Everett School Employee Benefit Trust
2016-17
Meeting Calendar

Trust meetings will be held on Wednesdays at 4:00 p.m. (unless otherwise noted below) at the Community Resource Center (CRC) located at 3900 Broadway in Everett.

Date	Time	Conference Room
August 9, 2016*	4:00-6:00 p.m.	**Monte Cristo Room**
August 24, 2016*	2:00-4:00 p.m.	Port Gardner Room B
September 14, 2016*	4:00-6:00 p.m.	Port Gardner Room B
September 28, 2016**	4:00-6:00 p.m.	**Monte Cristo Room**
October 19, 2016*	4:00-6:00 p.m.	Port Gardner Room B
November 16, 2016*	4:00-6:00 p.m.	Port Gardner Room B
December 14, 2016	4:00-6:00 p.m.	**Monte Cristo Room**
January 18, 2017	4:00-6:00 p.m.	Port Gardner Room B
February 15, 2017	4:00-6:00 p.m.	Port Gardner Room B
March 15, 2017	4:00-6:00 p.m.	Port Gardner Room B
April 19, 2017*	4:00-6:00 p.m.	Port Gardner Room B
May 17, 2017*	4:00-6:00 p.m.	Port Gardner Room B
June 14, 2017*	4:00-6:00 p.m.	Port Gardner Room B

*Consultant(s) attending
**Special meeting added 8/24/16

Approved: March 16, 2016
Revised: June 15, 2016
Revised: August 24, 2016

EVERETT BENEFIT TRUST
ANNUAL CALENDAR

July ✓ Beginning of Fiscal year	July 1
August ✓ Consultant presents proposed plan renewals and rates for upcoming Fiscal year to the Trustees (Sean) ✓ Trust audit by independent auditor (Darla)	Mid-Late August Consultant attending
September ✓ Finalize upcoming fiscal year plans and rates with consultant (Sean) ✓ Approve annual budget (Trustees) ✓ Open enrollment materials are prepared by the Benefits Department (Randi) ✓ Review and approval of audit by independent auditor (Darla) ✓ United Health Care claims data and appeals results (Sean)	Consultant attending
October ✓ Plan documents are finalized between the Consultant and Human Resources (Sean/Randi) ✓ Open enrollment begins (Randi)	Consultant attending
November ✓ Open enrollment closes (Randi) ✓ Investment Summary Review (Jayson) ✓ Annual investment policy review and recommendations from investment consultant (Jayson) ✓ Review performance of investment manager(s) (Jayson)	Consultant attending
December ✓ Approval of Annual investment policy review by Trustees (**if revisions are proposed in November**) ✓ Quarterly EAP report (Randi)	
January ✓ Human Resources provides an update on Open Enrollment processes and participation (Randi)	
February ✓ Review Fiduciary Liability Insurance Renewal (Darla) ✓ United Health Care claims data and appeals results	
March ✓ Approve Fiduciary Liability Insurance Renewal (Darla)	

EVERETT BENEFIT TRUST
ANNUAL CALENDAR

April ✓ Begin preliminary discussion with consultants on plan renewals (Sean) ✓ Review Operational Manual (Trustees) ✓ Quarterly EAP report (Randi) ✓ Investment Manager presentation (Becker & Jayson) ✓ Establish and adopt annual regular meeting calendar for the upcoming fiscal year (Trustees)	Consultants attending
May ✓ Review Auditor Engagement for annual audit (Darla) ✓ Review Consultant Engagement/Budget for upcoming fiscal year (Sean) ✓ Review performance of investment consultant (Executive Session) ✓ Review annual Wellness Program plan and budget (Rickie Lee)	Consultant attending
June ✓ Approval of Auditor Engagement for annual audit (Darla) ✓ Approval of Consultant Engagement/Budget for upcoming fiscal year (Sean) ✓ Approval of annual Wellness Program plan and budget (Rickie Lee) ✓ End of year Wellness Program report (Rickie Lee) ✓ Rotation of Trust Officers (Trustees) ✓ Review Compensation for Trust financial and support services (Executive Session) ✓ End of Fiscal year	Consultant attending June 30

Everett School Employee Benefit Trust Operations Manual for Trustees

Everett School Employee Benefit Trust
Operations Manual for Trustees

Table of Contents

Everett School Employee Benefit Trust
Operations Manual for Trustees

Table of Contents

Revised: September 25, 2008
Revised: January 24, 2011
Revised: April 30, 2012
Revised: October 16, 2013

ADMINISTRATION

General Administration

The goal of the Administration Policy is to enable the Trustees for the Everett School Employee Benefit Trust ("Trustees") to administer the Everett School Employee Benefit Trust ("Trust") in accordance with the terms of the Trust document, benefit document(s), Title 48, Chapter 62 RCW, if the Trust self-insures any Trust benefits, District policies and procedures, and procedures adopted by the Trustees. The Trust is sponsored by the Everett School District ("District") and the Everett Education Association ("Association").

Responsibilities

The Trustee's key administrative responsibilities are grouped by type of responsibility and are generally described below. The following is not intended to be a comprehensive listing of all responsibilities. From time to time, the Trustees shall review updates on typical administrative committee practices and may revise the following administrative responsibilities by Trustees action. The Trustees will develop appropriate procedures to address these responsibilities:

- Selection, appointment and monitoring any external third-party administrator, Trust fund investment advisor or manager, consultant or other advisor.
- Interpreting Trust document and benefit document terms.
- Appoint claims administrator(s) to determine initial claims for benefits funded directly by the Trust, and decide all benefit claim appeals in accordance with the claims procedures contained in the benefit documents specified in Appendix I of the Trust document.
- Select insurance carriers for benefits funded through insurance purchased by the Trust. Such insurance carriers must be licensed or authorized by the State of Washington to transact insurance in the State of Washington.
- Providing benefit statements.
- Ensuring only appropriate expenses are paid with Trust funds.

The Trustees may adopt such additional rules and procedures as it deems desirable for the conduct of its affairs, managing and controlling the Trust and administration of the benefits funded by the Trust, provided that any such rules and procedures shall be consistent with the provisions of the Trust document, other District policies and procedures, RCW 48.62 and its implementing regulations, and if the Trust self-insures any Trust benefits.

The Trustees will develop and adopt procedures for carrying out this policy.

Adopted: August 29, 2005
Revised: January 24, 2011
Revised: October 16, 2013

ADMINISTRATION

Trust Administration

The administration of the Trust in accordance with the terms of the Trust document, benefit document(s), applicable District policies and procedures through administrative procedures adopted by the Trustees, and if the Trust self-insures any Trust benefits, RCW 48.62 and its implementing regulations are vital to the Trust and to the District. As provided by the terms of the Trust, the District will maintain at least a fifty percent voting control of the Trust.

Cross References:	Trust Policy 100	General Administration
	Trust Procedure 100.2P	Adopting Procedures
	Trust document	Benefit documents specified in Appendix I of the Trust document
Legal References:	RCW 48.62.121(1)	General operating regulations—Employee remuneration—Governing control—School districts—Use of insurance producers and surplus line brokers—Health care services—Trusts
	WAC 200-110-010 et seq.	Local government self-insurance and welfare program requirements—Preamble and authority

Adopted: August 29, 2005
Revised: January 24, 2011
Revised: October 16, 2013

ADMINISTRATION

Adopting Procedures

The Trustees shall take reasonable actions to adopt procedures for administering the Trust and for executing Trust policies. Proposed procedures shall be circulated in draft form to the Trustees to ensure time for review and shall be approved at a subsequent Trustee meeting.

