the Trust. The Privacy Notice will contain a description of the complaint procedures for the Group Health Plan, the name and telephone number of the contact person for further information, and the date of the notice.

The Privacy Notice is located on the Trust's or the Health Insurance Issuer's website. The notice is also individually delivered:

- on an ongoing basis, at the time of an individual's enrollment in the Group Health Plan;
- to Participants requesting the notice; and
- to Participants within 60 days after a material change to the notice.

A notice of availability of the Privacy Notice (or a copy of the Privacy Notice itself) is distributed at least once every three years in compliance with the Privacy Rules.

E. Complaints

The contact person for receiving HIPAA privacy complaints regarding the Group Health Plan is:

Molly Ringo, Ed. D.
4730 Colby Avenue
Everett, WA 98203
425-385-4023

Upon request, the contact person will provide the Group Health Plan's process for individuals to lodge complaints about the Group Health Plan concerning the Privacy Rules and the system for handling such complaints. A copy of the complaint procedure shall be provided to any Participant upon request.

Complaints concerning HIPAA violations by a Health Insurance Issuer will be forwarded to the HIPAA contact person for the Health Insurance Issuer.

F. Workforce Sanctions for Violations of Privacy Policy

Workforce members are subject to sanctions for using or disclosing PHI in violation of Privacy Rules in accordance with the District's disciplinary rules for employees, up to and including termination. These rules are available upon request from the District's human resources department.

G. Mitigation of Inadvertent Disclosures of PHI

The Trust shall mitigate, to the extent possible, any harmful effects that are known to have resulted from a use or disclosure of an individual's PHI by a member of the Workforce in violation of the Privacy Rules or this Policy. If a Workforce member or Business Associate becomes aware of an unauthorized use or disclosure of PHI (either by a Workforce member or an outside consultant/contractor), the Workforce member or Business Associate must immediately contact the Privacy Official so that appropriate steps to mitigate the harm to the individual can be taken.

H. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No Workforce member may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment, or eligibility under the Group Health Plan.

I. Plan Document

The Group Health Plan documents include provisions describing the permitted and required uses and disclosures of PHI the Group Health Plan for administrative or other permitted purposes.

J. Documentation

This Policy and all other of the privacy policies and procedures relating to the Group Health Plan are documented and maintained for at least six years from the date last in effect. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements, and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

The Privacy Official shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. Such documentation will be maintained for at least six years.

III. POLICIES ON USE AND DISCLOSURE OF PHI

A. Use and Disclosure Defined: Other Definitions

The Group Health Plan will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use.* The sharing, employment, application, utilization, examination, or analysis of PHI by any person working for or on behalf of the Group Health Plan or by a Business Associate (defined below) of the Group Health Plan.
- *Disclosure.* For information that is PHI, disclosure means any release, transfer, provision of access to, or divulging in any other manner of PHI to persons who are not employees of the Health Insurance Issuers or who are not members of the Workforce.

Terms used but not otherwise defined in this document shall have the meaning given the terms in the HIPAA Privacy Rules.

B. Workforce Must Comply with the Policy

All members of the Workforce who have access to PHI of the Group Health Plan must comply with this Policy.

C. Permitted Uses and Disclosures for Plan Administrative Purposes

The Group Health Plan may disclose to the Workforce the following:

- de-identified health information relating to Participants;
- enrollment information;
- summary health information (as that term is defined in the Privacy Rules) for the purposes of obtaining premium bids for providing health insurance coverage under the Group Health Plan or for modifying, amending, or terminating the Group Health Plan; or
- PHI pursuant to an authorization from the individual whose PHI is disclosed.

The Group Health Plan may disclose PHI to members of the Workforce who have access to use and disclose PHI to perform functions on behalf of the Group Health Plan or to perform plan administrative functions ("Employees with Access").

Employees with Access may disclose PHI to other Employees with Access for administrative functions relating to the Group Health Plan (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with Access may not disclose PHI to employees (other than Employees with Access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and the Privacy Use and Disclosure Procedures. Employees with Access must take all appropriate steps

to ensure that the PHI is not disclosed, available, or used for employment purposes. For purposes of this Policy, "plan administrative functions" include the payment and health care operation activities described in Section III. D. of this Policy.

D. Permitted Uses and Disclosures: Payment and Health Care Operations

PHI may be disclosed for the payment purposes of the Group Health Plan, including use by and disclosures to a Business Associate of the Group Health Plan, and PHI may be disclosed to another Covered Entity for the Payment purposes of that Covered Entity. These uses and disclosures do not require an authorization from the individuals whose PHI is being used or disclosed.

Payment. Payment includes activities undertaken to obtain contributions to the Group Health Plan or to determine or fulfill the responsibility for provision of Group Health Plan, or to obtain or provide reimbursement for health care. Payment also includes:

- eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;
- risk-adjusting based on enrollee status and demographic characteristics;
- billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing; and
- any other payment activities permitted by the Privacy Rules.

PHI may be disclosed for purposes of the health care operations of the Group Health Plan. PHI may be disclosed to another Covered Entity for purposes of the other Covered Entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other Covered Entity has (or had) a relationship with the Participant and the PHI requested pertains to that relationship.

