HIPAA PRIVACY POLICY

Everett School Employee Benefit Trust

March 16, 2016

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, except such information ceases to be PHI 50 years after the person has died. 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

Debbie Kovacs, 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 in HIPAA and this Policy to members of the Workforce who have access to PHI of the Group Health Plan. 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 the 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 (1) within 60 days after a material change to the notice; or (2) during the open enrollment period for the Group Health Plan immediately following a material change.

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:

Debbie Kovacs
Human Resources
3900 Broadway
Everett, WA 98201
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. The resolution of a complaint will depend on the particular facts and circumstances of the complaint. Examples of complaint resolution include:

- Educating the individual about this Policy;
- Implementing changes to this Policy;
- Providing additional training for Workforce members on this Policy, the Privacy Rule, or other applicable laws or regulations;
- Obtaining confidentiality agreements with persons who received PHI in violation of the Privacy Rule or taking other steps to prevent further unauthorized uses and disclosures of the PHI;
- Monitoring the credit histories of affected individuals to prevent identity thefts;
- Discussing a complaint with the relevant parties and, if necessary, imposing sanctions on individuals who violate this Policy or the Privacy Rule; and
- Issuing new Workforce communication materials or a revised Privacy Notice regarding this Policy.

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

If, at any time, an individual wants to know the status of his or her complaint, he or she should contact the Privacy Official. Once a complaint has been resolved, the Privacy Official will contact the individual who filed the complaint in writing with the resolution.

The Privacy Official will maintain a record of the complaints and a brief explanation of each resolution, if any, for a period of six years.

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 of the Group Health Plan for administrative or other permitted purposes. Specifically, the Trust will:

- not use or further disclose PHI other than as permitted by the Group Health Plan documents or as required by law;
- ensure that any agents or subcontractors to whom the Trust provides PHI received from the Group Health Plan agree to the same restrictions and conditions that apply to the Trust;
- not use or disclose PHI for employment-related actions;
- report to the Group Health Plan any use or disclosure of the information that is inconsistent with the permitted uses or disclosures under HIPAA;

- make PHI available to individuals participating in the Group Health Plan, consider amendments to their PHI, and, upon request, provide them with an accounting of PHI disclosures in accordance with the HIPAA Privacy Rules;
- make the Trust's internal practices and records relating to the use and disclosure of PHI available to the Department of Health and Human Services ("HHS") upon request; and
- if feasible, return or destroy all PHI received from the Group Health Plan that the Trust still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

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.

The terms "use" and "disclosure" also include the creation, transmission, maintenance or receipt of PHI. 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, Health Care Operations and Treatment

PHI may be used and disclosed for the payment purposes of the Group Health Plan, including uses 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 the 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 used and 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.

Treatment. The Group Health Plan may disclose PHI to a health care provider for treatment activities of a health care provider. "Treatment" means the provision, coordination, or management of health care by one or more health care providers. It includes health care coordination or management between a health care provider and a third party, as well as consultation and referrals between providers.

E. Other Use and Disclosure Rules

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 III. I. "Disclosures of PHI Pursuant to an Authorization") or such use or disclosure is required or allowed by applicable state law and particular requirements under the Privacy Rules are met.

The Group Health Plan shall not use or disclose PHI that is genetic information for purposes of underwriting, and all other uses and disclosures of PHI that is genetic information shall be in compliance with the HIPAA Privacy Regulations. The term "genetic information" means genetic tests of an individual, fetus or embryo, genetic tests of an individual's family member or the fetus or embryo of a family member, the manifestation of a disease or disorder in an individual's family member, requests for or receipt of genetic services (genetic tests, genetic counseling or genetic education), and participation in clinical research which includes genetic services, all as defined in 45 C.F.R. § 160.103. Genetic information excludes information about the sex or age of any person and certain tests directly related to a manifested disease, disorder, or pathological condition of the individual.

The Group Health Plan shall not use or disclose PHI for marketing, fundraising, or research purposes, and shall not sell the PHI of individuals, unless the Group Health Plan complies with the applicable rules for such uses, disclosures, and sales under the HIPAA Privacy Rule.

F. Mandatory Disclosures of PHI

An individual's 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 to Personal Representatives, Family Members, Close Friends, and Others

Personal Representatives. The Group Health Plan will treat a personal representative of an individual as the individual, and the individual's PHI may be disclosed to the personal representative without an authorization. In general, the following are personal representatives of an individual:

- The parent or guardian is the personal representative of a minor child.
- The executor or administrator of an estate is the personal representative of a deceased individual.
- A person who is given a power of attorney to act for health care purposes for the individual is a personal representative of the individual.