If the Trust self-insures any Trust benefits, prior to implementing the following changes, the Trustees will request in writing and receive approval from the state risk manager:

- Elimination or reduction of stop-loss insurance;
- Acceptance of any loans or lines of credit;
- Provision of services to nonmembers; or
- Addition of members of other entity types than those included in the original application approved by the state risk manager.

Cross References:	Trust Policy 100	General Administration
	Trust Policy 110	Trustees
	Trust Policy 130	Administrative Authority

Adopted: August 29, 2005
Revised: January 24, 2011
Revised: October 16, 2013

ADMINISTRATION

Third Party Administrators, Consultants, Advisors and Insurers

The Trustees shall select, appoint and monitor any external third-party administrators ("TPA"), consultants, other advisors or insurers.

When selecting a TPA, consultant, other advisor or insurer the Trustees shall consider:

1. The TPAs, consultants, other outside advisors or insurers responsiveness, accuracy and business stability.
2. The TPAs, consultants, other outside advisors or insurers ability to meet the Trust's needs including, benefit administration, legal compliance, benefit projections and communications.
3. With respect to the TPA only, the TPA's technology (consideration of whether the District's current technology is compatible with and can interface the TPA's technology).

If the Trust self-insures any Trust benefits that are to be administered by a TPA, contracts with such TPAs are subject to the following requirements:

1. The TPA, the actuary, and the broker of record must contract separately with the Trust.
2. The contract must require that a written statement be submitted to the Trust on a form provided by the state risk manager providing assurance that no conflict of interest exists.
3. TPAs shall be selected using a competitive solicitation process.
4. The contract must include a complete written description of the services to be provided, remuneration levels, contract period and expiration date.
5. The contract must provide for the confidentiality of the Trust's information, data and other intellectual property developed or shared during the course of the contract.
6. The contract must provide for the Trust's ownership of the information, data, and other intellectual property developed or shared during the course of the contract.
7. The contract must provide for the expressed authorization of the Trust, the Trust's consultants, the state auditor, the state risk manager, or their designees, to enter the TPA's premises to inspect and audit the records and performance of the TPA which pertain to the Trust and to obtain such records electronically so that audit travel costs can be eliminated or reduced.
8. The contract must require compliance with all applicable local, state and federal laws.
9. The contract must contain indemnification provisions and set forth insurance requirements between the parties.

The Trustees monitoring function shall include:

1. Periodic evaluations of the TPA, consultant or other advisor.
2. Meetings with the TPA, consultant or other advisor.
3. Discussion and resolution of problems.

Cross References:	Trust Procedure 110.7P	Delegation of Duties
	District Policy 5225	Technology
	District Procedure 5225P	Technology
Legal References:	WAC 200-110-100	Standards for management—Standards for contracts—Third-party administrator contracts.
	WAC 200-110-150	Standards for management and operations—Conflict of interest.

Adopted: August~~,~~ 29, 2005
Revised: January 24, 2011
Revised: October 16, 2013

ADMINISTRATION

District or Association Action

Any decisions or actions by the District or Association pursuant to the provisions of the Trust shall be evidenced by a written instrument executed by the District or Association respectively or anyone authorized to take such action as a representative of the District or Association.

Cross Reference: Trust document Section 4.10

Adopted: August 29, 2005
Revised: January 24, 2011

ADMINISTRATION

Non Discrimination

The Trustees shall administer the benefits funded directly by the Trust in a nondiscriminatory manner, in accordance with the District's policy on non discrimination and affirmative action and the District's equity policy.

If the Trust self-insures any Trust benefits, contribution rate schedules shall be consistent and nondiscriminatory among beneficiaries. This provision is not intended to prohibit choice of coverage for beneficiaries, classes of beneficiaries, or bargaining groups from the options offered by the Trust, or to prohibit different contribution schedules between classes of beneficiaries or bargaining groups.

Cross Reference:	Board Policy 5010	Nondiscrimination and Affirmative Action
Legal Reference:	WAC 200-110-050	Nondiscrimination in contributions

Adopted: August 29, 2005
Revised: January 24, 2011
Revised: October 16, 2013

ADMINISTRATION

Trustees

The role of the Trustees is to manage and control the Trust and to administer the benefits funded directly by the Trust. The Trustees are the "Administrator" under the terms of the Trust. Pursuant to the Trust document, the Trustees are appointed by the District and the Association.

Cross References:	Trust Policy 100	General Administration
	Trust Procedure 110.1P	Membership
	Trust Policy 120	Trust and Plan Terms
	Trust Policy 130	Administrative Authority
	Trust document Preamble	

Adopted: August 29, 2005
Revised: January 24, 2011

ADMINISTRATION

Membership

The appointment of, resignation, removal and succession of Trustees is determined as follows:

Removal of Trustee

The District may remove any Trustee appointed by the District at any time by delivery to such Trustee, and to the other Trustees then acting, an instrument signed by the District. Likewise, the Association may remove any Trustee appointed by the Association at any time by delivery to such Trustee and to the other Trustees then acting, an instrument signed by the Association.

Resignation of Trustee

Any Trustee may resign, without the permission of any court or judge and without first accounting for his actions as Trustee, by giving written notice to the District, Association and to the other Trustees then acting, but the foregoing shall not relieve any Trustee so resigning of the obligation ultimately to account for his or her actions as such Trustee.

Appointment of Successor Trustees

In the event of the death, resignation or removal for any reason of any Trustee, a successor Trustee may be appointed by an instrument signed by the District or Association, accepted in writing by such successor Trustee, copies of which shall be delivered by the District or Association to the other Trustees then acting. The District shall appoint the successor of a District Trustee and the Association shall appoint the successor of an Association Trustee.

Cross References: Trust Policy 110 Trustees
Trust Policy 120 Trust and Plan Terms
Trust document Section 5

Adopted: August 29, 2005
Revised: January 24, 2011

ADMINISTRATION

Appointments

The Trustees shall select a Chairperson and Secretary who shall serve for terms of one fiscal year and until selection of their successors. For the first year of existence of the Trust, the Chairperson position shall be filled from the District-appointed Trustees and the Secretary position shall be filled from the Association-appointed Trustees. For the second and all succeeding years, the position of Chairperson and Secretary shall alternate between the respective Trustee groups. Each Trustee group shall select the individual who will serve in the appropriate capacity from among its own members by majority vote.

Cross Reference: Trust Policy 120 Trust and Plan Terms
Trust document Section 4.7(d)

Adopted: August 29, 2005
Revised: January 24, 2011

ADMINISTRATION

Meetings

The Trustees shall annually set a calendar of meeting dates and will meet as often as is necessary to carry out the purpose of the Trust, and special meetings will be called as necessary.

The Chairperson may schedule meetings, including special meetings, with seventy-two (72) hours notice. In cases of emergency, the seventy-two (72) hour notice is not required. Further, any two (2) Trustees may call a meeting of the Trustees at any time by giving at least ten (10) days written notice of the time and place of the meeting to each of the other Trustees. Meetings of the Trustees may also be held at any time without notice if all of the Trustees consent thereto.

Cross Reference: Trust document Section 4.7(b)

Adopted: August 29, 2005
Revised: January 24, 2011

ADMINISTRATION

Trustee Action

Decisions or actions of the Trustees taken at any meeting shall be determined by majority vote of the Trustees present at the meeting, provided that a quorum is present. A quorum shall require four (4) Trustees be present with at least 50 percent of those Trustees present representing the District. No proxy voting shall be allowed. In the event of a deadlock among the Trustees, no decision or action shall be taken by the Trustees.