Health Care Operations. Health care operations means any of the following activities:

- conducting quality assessment and improvement activities;
- reviewing health plan performance;
- underwriting and premium rating;
- conducting or arranging for medical review, legal services and auditing functions;
- business planning and development;
- business management and general administrative activities; and
- other health care operations permitted by the HIPAA Privacy Rules.

E. No Disclosure of PHI for Non-Health Plan Purposes

PHI may not be used or disclosed for Non-Health Plan Purposes, unless the individual who is the subject of the PHI has provided an authorization for such use or disclosure (as discussed in Section II. H. "Disclosures Pursuant to an Authorization") or such use or disclosure is required or allowed by applicable law and particular requirements under the Privacy Rules are met.

F. Mandatory Disclosures of PHI

PHI must be disclosed, in accordance with the Privacy Rules, in the following situations:

- the disclosure is to the individual who is the subject of the information (see Section IV.A. of this Policy);
- the disclosure is required by law; or
- the disclosure is made to HHS for purposes of enforcing HIPAA.

G. Other Permitted Disclosures of PHI

Disclosures of PHI Permitted Unless the Individual Objects (Authorization Not Required)

The Group Health Plan's PHI may be disclosed in the following instances without an Authorization unless an individual objects:

- When such disclosure is to the individual's family member, relative, close friend or other person identified by the individual as involved in the individual's health care or for the payment of the individual's health care. The disclosure must be limited to the Group Health Plan' PHI relevant to that person's involvement in the individual's health care or payment.
- When such disclosure is to notify or assist in notifying a family member, personal representative, or other person responsible for the individual's care or the individual's location, general condition, or death.

Other Permitted Disclosures of PHI

PHI may be disclosed in the following situations without an individual's authorization, when specific requirements of Section 164.512 of the HIPAA Privacy Rules are satisfied:

- when such disclosure is to a government authority, as described in Section 164.512(c)(1) of the Privacy Rules, about an individual whom the Group Health Plan reasonably believe to be a victim of abuse, neglect or domestic violence, so long as the Group Health Plan informs the individual, unless the Group Health Plan believe informing the individual would place the individual in risk of serious harm or would not be in the best interests of the individual;
- for judicial and administrative proceedings;
- for law enforcement purposes;
- for public health activities described in Section 164.512(b)(1) of the Privacy Rules;
- for health oversight activities authorized by law to a health oversight agency;

- about decedents;
- for cadaveric organ-, eye- or tissue-donation purposes;
- for certain limited research purposes;
- to avert a serious threat to health or safety;
- for specialized government functions; and
- that relate to workers' compensation programs.

These disclosures require the prior approval of the Privacy Official.

H. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose listed in an authorization if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the individual who is the subject of the PHI, or the individual's personal representative. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization. The authorization must comply with the Privacy Rules.

I. Complying With the Minimum Necessary Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

However, the minimum necessary standard does not apply to any of the following:

- uses or disclosures made to the individual;
- uses or disclosures made pursuant to a valid authorization;
- disclosures made to HHS;
- uses or disclosures required by law; and
- uses or disclosures required to comply with HIPAA.

The Group Health Plan, when disclosing PHI subject to the minimum necessary standard, must take reasonable and appropriate steps to ensure that only the minimum amount of PHI that is necessary for the requestor is disclosed.

Minimum Necessary When Disclosing PHI. For making disclosures of PHI to any Business Associate or medical providers for claims payment/adjudication, plan design and pricing or internal/external auditing purposes, only the minimum necessary amount of information will be disclosed. All other disclosures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. For making requests for disclosure of PHI from Business Associates, medical providers or Participants for purposes of claims payment/adjudication, plan design and pricing or internal/external auditing purposes, only the minimum necessary amount of information will be requested. All other requests must be

reviewed on an individual basis with the Privacy Official to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

Disclosing or requesting a Limited Data Set is considered to be complying with the minimum necessary standard in most instances, and disclosures and requests should be limited to a Limited Data Set when appropriate for purposes of the Group Health Plan.

J. Disclosures of PHI to Business Associates

The Trust may disclose or authorize the disclosure of PHI to the Business Associates of the Group Health Plan and allow the Business Associates to create or receive PHI on behalf of the Group Health Plan. However, prior to doing so, the Group Health Plan must first obtain assurances from the Business Associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "Business Associate," employees must contact the Privacy Official and verify that a Business Associate Agreement is in place.

A *Business Associate* is an entity that:

- performs or assists in performing a function or activity involving the use and disclosure of PHI (including claims processing or administration, data analysis, underwriting, etc.) for the Group Health Plan; or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

However, the Health Insurance Issuers writing insurance policies for the Group Health Plan and medical providers are not Business Associates.

The Privacy Officer will verify that Business Associate Agreements for the Group Health Plan comply with the Privacy Rules. The Group Health Plan will keep all Business Associate Agreements for six years after the date of termination of such agreements.