In certain instances, a parent will not be treated as a personal representative of a minor child. For example, the parent will not be treated as the personal representative of the minor child for certain PHI if:

- The minor child lawfully obtained the medical services relating to such PHI with the consent of someone, other than the parent, who is authorized by law to give that consent (e.g., a court);
- The minor lawfully consented to and obtained the medical services relating to such PHI and state law does not require the consent of anyone else; or
- The parent has agreed to a confidentiality agreement between the health care provider and the minor with respect to the medical services relating to the PHI.

However, even if a parent or guardian is not treated as a personal representative of a minor child under these rules, the Group Health Plan will follow applicable state law on this subject: the Group Health Plan will disclose, or provide access to, PHI about the minor child to the parent or guardian if permitted or required to do so by applicable state or other law, and if any disclosure or access to a parent or guardian is prohibited by state or other law, the Group Health Plan may not disclose, or provide access to, PHI about a minor child to the parent or guardian.

Even if a parent, spouse, guardian or other person does not qualify as a personal representative under these rules, disclosure to these persons may be acceptable under the next section, "Others Acting on an Individual's Behalf."

The Group Health Plan may elect not to treat a person as an individual's personal representative if, in the exercise of professional judgment, the Group Health Plan decides that it is not in the best interest of the individual because of a reasonable belief that:

- The individual has been or may become subject to abuse, domestic violence, or neglect by the person; or
- Treating the person as a personal representative could endanger the individual.

Others Acting on an Individual's Behalf. The HIPAA Privacy Rule allows the Group Health Plan to disclose an individual's PHI to certain individuals other than the individual or the personal representative of the individual without an authorization, if necessary, for payment, health care operations and for certain other purposes. This can include disclosures of an individual's PHI to the individual's family members, close friends, and others involved in the individual's care or payment for such care. In making these disclosures, the Group Health Plan will make reasonable efforts to limit disclosures to the minimum necessary to accomplish the intended purpose. "Family member" includes members of the individual's immediate family, as well as other relatives of the individual.

PHI can be disclosed without an authorization to an individual's family members, friends, and others who are not personal representatives, if any of the following conditions apply:

- Information describing the individual's location, general condition, or death may be provided to a family member, close friend, or other person responsible for the individual's care (including disclosing PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts).
- When the individual is present or available prior to the disclosure, PHI may be disclosed to a family member, close friend, or other person identified by the individual who is involved in the individual's care or payment for that care of any PHI directly relevant to the person's involvement with the individual's care or payment for that care, if: (1) the individual has agreed orally or in writing to such disclosure; (2) the individual had the opportunity to agree or object to the disclosure, and did not express an objection; or (3) the Group Health Plan can reasonably infer, based on professional judgment, that the individual does not object to the disclosure.
- When an individual is not present or the individual's agreement cannot be obtained due to incapacity or emergency, PHI may be disclosed to family members, close friends, or others involved in the individual's care or payment for such care if, in the exercise of professional judgment, it is determined that the disclosure is in the best interest of the individual, limited to disclosures of PHI that are directly relevant to the person's involvement in the individual's care or payment.
- When an individual is deceased, the Group Health Plan may disclose to family members, close friends, or others involved in the individual's care or payment for health care prior to the individual's death, PHI of the deceased individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the Group Health Plan.

H. 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 required by law;
- 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 believes 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 believes 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.

I. 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.

J. 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 other covered entity, 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 covered entities, 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.

K. 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 use, disclose, maintain, transmit, 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 third parties who meet the definition of a "Business Associate," employees must contact the Privacy Official and verify that a Business Associate Agreement is in place.

In general, a Business Associate is a person or organization, other than a member of the Workforce, that creates, uses, discloses, receives, maintains, or transmits PHI for functions of the Group Health Plan that are regulated by the Privacy Rule. A Business Associate also includes: (1) a Health Information Organization, E-prescribing Gateway, or other entity or person that provides data transmission services with respect to PHI of the Group Health Plan and that requires access to the PHI of the Group Health Plan on a routine basis; (2) a person or entity that offers a personal health record to individuals on behalf of the Group Health Plan or other covered entity; and (3) a subcontractor that uses, discloses, creates, receives, maintains, or transmits PHI on behalf of a Business Associate.