Cross Reference: Trust document Section 4.7(c)

Legal Reference:	RCW 48.62.121(2)(iii)	(Applies only if the Trust self-insures any Trust benefits.) General operating regulations—Employee remuneration—Governing control—School districts—Use of insurance producers and surplus line brokers—Health care services—Trusts

Adopted: August 29, 2005
Revised: January 24, 2011
Updated: October 16, 2013

ADMINISTRATION

Agendas, Minutes and Records

1. The Chairperson shall establish agendas for the Trustees' meetings. The Chairperson shall endeavor to provide the agenda, together with materials relating to the subject matter of each meeting, to the Trustees prior to each meeting.
2. Minutes shall be kept of all Trustee meetings. The minutes shall be circulated in draft form to the Trustees to ensure an accurate record, and shall be approved at a subsequent Trustee meeting.
3. The Chairperson may delegate his or her responsibilities regarding agendas, minutes and records, in accordance with the Trust's delegation procedure.
4. The Trustees shall keep records of all decisions regarding benefit document interpretations and benefit claim determinations.

Cross References:		
	Trust Procedure 110.7P	Delegation of Duties
	Trust Procedure 410.1P	Claims Procedure
	Trust Policy 430	Health Insurance Portability and Accountability Act of 1996 (HIPAA) – Privacy and Security (referencing HIPAA Privacy Manual, as amended for Security)
	Trust Policy 450	Records Retention and Management
	District Policy 6560	Records Management and Retention
	District Procedure 6560P	Records Management and Retention

General Records Retention Schedule, School Districts and Educational Districts, provided by the Office of the Secretary of State, Division of Archives and Records Management

Adopted: August 29, 2005
Revised: January 24, 2011

ADMINISTRATION

Signing of Documents

Documents may be signed for the Trustees by the Chairperson or other Trustee designated by the Chairperson or other Trustees.

Cross References:	Trust Procedure 110.7P	Delegation of Duties
	Trust Policy 440	Reports
	Trust document Section 4.7	

Adopted: August 29, 2005
Revised: January 24, 2011

ADMINISTRATION

Delegation of Duties

The Trustees may delegate duties to one or more persons, in writing. Duties may be delegated to employees of the District and other outside advisors. Duties currently delegated and the District employees to whom they are delegated include the following:

- General Benefits Administration: Human Resources Administration, Benefits and Employee Records Departments.
- Eligibility and Enrollment Determinations: Human Resources Administration, Benefits and Employee Records Departments.
- Trust Financial Management: Delegations pursuant to Finance Policies and Procedures.

For Duties delegated to outside advisors, the below-referenced documents outline the duties that have been delegated and the outside parties to whom such duties have been delegated.

Cross References:	Trust Procedure 100.3P	Third Party Administrators, Consultants and Advisors
	Trust Policy 200	Financial Policy
	Trust Procedure 200.1P	Financial Management
	Trust Policy 220	Investment Guidelines
	Trust Policy 410	Claims and Appeals
	Trust Procedure 410.1P	Claims Procedure
	Trust document sections 4.2(k) and 4.5	

Adopted: August 29, 2005
Revised: January 24, 2011

ADMINISTRATION

Reliance on Information

The Trustees may, in good faith, rely on information provided by the Trust's investment consultant and any Trustee advisor. The Trustees shall also be protected to the fullest extent possible in taking or omitting any action in accordance with written directions from any Trustee advisor.

Cross References:	Trust Procedure 100.4P	District or Association Action
	Trust Procedure 110.7P	Delegation of Duties
	Trust Policy 220	Investment Guidelines

Adopted: August 29, 2005
Revised: January 24, 2011

ADMINISTRATION

Compensation

The Trustees shall serve without compensation for services to the Trust, however, reasonable and necessary Trustee expenses incurred in the discharge of Trustee shall be reimbursed by the Trust.

Cross Reference:	Trust Policy 240	Payment for Travel Expenses
	District Policy 6213	Reimbursement for Travel Expenses
	District Procedure 6213P	Reimbursement for Travel Expenses
	Trust document section 4.3	
Legal Reference:	RCW 48.62.121(1)	(Applies only if the Trust self-insures any Trust benefits.) General operating regulations—Employee remuneration—Governing control—School districts—Use of insurance producers and surplus line brokers—Health care services—Trusts.

Adopted: August 29, 2005
Revised: January 24, 2011
Updated: October 16, 2013

ADMINISTRATION

Trust and Plan Terms

The Trustees are responsible for managing and controlling the Trust in accordance with the Trust document terms and referenced District policies and procedures. The Trustees are also responsible for administering the benefits funded directly by the Trust in accordance with applicable benefit documents and with applicable laws.

Cross Reference: Trust document Section 1.6
Benefit documents specified in Appendix I of the Trust document

Adopted: August 29, 2005
Revised: January 24, 2011

ADMINISTRATION

Administrative Authority

The Trustees have sole authority and responsibility for the administration of the Trust as specified in the Trust document and RCW 48.62 if the Trust self-insures any Trust benefits, including the discretionary authority to interpret the provisions of the benefit documents and the facts and circumstances of claims for benefits.

Cross Reference: Trust Procedure 410.1P Claims Procedure
Trust document section 4.16

Adopted: August 29, 2005
Revised: January 24, 2011
Revised: October 16, 2013

FINANCE

Financial Policy

The Trustees for the Everett School Employee Benefit Trust ("Trustees") serve as the fiduciaries responsible for managing and controlling the Everett School Employee Benefit Trust ("Trust") and administering the benefits funded directly by the Trust.

The Trustees have all fiduciary responsibilities with respect to the Trust and for the benefits funded directly by the Trust, except for the following:

1. The Everett School District ("District") and the Everett Education Association ("Association") are responsible for appointing Trustees; and
2. The investment manager is responsible for those duties and responsibilities assigned to the investment manager under the terms of the Trust document, the Trust's investment policy and the investment manager agreement.

The Trustees will develop and adopt procedures for carrying out this policy.

Cross Reference: Trust Procedure 200.1P Financial Management
Trust document

Adopted: August 29, 2005
Revised: January 24, 2011

FINANCE

Financial Management

1. The Trustees will adopt an investment policy, review the investment policy periodically, and update the investment policy as needed.
2. The Trustees will select, appoint and monitor the Trust's auditor. The Trustees will determine the criteria necessary for selection, appointment and monitoring of the Trust auditor.
3. The Trustees will select and retain an individual to perform the bookkeeping function for the Trust, including preparing Trust financials, preparing and paying Trust bills and interfacing with the Trust's auditors.

Cross Reference:	Trust Policy 220	Investment Guidelines
	Trust Policy 420	Audits
Legal Reference:	WAC 200-110-090(1)	(Applies only if the Trust self-insures any Trust benefits.) Standards for management—Standards for operations—Financial plans.

Adopted: August 29, 2005
Revised: January 24, 2011
Updated: October 16, 2011

FINANCE

Trust Fund Management

1. The Trustees will select, appoint and monitor investment advisor(s), investment manager(s) and investment consultant(s) pursuant to the Trust document.
2. The Trustees will review investment performance and oversee compliance with the investment policy annually.

Cross References:	Trust Policy 200	Financial Policy
	Trust Policy 210	Loyalty and Prudence
	Trust Policy 220	Investment Guidelines
	Trust Policy 420	Audits
	Trust document	

Adopted: August 29, 2005
Revised: January 24, 2011

FINANCE

Reporting

If the Trust self-insures any Trust benefits, the Trustees shall ensure the preparation and submission of accurate and timely annual financial reports to the state risk manager within one hundred and fifty days of the end of the fiscal year.