K. Disclosures of De-Identified Information

The Group Health Plan may freely use and disclose information that has been "de-identified" in accordance with the Privacy Rules. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

Employees with Access can determine that information is de-identified either by (1) professional statistical analysis; or (2) removing the following identifiers:

- Names.
- All geographic subdivisions smaller than a state.
- All elements of dates (except years) for dates directly related to the individual.

- Telephone numbers.
- Fax numbers.
- Email addresses.
- Social Security numbers.
- Medical record numbers.
- Health plan beneficiary numbers.
- Account numbers.
- Certificate/license numbers.
- Vehicle identifiers.
- Device identifiers.
- Web Universal Resource Locators (URLs).
- Internet Protocol (IP) address numbers.
- Biometric identifiers.
- Full-face photographic images.
- Any other unique or identifying characteristics.

IV. POLICIES ON INDIVIDUAL RIGHTS

A. Access to and Requests for Amendment of Designated Record Set

HIPAA gives individuals the right to access and obtain copies of their PHI that the Group Health Plan (or a Business Associate) maintains in Designated Record Sets.

Designated Record Set means a group of records maintained by or for the Group Health Plan that includes:

- the enrollment, payment, and claims adjudication record of an individual maintained by or for the Group Health Plan; or
- other PHI used, in whole or in part, by or for the Group Health Plan to make coverage decisions about an individual.

Individuals may access copies of their own PHI by submitting a written request to the Privacy Official. However, if the PHI is being held by the Health Insurance Issuer, the Privacy Official may require that the individual make the request to the Health Insurance Issuer.

The Privacy Official must respond to a request within 30 days, or 60 days in certain circumstances. Individuals may be charged a reasonable cost-based fee for providing the records. The Privacy Official may deny the request in writing if the individual seeks psychotherapy notes, information compiled in anticipation of legal proceedings, or information that is protected by applicable law. If access is denied, the individual has the right to have the denial reviewed.

HIPAA also provides that individuals may request to have their PHI amended. The Group Health Plan will provide access to PHI and it will consider requests for amendment that are submitted in writing by individuals. An individual may request the amendment by submitting a

request in writing to the Privacy Official. If the PHI is being held by the Health Insurance Issuer, the Privacy Official may require that the individual make the request to the Health Insurance Issuer.

The Privacy Official must respond to a request within 60 days, or 90 days in certain circumstances. The Group Health Plan may deny the request in writing if (1) the Group Health Plan did not create the PHI on record, unless the individual provides a reasonable basis to believe that the originator is no longer available; (2) access to the PHI would not be available for inspection under the Privacy Rules; or (3) the Group Health Plan determine that the PHI record is accurate and complete. If the request for amendment is denied, the individual has a right to submit a statement of disagreement and to have the statement attached to the PHI record.

B. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

- to carry out treatment, payment or health care operations;
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- to persons involved in the individual's care or payment for the individual's care or for certain other notification purposes;
- to correctional institutions or law enforcement when the disclosure was permitted without authorization;
- as part of a limited data set; or
- for specific national security or law enforcement purposes.

Response to an accounting request is normally made within 60 days. If unable to provide the accounting within 60 days, the Group Health Plan may extend the period by 30 days, provided that it gives the individual notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure (or a copy of the written request for disclosure, if any). If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the disclosure.

The first accounting in any 12-month period is provided free of charge. The Privacy Official may impose reasonable production and mailing costs for subsequent accountings.

C. Requests for Alternative Communication Means or Locations

Individuals have the right to request to receive communications regarding their PHI by alternative means or at alternative locations. For example, individuals may ask to be called only at work rather than at home. Individuals wishing to do so must submit such a request in writing to the Privacy Official. The Group Health Plan may, but need not, honor such requests. The decision to honor such a request shall be made by the Privacy Official in consultation, as necessary, with the Health Insurance Issuer. The Group Health Plan may condition the accommodation on information as to how payment, if any, will be handled or specification of an alternative address or other method of contact.

However, the Group Health Plan shall accommodate such a request if the individual clearly states that the disclosures of all or part of the information could endanger the individual. The Privacy Official has responsibility for administering requests for confidential communications.

D. Requests for Restrictions on Use and Disclosure of PHI

An individual may request restrictions on the use and disclosure of the individual's PHI. The Group Health Plan may, but need not, honor such requests, except as provided below. Such a request must be made in writing to the Privacy Official. The decision to honor such a request shall be made by the Privacy Official in consultation, as necessary, with the Health Insurance Issuer. If the Privacy Official agrees to a restriction in writing, the Group Health Plan will comply with the restriction unless an emergency or the law prevents such compliance, or until the restriction is terminated by either the individual or the Privacy Official.

If the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full, the Group Health Plan must comply with the request for restriction.

V. REPORTABLE BREACH NOTIFICATION POLICY

The Group Health Plan has adopted a Reportable Breach Notification 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").

Under the HHS Breach Regulations, the Group Health Plan is required to provide notice to the affected individuals, to HHS, and, in certain instances, to the media if a breach of unsecured PHI of the Group Health Plan has occurred, including instances in which the breach occurred regarding the unsecured PHI of the Group Health Plan being used or held by Business Associates of the Group Health Plan.