However, persons or organizations are not considered Business Associates if their functions or services do not involve the use, disclosure, creation, receipt, maintenance, or transmittal of PHI, and where any access to Protected Health Information by such persons or organizations would be incidental, if at all. A Business Associate does not include: (1) a health care provider, with respect to disclosure by the Group Health Plan or other

covered entity to a health care provider concerning the treatment of the individual; (2) a plan sponsor, with respect to disclosures by a group health plan to the plan sponsor in accordance with the Privacy Rule; (3) certain governmental agencies; and (4) insurance companies writing insurance policies for the Group Health Plan.

The Privacy Rule requires each Business Associate who is a prime contractor with the Group Health Plan ("Prime Business Associate") to enter into a written contract (a "Business Associate Agreement") with the Group Health Plan before the Group Health Plan can disclose PHI to the Prime Business Associate. The Trust will also be a signatory to each such Business Associate Agreement. Each Prime Business Associate must also enter into a Business Associate Agreement with each of its subcontractors who use, disclose, maintain, transmit, create, or receive the PHI of the Group Health Plan ("Subcontractor Business Associate"). The Prime Business Associate and the Subcontractor Business Associate can use and disclose PHI of the Group Health Plan only for the purposes provided in the Business Associate Agreement between the Group Health Plan and the Prime Business Associate. The Privacy Official will monitor how PHI maintained by the Prime Business Associate and the Subcontractor Business Associate is handled at the termination of the Business Associate Agreement with the Prime Business Associate and will, while the agreement is in force, act upon complaints of privacy violations and breaches of PHI.

Identifying Business Associates. The Group Health Plan will determine which service providers are Prime Business Associates. Upon request, the Prime Business Associates will identify the Subcontractor Business Associates and the agents of the Prime Business Associates with access to the PHI of the Group Health Plan.

Preparing and Signing Business Associate Agreements. The Group Health Plan will require each Prime Business Associate to sign a Business Associate Agreement. Each Prime Business Associate will be required to sign a Business Associate Agreement with each of its Subcontractor Business Associates containing substantially the same terms as the Business Associate Agreement between the Group Health Plan and the Prime Business Associate.

Timing of Business Associate Agreements. The Group Health Plan will not disclose PHI to a Prime Business Associate or to a Subcontractor Business Associate unless the required Business Associate Agreements have been signed.

Responsibilities of the Privacy Official. The Privacy Official will monitor the PHI that the Prime Business Associate and Subcontractor Business Associate must return to the Group Health Plan or destroy (or extend the protections of the Business Associate Agreement if the PHI is not returned or destroyed) upon termination of the Business Associate Agreement with the Prime Business Associate.

The Privacy Official will ensure that all complaints about privacy violations by a Business Associate are reviewed in accordance with this Policy. If the Privacy Official knows of acts or patterns of activity by a Business Associate that are material violations of the Business Associate Agreement, the Privacy Official will take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the Privacy Official will determine, in consultation with legal counsel, whether termination of the business

relationship with the Prime Business Associate and/or the Business Associate Agreement is feasible.

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.

L. 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, unless the Privacy Official extends the response time for up to an additional 30 days in accordance with 45 C.F.R.§164.524. Individuals may be allowed to inspect the records or may request a copy of the records. If the individual requests a copy of the records, the individual 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.

If the individual's request to inspect or copy directs the Group Health Plan to transmit a copy of the PHI directly to another person designated by the individual, the Group Health Plan must provide the copy to the person so designated. The individual's request must be in writing, signed by the individual, and must clearly identify the other person and where to the send the copy of the PHI.

If the PHI in the Designated Record Set being requested is maintained electronically, and the individual requests an electronic copy of such PHI, the Group Health Plan will provide the individual with access to the PHI in the electronic form and format requested by the individual if readily producible by the Group Health Plan. If not readily producible in the form and format requested by the individual, the Group Health Plan will produce the PHI in a readable electronic form and format agreed to by the Privacy Official and the individual.

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, unless the Privacy Official extends the response time for up to an additional 30 days in accordance with 45 C.F.R. § 164.524. 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 made in the last six years. However, this right to an accounting not include the following 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 by regular means 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 adopts this policy to comply with the HIPAA rules on Breach Notification for Unsecured Protected Health Information, found at 45 C.F.R. Part 164, Subpart D ("HHS Breach Regulations"). This policy replaces any prior Reportable Breach Notification Policy adopted by the Trust and/or Group Health Plan.

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.

A. Reportable Breach

The first step is to determine whether a Reportable Breach has occurred. If there is not a Reportable Breach, then there is no Notification Requirement. All Workforce members and Business Associates are required to report incidents involving breaches or possible breaches to the Privacy Official. The Privacy Official is responsible for determining if a Reportable Breach has occurred in accordance with the following rules.