Cross Reference:	Trust Policy 200	Financial Policy
Legal Reference:	WAC 200-110-090	Standards for management—Standards for operations—Financial plans

Adopted: January 24, 2011
Revised: October 16, 2013

FINANCE

Interfund Loans

If the Trust self-insures any Trust benefits, interfund loans from assets held against liabilities for unpaid claims and claim adjustment expenses are not permitted except for those amounts which are clearly inactive or in excess of Trust reserve and contingency reserve requirements.

Cross References:	Trust Policy 200	Financial Policy
	Trust Policy 210	Loyalty and Prudence
	Trust Policy 220	Investment Guidelines
Legal Reference:	WAC 200-110-090	Standards for management—Standards for operations—Financial plans

Adopted: January 24, 2011
Revised: October 16, 2013

FINANCE

Loyalty and Prudence

As fiduciaries, the Trustees shall act solely in the interest of participants and their beneficiaries and for the exclusive purpose of providing benefits to participants and their beneficiaries and of defraying reasonable expenses of administering the Trust and the benefits funded directly by the Trust. The Trustees shall act prudently, with the skill and diligence that a prudent person acting in a similar capacity and familiar with such matters would employ.

Legal Reference:	WAC 200-110-150	(Applies only if the Trust self-insures any Trust benefits.) Standards for management and operations—Conflict of interest

Adopted: August 29, 2005
Revised: January 24, 2011
Updated: October 16, 2013

FINANCE

Conflict of Interest

The Trustees recognize the importance of avoiding conflicts of interest in administering the Trust. The Trustees will adopt conflict of interest procedures for Trustees and all Trust administrators to ensure such conflicts of interest are avoided.

Cross Reference:	Trust Procedure 211P	Conflict of Interest
Legal Reference:	WAC 200-110-150	(Applies only if the Trust self-insures any Trust benefits.) Standards for management and operations—Conflict of interest

Adopted: January 24, 2011
Updated: October 16, 2013

FINANCE

Conflict of Interest

1. If the Trust self-insures any Trust benefits, no Trustee; administrator, including a third-party administrator; or any other person having responsibility for the management or administration of the Trust or the investment or other handling of the Trusts' money shall:
   A. Receive directly or indirectly or be pecuniarily interested in any fee, commission, compensation, or emolument arising out of any transaction to which the Trust is or is expected to be a party except for salary or other similar compensation regularly fixed and allowed for because of services regularly rendered to the Trust.
   B. Receive compensation as a consultant to the Trust while also acting as a Trustee, third-party administrator, or employee.
   C. Have any direct or indirect pecuniary interest in any loan or investment of the program.
2. If the Trust self-insures any Trust benefits, no consultant or legal counsel to the Trust shall directly or indirectly receive or be pecuniarily interested in any commission or other compensation arising out of any contract or transaction between the Trust and any insurer, health care service contractor, health care supply provider or consultant.
3. Brokers of record for the Trust may receive compensation for insurance transactions performed within the scope of their licenses. The terms of compensation shall be provided for by contract between the broker of record and the Trust, and the amount or percentage of the compensation must be disclosed in writing. Contracts between brokers of record and the Trust shall include a provision that contingent commissions or other forms of compensation not specified in the contract shall not be paid to the broker of record as a result of any Trust insurance transactions. If the Trust self-insures any Trust benefits, the Trust shall establish a contract provision which requires the broker to provide to the Trust a written annual report on a form provided by the state risk manager which discloses the actual financial compensation received. The report shall include verification that no undisclosed commission was received as a result of any such insurance transaction made on behalf of the program.
4. No third-party administrator shall serve as a Trustee or Trust officer.

Cross Reference:	Trust Policy 210	Loyalty and Prudence
Legal Reference:	WAC 200-110-150	Standards for management and operations—Conflict of interest

Adopted: January 24, 2011
Revised: October 16, 2013

FINANCE

Investment Guidelines

Role of Trustees

The Trustees are responsible to ensure that the Trust fund is managed:

- Effectively and prudently, in full compliance with the law and the Trust; and
- For the exclusive purposes of providing benefits to participants in the Trust and defraying the costs of administering the Trust.

The Trustees will select, retain, and replace an Investment Consultant, one or more Investment Managers and may select other professional service providers in connection with the investment of the Trust funds.

Objectives

The investment objectives of the Trust funds shall be the following, in the order given:

1. Preservation of principle.
2. Meeting the liquidity needs of the Trust to pay claims and other expenses.
3. Diversification of investment to minimize the risk of large losses, within the permissible investment parameters of the Trust.

In that regard, the Investment Manager will manage a diversified portfolio of cash, U.S. government treasury bonds (hereinafter "Treasury"), U.S. government agency bonds (hereinafter "Agency") and bank issued FDIC insured Certificates of Deposit with the goal of meeting the expenditure needs of the Trust. The strategy will be implemented via a portfolio that seeks to manage security purchases and maturities such that the Trust is able to maintain on account, available for immediate use, the equivalent of two (2) months of expenditure requirements, as directed from time to time by the Trustees. Additionally, the Treasury portion of the portfolio will also be structured to hold assets equal to at least two (2) months of projected net expenditures in order to provide added liquidity in the event of an unforeseen expenditure event. To the extent that expected Trust expenditures over the prospective two (2) month period require immediate, unencumbered liquidity, Trust funds will be invested in a designated cash account and held in a money market fund rather than in individual bonds. Investments in this money market fund will also be considered Treasury securities for purposes of the allocation targets of these Investment Guidelines.

Investment Consultant

The Investment Consultant ("Investment Consultant") shall be selected by the Trustees. The Investment Consultant is responsible to monitor and evaluate the conduct and performance of the Trust's Investment Managers on a periodic basis as directed by the Trustees. The Investment Consultant shall be completely independent of the Investment Managers. The Investment Consultant's review of the performance of the Investment Manager shall include, among other things, an evaluation of the Investment Manager's compliance with these Investment Guidelines and of the results of the Investment Manager in comparison to the benchmark index and with the performance of funds with similar investment strategies to the Trust. The review may also include recommendations on changes to the Permitted Investments or other portions of these Investment Guidelines. The Investment Consultant shall report the results of its independent monitoring and evaluation to the Trustees on an annual basis, or as otherwise directed by the Trustees. The Investment Consultant also may be asked to provide educational meetings or seminars on financial, fiduciary, investment, or similar matters to the Trustees.

Investment Manager

The Trust fund shall be invested by one or more professional investment managers or management companies selected by the Trustees ("Investment Manager"). The day-to-day decisions concerning investments shall be made by the Investment Manager, who shall be a fiduciary of the Trust funds and who shall make such investments in accordance with these Investment Guidelines. The Investment Manager shall provide monthly, quarterly, annual, and other reports on the investments as required in the contract between the Trust and the Investment Manager.

The Trustees shall consider a variety of factors in selecting an Investment Manager, including costs and fees, past performance, prior experience with the investment of funds similar to the Trust, responsiveness, technical capabilities, experience and reputation of personnel, decision structure, and any other matter deemed relevant by the Trustees. The Investment Manager is required to report to the Trustees any material changes in the following which occur while the Investment Manager has been retained by the Trust:

- Material changes in the Investment Manager's investment decision structure or process.
- Changes in organization of the Investment Manager, including mergers and acquisitions.
- Any change in key personnel of the Investment Manager responsible for the formulation and execution of investment strategy.