There is a Reportable Breach when all of the following occur:

- The PHI in question was "unsecure."
- The violation involved unauthorized access, use, acquisition, or disclosure of unsecure PHI in a manner that is not permitted or authorized by the Privacy Rules and which compromised the security or privacy of the PHI.
- One of the exceptions to the Notification Requirement does not apply.

The following steps are used to determine if there is a Reportable Breach:

- Violation of HIPAA Privacy Rules. There must be an impermissible use or disclosure resulting from or in connection with a violation of the HIPAA Privacy Rules by the Group Health Plan or Business Associate of the Group Health Plan. If not, then there is no Notification Requirement.
- Was PHI involved? If not, then there is no Notification Requirement.
- Was the PHI secured? If yes, then there is no Notification Requirement.

- Electronic PHI: must be destroyed or encrypted to NIST standards to be secured.
- Paper PHI: must be destroyed to be secured.

- Unauthorized Access, Use, Acquisition or Disclosure of PHI. The violation of the Privacy Rules must involve one of the following. If it did not, then there is no Notification Requirement.
  - Unauthorized access of PHI.
  - Unauthorized use of PHI.
  - Unauthorized acquisition of PHI.
  - Unauthorized disclosure of PHI.
- More than a Low Probability that the PHI has been Compromised. The Group Health Plan will presume that the unauthorized access, use, acquisition or disclosure of PHI is a Reportable Breach unless the Privacy Official can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:
  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
  - The unauthorized person who used the PHI or to whom the disclosure was made.
  - Whether the PHI was actually acquired or reviewed.
  - The extent to which the risk to the PHI has been mitigated.

If the Privacy Official determines that there was a low probability that the PHI has been compromised, the Privacy Official must document this decision in writing and keep the written document on file.

Exceptions to the Rule. There is no Notification Requirement if one of the following exceptions applies.

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 Group Health Plan or Business Associate and no further unauthorized access, use, acquisition, or disclosure occurred, if:

- The unauthorized access, use, acquisition, or disclosure was in good faith; and
- The unauthorized access, use, acquisition, or disclosure was in the scope of authority of the Workforce member.

Examples of Exception 1:

- Inadvertent email to wrong co-worker: exception may apply.
- Unauthorized employee looks up PHI of neighbor: exception does not apply.

Exception 2: There is no Notification Requirement if the breach involved an inadvertent disclosure from one person authorized by the Group Health Plan to have access to PHI to another person authorized by the Group Health Plan to have access to PHI.

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.

Examples of Exception 3:

- EOB sent to wrong person, but was returned to the Group Health Plan unopened.
- 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. The Group Health Plan has reasonable systems and procedures in place to discover the existence of breaches.

Trigger: *Discovery of Reportable Breach*. The deadline for giving Notice of Reportable Breach is triggered from the date the discovery of the Reportable Breach occurs ("Discovery Date"). The Discovery Date of the Reportable Breach is the earlier of the two following dates:

- Date of Actual Knowledge. The date that a Workforce member (other than a Workforce member who committed the Reportable Breach) knows of the Reportable Breach. Employees are informed to notify the Privacy Official of the Group Health Plan or other responsible person immediately so the Group Health Plan can meet the deadlines.
- Date of Deemed Knowledge. The date that a Group Health Plan Workforce member or agent of the Group Health Plan (other than the person who committed the Reportable Breach) would have known of the Reportable Breach if the person was exercising reasonable due diligence. Reasonable due diligence is the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

Rules for Business Associates. If a Business Associate has a Reportable Breach relating to the participants in the Group Health Plan, the Group Health Plan is responsible for giving Notices of Reportable Breaches (the Business Associate must give notice of the Reportable Breach to the Group Health Plan).

The Discovery Date for the Group Health Plan of a Reportable Breach by a Business Associate is the date that the Group Health Plan is informed of the Reportable Breach by the Business Associate.

The Group Health Plan must require prompt notification of Reportable Breaches by Business Associates.
In the Business Associate Agreements with Business Associates, the Group Health Plan shall endeavor to require that: (1) the Business Associates report incidents involving breaches or possible breaches to the Privacy Official promptly upon discovery; (2) the Business Associates provide any and all information to the Group Health Plan as requested by the Group Health Plan regarding the Reportable Breach, including, but not limited to, the information required to be included in the Notices, as described below; (3) the Subcontractor Business Associates promptly report incidents involving breaches or possible breaches to the Prime Business Associate and/or the Privacy Official; and (4) the Business Associates 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.

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

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.

Examples:

Investigation is completed 15 days after the Discovery Date. Notice must be given shortly thereafter (20-25 days after the Discovery Date) because waiting until day 55 would be an unreasonable delay.

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

There is an exception to these rules if a law enforcement official requests that the Group Health Plan delay giving the Notices.

Urgent Notices (see below) must be given sooner.

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

There are three types of required notices under the HHS Breach Regulations.

Notice to Individuals. (See Section D.)

- Actual Notice.
- Substitute Notice.
- Urgent Notice.

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

Notice to HHS. (See Section F.)

- The Reportable Breach involved 500 or more affected persons: immediate notice to HHS.
- The Reportable Breach involved less than 500 affected persons: annual report to HHS.

Privacy Official Responsible for Notices. The Privacy Official of the Group Health Plan is responsible for the content of the Notices and for delivering the Notices in a timely manner in accordance with the rules set forth below.

D. Notice to Individuals

The Notice to Individuals is always required when there is a Reportable Breach and must be written in plain language. The Notice to Individuals must contain all of the following:

- A brief description of the incident.

- If known, the date of the Reportable Breach and Discovery Date.
- A description of the PHI involved in the Reportable Breach (for example, full name, SSN, address, diagnosis, date of birth, account number, disability code, or other).
- The steps individuals should take to protect themselves, such as:
    - Contacting credit card companies.
    - Contacting credit bureaus.
    - Obtaining credit monitoring services.
- A description of what the Group Health Plan is doing to investigate the Reportable Breach, such as:
    - Filing a police report.
    - Reviewing security logs or tapes.
- A description of what the Group Health Plan is doing to mitigate harm to individuals.
- A description of what measures the Group Health Plan is taking to protect against further breaches, such as:
    - Sanctions imposed on Workforce members involved in the Reportable Breach.
    - Encryption.
    - Installing new firewalls.
- Contact information where individuals can learn more about the Reportable Breach or ask other questions, which must include one of the following:
    - Toll-free telephone number.
    - Email address.
    - Website.
    - Postal address.

There are three types of Notices to Individuals which may be required to be delivered. All Notices must have the contents described above.

Actual Notice

- Sent first class mail to last known address of the individual(s).
- Sent via email if the individual has agreed to receive electronic notices.
- Sent to the parent of a minor child.
- Sent to next-of-kin or personal representative of deceased person.

Substitute Notice

If the Group Health Plan has insufficient or out-of-date addresses, then Substitute Notice is required.

If addresses of fewer than ten living individuals are insufficient or out-of-date, Substitute Notice can be given in the following manner:

- Telephone notice.
- Notice in person.
- Email notice.

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

- Website. Conspicuous posting on home page of the website of the Group Health Plan for 90 days, including a toll-free number which can be called to obtain information about the Reportable Breach. Contents of the notice can be provided directly on the website or via hyperlink.
- Media. Conspicuous notice in major print or broadcast media in the geographic areas where the individuals affected by the Reportable Breach likely reside, including a toll-free number which can be called to obtain information about the Reportable Breach. The Substitute Notice may have to be given in both local media outlet(s) and state-wide media outlet(s).

Substitute Notice is only required for living persons.

Urgent Notice

The Urgent Notice is required when possible imminent misuse of unsecured PHI may have occurred. The Urgent Notice must be given by telephone or other appropriate means.

The Urgent Notice is required in addition to the other Notices that are required. Example: Urgent Notice is given to the Group Health Plan participant by telephone call. The Group Health Plan must also send Individual Notice via first class mail to the Group Health Plan participant.

E. Notice to Media (Press Release)

The Notice to Media is required when the Reportable Breach involves more than 500 residents of any one state or jurisdiction. Examples:

- Reportable Breach involves 600 residents of Washington: Notice to Media required.
- Reportable Breach involves 450 residents of Washington and 60 residents of Idaho: Notice to Media not required.

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

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

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

Notice of all Reportable Breaches must be given to the HHS Secretary.

Immediate Notice to HHS. This Notice is required where the Reportable Breach involves 500 or more individuals, regardless of where the individuals reside.

Example:

- Reportable Breach involves 450 residents of Washington and 60 residents of Idaho: Notice to HHS required.

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

Yearly Report of Reportable Breaches. If the Reportable Breach involves less than 500 individuals, the Group Health Plan 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 Privacy Official of the Group Health Plan is responsible for filing such reports.

G. Training

The Privacy Official of the Group Health Plan shall cause appropriate Workforce members to receive training in the Reportable Breach rules described in this Section V. "Reportable Breach Notification Policy."