The Investment Consultant shall review the performance of the Investment Manager annually or otherwise as directed by the Trustees. The Trustees may, but need not, consult with other investment professionals concerning such performance as necessary or desirable. The Trustees may replace the Investment Manager or add additional Investment Managers at any time in their discretion. The Investment Manager may be selected by a request for proposal or other process on a periodic basis and as determined by the Trustees.

Liquidity Needs

It is acknowledged that the liquidity needs of the Trust fund will vary from time to time depending upon circumstances then prevailing. Thus the administrative agent shall keep the Investment Manager informed on a periodic basis of the expected liquidity needs of the Trust.

Periodic Review of Guidelines

The circumstances that bear on these Investment Guidelines may change from time to time. The Trustees, in consultation with the Investment Consultant, will review these Investment Guidelines at least once annually.

Portfolio Guidelines

The Trust portfolio will be benchmarked against the Bank of American/Merrill Lynch 0-5 Year US Treasury Index and as such should generally be structured with similar credit and interest rate characteristics. Average portfolio duration is to be managed within 1-3 years and average credit quality at A+ or higher by Standard & Poor's rating agency (or equivalent Moody's rating) with no individual securities rated lower than BBB-. In addition, to insure appropriate diversification no single issuer, with the exception of government and agency issuers, shall exceed 3% of the portfolio at purchase. No single credit industry shall exceed 15% of the portfolio at purchase.

Permitted Investments

The Investment Manager may select from the following permitted investments. These investments should have varying maturity dates as necessary to comply with liquidity needs, manage interest rate risk, to and in order to achieve diversification of the Trust funds. Provided, however, that the maturity date for any permitted investment will not be longer than ten (10) years. The Trustees, in consultation with the Investment Consultant, may establish additional maturity and asset allocation parameters for each type of permitted investment.

Total Portfolio Benchmark	Bank of America/Merrill Lynch 0-5 Year US Treasury Index
Permitted Investment	**Criteria**
Cash/Money Market Funds	The money market fund is invested in the highest quality debt with a weighted average maturity of 90 days or less. The fund is registered with and regulated by the Securities and Exchange Commission. The fund is rated by at least one nationally recognized rating firm of not less than AAA or its equivalent. The fund shall not be subject to any sales loads or other such contingent charges.

Permitted Investment	**Criteria**
U.S. Government Fixed Income	Invested in public obligations of the U.S. Treasury including U.S. Treasury Notes, Bonds and other issues backed by the full faith and credit of the U.S. Government.
U.S. Government Agency Fixed Income	Invested in issues of federal agencies of the U.S. Government, including FNMA, federal land banks, federal intermediate credit banks, federal farm credit banks, federal home loan banks, FHLMC, any agency created by Act of Congress that is authorized to issue direct debt obligations of the U.S. Government.
Domestic Certificates of Deposit	Invested in certificates issued or endorsed by a domestic bank or a savings and loan association, organized and supervised under federal laws in which principal and interest are fully insured and unconditionally guaranteed by the U.S. Government. Certificates will be rated by at least one nationally recognized rating firm of not less than A-1 or P-1.

Legal Reference: WAC 200-110-090 (Applies only if the Trust self-insures any Trust benefits.) Standards for management—Standards for operations—Financial plans

Adopted: August 29, 2005
Revised: December 8, 2008
Revised: January 24, 2011
Updated: February, 2011
Revised: December 12, 2011
Updated: October 16, 2013
Revised: May 13, 2015
Revised: January 20, 2016
Revised: November 16, 2016

FINANCE

Accounting Period

The annual fiscal year for the Trust shall be the twelve month period commencing July 1 and ending June 30.

Cross Reference:	Trust Procedure 230P Trust document Section 7.1	Accounting
Legal Reference:	WAC 200-110-090	(Applies only if the Trust self-insures any Trust benefits.) Standards for management—Standards for operations—Financial plans

Adopted: August 29, 2005
Revised: January 24, 2011
Revised: October 16, 2013

FINANCE

Accounting Procedure

The Trustees shall render annually to the District and the Association an account of its administration of the Trust.

Cross Reference: Trust Policy 230 Accounting Period
Trust document section 4.4

Adopted: August 29, 2005
Revised: January 24, 2011

FINANCE

Payment For Travel Expenses

The Trust may pay travel expenses incurred by Trustees while on approved travel for meetings, seminars and conferences. The District's travel procedure is to be followed by Trustees, except that travel requests must be approved by the Trustee and travel expenses must be submitted to the Trust for reimbursement. Payment for meals is based upon per diem rates included in the District's travel procedure; all other allowable expenses shall not exceed the actual incurred expenses. Reimbursement of personal vehicle mileage is limited to current IRS regulations.

Cross References:	Trust Procedure 110.9P	Compensation
	Board Policy 6213	Reimbursement for Travel Expenses
	Board Procedure 6213P	Reimbursement for Travel Expenses

Adopted: August 29, 2005
Revised: January 24, 2011

FINANCE

Fund Balance and Solvency

Under Policy number 220, the Trustees for the Everett School Employee Benefit Trust ("Trustees") are responsible for ensuring that the Everett School Employee Benefit Trust ("Trust") is managed:

- Effectively and prudently, in full compliance with law and the Trust.
- For the exclusive purposes of providing benefits to participants in the Trust and defraying the costs of administering the Trust.

The Trustees believe this responsibility includes the requirement that sufficient funds be retained to meet the Trust's liquidity needs, which vary from time to time. To retain a stable financial base and to comply with regulatory solvency requirements, the Trust needs to maintain a Trust fund balance sufficient to: (i) pay claims for benefits funded directly by the Trust, (ii) pay costs associated with administering the Trust, and (iii) provide financial reserves for unanticipated benefit and cost expenditures and/or revenue shortfalls of an emergency nature.

The Trustees will develop and adopt procedures for carrying out this Policy.

Cross References:	Trust Policy 200	Financial Policy
	Trust Policy 220	Investment Guidelines and Rules
	Trust Procedure 250P	Fund Balance and Solvency
Legal Reference:	WAC 200-110-040	(Applies only if the Trust self-insures any Trust benefits.) Standards for solvency—Program funding requirements

Adopted: January 24, 2011
Updated: October 16, 2013

FINANCE

Fund Balance and Solvency

In order to retain a stable financial base and comply with applicable regulatory solvency requirements, the Trustees shall:

1. Maintain sufficient funds to meet the Trust's liquidity needs;
2. Establish reserves in an amount equal to the sum of three months of insurance premium costs for fully insured Trust benefits;
3. If the Trust self-insures any Trust benefits, establish reserves in an amount equal to the sum of eight weeks of (i) claim costs for all benefits funded directly by the Trust, (ii) costs, and (iii) expenses;
4. If the Trust self-insures any Trust benefits, maintain an aggregate stop-loss insurance policy with an attachment point set at or below one hundred twenty-five percent of annual expected claim costs for all benefits funded directly by the Trust; and
5. If the Trust self-insures any Trust benefits, in addition to establishing the reserves in item 3 above, establish by resolution an additional contingency reserve in an amount equal to the sum of (i) eight weeks of claims costs for all benefits funded directly by the Trust, (ii) costs, and (iii) expenses.

If the Trust self-insures any Trust benefits, in lieu of the requirements in 1, 3, 4 and 5 above, the Trustees may obtain an independent actuarial study and fund the Trust to the actuarially determined liability.

If the Trust self-insures any Trust benefits, if at the end of a program year the requirements in 1 and 4, or 5 are not met, the Trustees shall notify the Washington State risk manager of the condition, and comply with the risk manager's corrective action plan.

Cross References:	Trust Procedure 100.3P	Third Party Administrators, Consultants and Advisors
	Trust Policy 200	Financial Policy
	Trust Policy 220	Investment Guidelines and Rules
	Trust Policy 250	Fund Balance and Solvency
	Trust Policy 440	Reports
Legal Reference:	WAC 200-110-040	Standards for solvency—Program funding requirements

Adopted: January 24, 2011
Revised: October 16, 2013

COMMUNICATIONS

Communications

The goal of the Trustees for the Everett School Employee Benefit Trust ("Trustees") is to address questions or concerns of participants in or beneficiaries of the benefits provided by the Everett School Employee Benefit Trust ("Trust").

Appropriate procedures will be in place to respond to any Everett School District ("District") employee, any Everett Education Association ("Association") member, any Trust participant or beneficiary who has questions or concerns about: Trust fund management or control, benefits funded directly by the Trust, Trust accounting or audit matters, compliance by the Trustees with applicable Federal and Washington law.

The Trustees will develop and adopt procedures for carrying out this policy.

Cross References:	Trust Procedure 300.1P	Communications
	Trust Procedure 300.2P	Participant Communications
	Trust Policy 440	Reports

Adopted: August 29, 2005
Revised: January 24, 2011

COMMUNICATIONS

Communications

1. If a District employee, Association member or Trust participant or beneficiary questions a Trust benefit denial or has a question concerning eligibility for or enrollment for a benefit provided by the Trust, the Trustees will follow the Everett School Employee Benefit Trust claims and appeals procedures policy.

2. For all other questions or concerns regarding the Trust, Trust fund management or Trustee activities, the District employee, Association member or Trust participant or beneficiary should submit such question or concern to the Trustees in writing, and the Trustees will respond to the request within 120 days of receiving the request.

Cross References:	Trust Policy 300	Communications
	Trust Policy 410	Claims and Appeals
	Trust Procedure 410.1P	Claims Procedure

Adopted: August 29, 2005
Revised: January 24, 2011

COMMUNICATIONS

Participant Communications

The Trust will communicate to participants at least annually in writing or via electronic means. The Trust shall furnish each employee or retiree covered by the Trust a written description of the benefits allowable under the program, together with:

- Applicable restrictions, limitations, and exclusions;
- The procedure for filing a claim for benefits;
- The procedure for requesting an adjudication of disputes or appeals arising from beneficiaries regarding the payment or denial of any claim for benefits; and
- A schedule of any direct monetary contributions toward the program financing required by the employee.

The Trust will provide all notices it is required to directly provide under State and Federal law.

Legal Reference:	WAC 200-110-060	(Applies only if the Trust self-insures any Trust benefits.) Standards for operations—Standards for management—Disclosures
	Patient Protection and Affordable Care Act of 2010, as amended by the Health care and Education Reconciliation Act of 2010, and its implementing regulations	

Adopted: August 29, 2005
Revised: January 24, 2011
Revised: October 16, 2013

COMPLIANCE AND RISK MANAGEMENT

Compliance and Risk Management

The Trust funds are expended only for purposes of the Trust consistent with statutes and rules governing the local government or governments creating the Trust. An important responsibility of the Trustees for the Everett School Employee Benefit Trust ("Trustees") is to assure the Everett School Employee Benefit Trust ("Trust") complies with applicable federal and state law and regulations, and District policies and procedures. This includes filing and reporting as required in a timely manner and maintaining fiduciary insurance.

Appropriate procedures will be in place to verify compliance by the Trustees with applicable federal and state law and regulations, and District policies and procedures.

The Trustees will develop and adopt procedures for carrying out this policy.

Cross Reference:	Trust document Section 1.1	
Legal References:	RCW 48.62.091	(Applies only if the Trust self-insures any Trust benefits.) Program approval or disapproval—Procedures—Annual report
	RCW 48.62.121(6)	(Applies only if the Trust self-insures any Trust benefits.) General operating regulations—Employee remuneration—Governing control—School districts—Use of insurance producers and surplus line brokers—Health care services–Trusts

Adopted: August 29, 2005
Revised: January 24, 2011
Revised: October 16, 2013

COMPLIANCE AND RISK MANAGEMENT

Claims and Appeals

Benefits under the Everett School Employee Benefit Trust ("Trust") will be paid only if the Trustees of the Trust ("Trustees") or their delegate decides, in their discretion, that participants and their dependents are entitled to them. Any person claiming a benefit, requesting an interpretation or ruling under a benefit plan offered through or by the Trust or requesting information under a benefit plan offered through or by the Trust shall follow the claims procedure established by the Trustees or any insurance carrier insuring Trust benefits. The claims procedure shall conform to the requirements of applicable Washington law.

The Trustees will also establish procedures for claims audits, in compliance with Washington law.

Cross References:	Trust Procedure 410.1P	Claims Procedure
	Trust document Section 4.16	
Legal Reference:	WAC 200-110-120	(Applies only if the Trust self-insures any Trust benefits.) Standards for claims management—Claims administration

Adopted: January 1, 2004
Revised: January 24, 2011
Revised: October 16, 2013

COMPLIANCE AND RISK MANAGEMENT

Claims Procedure

Where a third party administrator, insurance company, health care services contractor or HMO is in place with respect to a certain benefit, such third party has been delegated the responsibility for administering and determining initial claims and reviewing and reconsidering benefit, enrollment or eligibility denials if appealed ("appeals"). The entities that are responsible for administering and determining initial claims and appeals are called "Claims Administrators."

In certain limited instances, however, the Trustees may also be a Claims Administrator. The Trustees are a Claims Administrator in the following circumstances:

1. If the Everett School District ("District") denies a request for enrollment in or eligibility for a benefit plan offered through the Trust, the employee can appeal the denial to the Trustees.
2. If a participant in a self-funded benefit offered through the Trust exhausts a third party administrator's appeal process, the participant can submit a final appeal of the benefit, enrollment or eligibility denial to the Trustees.

The Claims Administrator generally will make decisions on a claim within the time frames outlined in participant communications, such as Certificates of Coverage issued by insurance carriers or summaries of plan benefits issued by third party administrators. If a participant or his or her dependent submits a claim ("claimant") and the claim is denied in full or in part, the claimant will be notified in writing.

Claims for benefits are considered filed when the Claims Administrator receives the claim.

I. Initial Claim Determinations

A. Benefit Denials

The Trust has delegated the responsibility of administering and determining initial claims for benefits to the following third-party administrators and insurance carriers:

1. Premera (the Washington Education Association (WEA) Premera Medical Plans
2. Washington Dental Service (Delta Dental of Washington) (the WEA Delta Dental of Washington Plan)
3. Willamette Dental (the WEA Willamette Dental Plan)
4. Premera (the WEA Vision Plans)
5. Group Health Cooperative (Medical Plan)
6. Metropolitan Life Insurance Company (Life and Accidental Death & Dismemberment Insurance Plans)
7. The Standard (Voluntary Short-Term and Long-Term Disability Plans)
8. Magellan (Employee Assistance Plan)

Every effort will be made by the Claims Administrators to process claims as quickly as possible. The Claims Administrator will notify a claimant in writing if all or part of the claim will be denied within the time frames outlined in participant communications, such as Certificates of Coverage issued by insurance carriers or summaries of plan benefits issued by third party administrators.

The Claims Administrator may secure independent medical or other advice and require such other evidence as it deems necessary to decide claims.

At any time, a claimant has the right to appoint someone to pursue the claim on his or her behalf. The claimant must notify the Claims Administrator in writing and give the Claims Administrator the name, address, and telephone number where the claimant's appointee can be reached.

If a claimant submits an initial claim for benefits directly to the Trust rather than to the applicable above-listed Claims Administrator, the Trustees will direct the claimant to the appropriate above-listed Claims Administrator as soon as is reasonably possible.

B. Eligibility or Enrollment Denials

If a claimant submits a claim to the Trustees rather than to the applicable Claims Administrator regarding eligibility for or enrollment in a benefit plan offered through the Trust, the Trustees will refer the claimant to the Everett School District ("District") or to the appropriate Claims Administrator listed in I.A. above.

C. Notification of Denial

If the Claims Administrator issues a benefit denial, the claimant will be notified of the denial in writing. Except due to Trust amendment or termination, a "benefit denial" is a denial or reduction of benefits, failure to provide benefits, termination of benefits (in whole or in part). The notification of denial will be in the standard written format used by the Claims Administrator.

If the District or a Claims Administrator issues an eligibility or enrollment denial, the claimant will be notified of the determination either orally or in writing. An "eligibility or enrollment denial" is a denial of enrollment in or eligibility for a benefit plan offered through the Trust. If the denial is in writing, the notification of denial will be in the standard written format used by the District or the Claims Administrator.

II. <u>Appealing Denied Claims</u>

A. Appealing Benefit Denials

The claimant or his or her authorized representative may appeal a benefit denial. Appeals of benefit denials must be made to the Claims Administrators listed in 1.A. above. Such appeal must be made in writing and submitted within the time frames outlined in participant communications, such as Certificates of Coverage issued by insurance carriers or summaries of plan benefits issued by third party administrators.

If the claimant does not follow the Claims Administrator's proscribed procedures, he or she loses the right to appeal the denial.

B. Appealing Eligibility or Enrollment Denials

The claimant or his or her authorized representative may appeal an eligibility or enrollment denial. If the eligibility or enrollment denial was made by a Claims Administrator, the appeal must be made to the Claims Administrator. Such appeal must be in writing and submitted within the time frames outlined in participant communications, such as Certificates of Coverage issued by insurance carriers or summaries of plan benefits issued by third party administrators.

If the eligibility or enrollment denial was made by the District, the claimant may appeal the denial to the Trustees by using the Final Appeal Form. In this instance, the appeal must be made on the Final Appeal Form within 180 days of the District's notification of denial or else the claimant loses the right to appeal.

C. Notification of Appeal Denial

If the claimant appeals a benefit, eligibility or enrollment denial made by a Claims Administrator listed in 1.A. above, and if the decision on appeal affirms the initial claim denial, the claimant will be notified of the decision upon appeal in writing. Such notification will be in the standard written format used by the Claims Administrator and be provided by the Claims Administrator within the time frames outlined in participant communications, such as Certificates of Coverage issued by insurance carriers or summaries of plan benefits issued by third party administrators.

If the claimant appeals an eligibility or enrollment denial made by the District, the Trustees will review and render a written decision on the claimant's appeal, adverse or not, no later than 120 days after the Trustees received the appeal. Such notification will be on the Everett School Employee Benefit Trust Notice of Eligibility/Enrollment Appeal Denial form.

III. Final Appeal for Self-Funded Benefits

For insured benefits, any claim or appeal determination made by the insurance carrier is final and cannot be appealed to the Trustees. For benefits that are funded directly by the Trust and not through a contract of insurance between the Trust and an insurance carrier, once a participant exhausts the third party administrator's appeal process, the participant may submit a final appeal to the Trust. The appeal must be made on the Trust's Final Appeal Form within 180 days of the third party administrator's notification of a benefit denial on appeal or else the claimant loses the right to appeal to the Trustees. For insured benefits, any claim or appeal determination made by the insurance carrier is final and cannot be appealed to the Trustees.

The Trustees will review and render a written decision on the claimant's final appeal, adverse or not, no later than 120 days after the Trustees received the appeal. Such notification will be on the Everett School Employee Benefit Trust Notice of Benefit Appeal Denial form.

Cross Reference:	Trust Policy 410	Claims and Appeals
Legal Reference:	WAC 200-110-120	(Applies only if the Trust self-insures any Trust benefits.) Standards for claims management—Claims administration

Adopted: January 1, 2004
Revised: October 10, 2008
Revised: January 24, 2011
Revised: October 16, 2013

COMPLIANCE AND RISK MANAGEMENT

Claims Audits

The Trustees shall obtain a claims audit of claim reserving, adjusting, and payment procedures every three years at a minimum. The claims audit shall be conducted by a qualified claims auditor not affiliated with the Trust, its broker of record, or its third-party administrator. Such review shall be in writing and identify strengths, areas of improvement, findings, conclusions and recommendations. Such review shall be provided to the Trustees and retained for a period of not less than six years. The scope of the claims audit shall include the claims administration procedures in Procedure No. 410.1P. The Trustees will obtain more frequent claims audits if required by the state risk manager.

Cross Reference:	Trust Policy 410	Claims and Appeals
Legal Reference:	WAC 200-110-120	(Applies only if the Trust self-insures any Trust benefits.) Standards for claims management—Claims administration

Adopted: January 24, 2011
Revised: October 16, 2013

COMPLIANCE AND RISK MANAGEMENT

Audits

If the Trust self-insures any Trust benefits, the Trust is subject to audit by the Washington State auditor, and it is the policy of the Trustees to assist as necessary with the audit. In such event, the Trust has decided to assume a risk of loss and will have available for inspection by the state auditor a written report indicating the class of risk or risks the Trustees have decided to assume.

The Trust is audited annually by an independent auditor for purposes of compliance with the Internal Revenue Code.

Cross Reference:	Trust Procedure 200.1P	Financial Management
Legal References:	RCW 48.62.031(3 & 5)	Authority to self-insure—Options—Risk manager
	Internal Revenue Code 501(c)(9)	

Adopted: August 29, 2005
Revised: January 24, 2011
Revised: October 16, 2013

COMPLIANCE AND RISK MANAGEMENT

Health Insurance Portability and Accountability Act of 1996 (HIPAA) – Privacy, Security, and Reportable Breach Notification Policies

The Trustees intend these policies to provide guidelines to protect the privacy of participants and beneficiaries participating in the Everett School Employee Benefit Trust ("Trust"), and to ensure that all information related to participants and beneficiaries is maintained in the strictest confidence and in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing privacy regulations (the "Privacy Rule") and security regulations (the "Security Rule"). Under the Privacy Rule, the Trust's policy restricts the Group Health Plan's use and disclosure of protected health information, or "PHI." Under the Security Rule, this policy ensures the confidentiality, integrity and availability of electronic PHI, or "ePHI," and protects against any reasonably anticipated threats or hazards to the security or integrity of ePHI. The Trustees also intend to comply with the rules for reporting certain breaches of confidentiality to plan participants under HIPAA and Washington state law.

Details of the policies and implementing procedures may be found in the Trust's HIPAA Privacy Policy and HIPAA Security Policy.

Cross References:

HIPAA Privacy Policy	
HIPAA Security Policy	
District Policy 3245	Technology
District Procedure 3245P	Technology
District Policy 5225	Technology
District Procedure 5225P	Technology

Approved: August 29, 2005
Revised: January 24, 2011
Revised: April 30, 2012
Revised: March 17, 2016

COMPLIANCE AND RISK MANAGEMENT

Reports

The Trustees shall file or cause to be filed all documents within the time prescribed by law or regulation for filing such documents. The Trustees will furnish such reports, statements or other documents to participants and beneficiaries as required by federal or state statute or regulation, within the time prescribed for furnishing such documents. If the Trust self-insures any Trust benefits, this includes electronic submission of the annual report and a list of contracted consultants, to the state risk manager no later than 150 days after the end of the fiscal year.

Cross References:	Trust Policy 300	Communications
	Trust Policy 400	Compliance and Risk Management
	Trust document Section 4.12	
Legal References:	RCW 48.62.091	Program approval or disapproval—Procedures—Annual report
	WAC 200-110-130	Standards for management and operations—State risk manager reports
	Internal Revenue Service Form 990	

Adopted: August 29, 2005
Revised: January 24, 2011
Revised: October 16, 2013

COMPLIANCE AND RISK MANAGEMENT

Records Retention and Management

The Trustees recognize the importance of Trust records as the record of acts of the Trustees and the repository of such information. The records of the Trust include but are not limited to, agendas, meeting minutes, individual claim appeal information and documents prepared by outside advisors necessary to administer the Trust.

Some of these records are public records and must be retained and destroyed in accordance with the Records Retention Manual and General Records Retention Schedule provided by the Office of the Secretary of State, Division of Archives and Records Management. Some of the records may contain protected health information (as the term is defined by HIPAA) and must be handled by the Trustees and others authorized to handle PHI in accordance with the Trust's HIPAA Privacy Manual (as amended for Security). In addition, PHI must be retained and destroyed as described in the HIPAA Privacy Manual (as amended for Security).

Cross Reference:	Trust Policy 430	Health Insurance Portability and Accountability Act of 1996 (HIPAA) – Privacy and Security HIPAA Privacy Manual, as amended for Security
	Board Policy 6560	Records Management and Retention
	Board Procedure 6560P	Records Management and Retention
	General Records Retention Schedule, School Districts and Educational Service Districts, provided by the Office of the Secretary of the State, Division of Archives and Records Management	

Adopted: August 29, 2005
Revised: January 24, 2011

COMPLIANCE AND RISK MANAGEMENT

Family and Medical Leave Act and Continuation of Coverage

Benefits under the Everett School Employee Benefit Trust ("Trust") are provided for participants and beneficiaries during periods covered by the Family and Medical Leave Act of 1993 ("FMLA") and other approved paid leaves of absence. When a participant's FMLA leave or other approved paid leave ends, continuation coverage will cease under the Trust unless a qualified beneficiary elects continuation coverage pursuant to the Consolidated Omnibus Budget Reconciliation Act of 1985 ("COBRA"). Qualified beneficiaries who elect COBRA continuation coverage must pay the full cost of such coverage.

For participants on an approved paid medical leave of absence, including FMLA leave, commencing prior to September 1, 2006 and who continue to make employee contributions as required for continuation coverage, the Trust will continue to contribute the employer-paid portion of the cost of coverage until the expiration of the applicable twelve month period.

Adopted: August 18, 2006
Revised: January 24, 2011

COMPLIANCE AND RISK MANAGEMENT

Wellness Program

The Trustees recognize the importance of a multi-faceted wellness program to promote the overall health and well-being of the District's employees. The Trustees desire to incorporate a comprehensive wellness program into the Trust benefits, as shown in the attached graphic, in order to:

1. Promote healthy lifestyles by District employees and their families.
2. Provide health education and health awareness among District employees.
3. Reduce the Trust's medical plan costs over the long-term.
4. Increase District employee productivity, job performance, and morale and decrease health-related absenteeism.

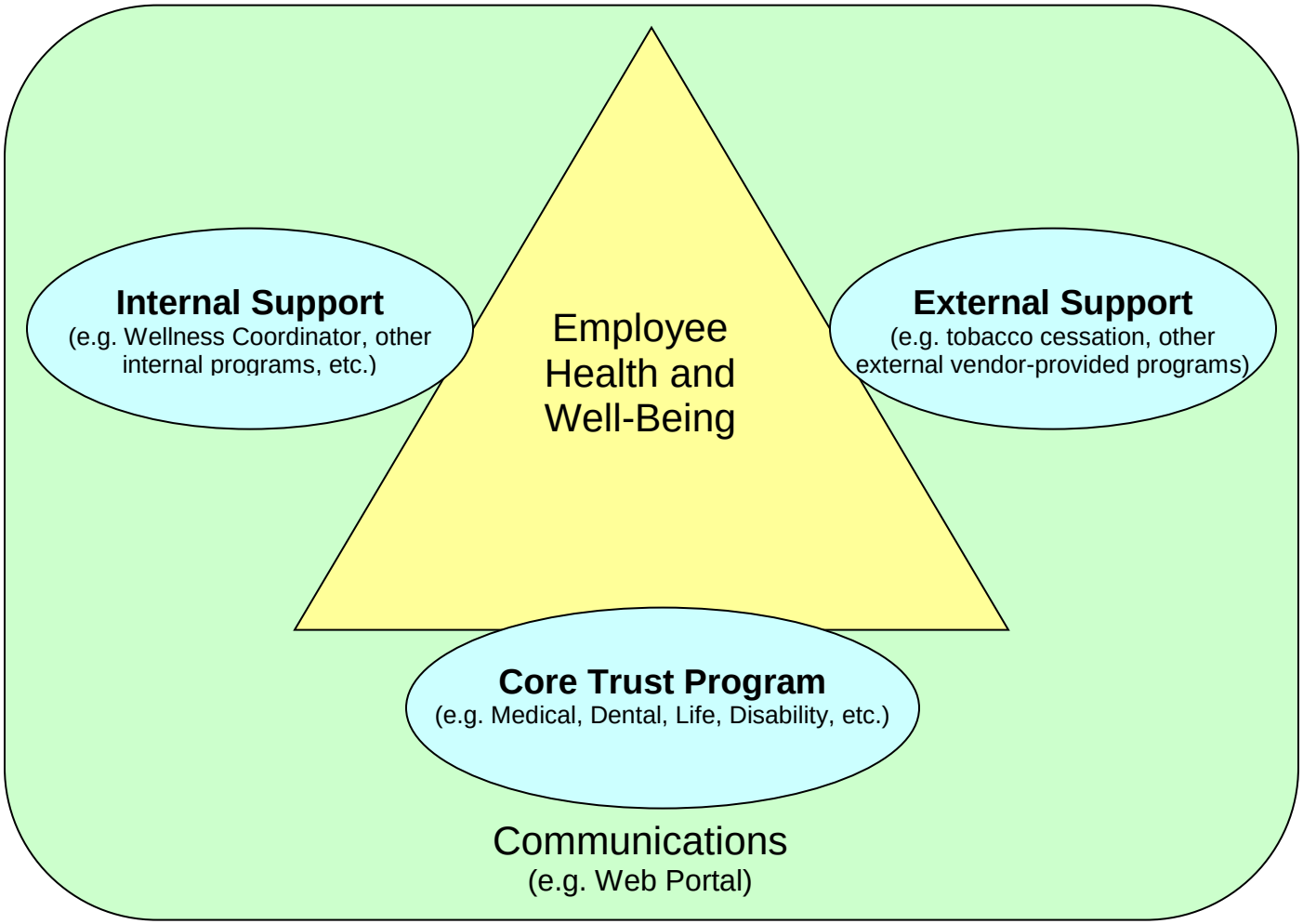
The goal of the wellness program is to create a culture of wellness that encourages employees to make healthier life-style choices through incentives, education, and enhanced benefits. The comprehensive wellness program may include some or all of the following:

1. Hiring of full-time wellness coordinator.
2. Health risk assessments.
3. Enhanced wellness benefits in the Trust's medical, EAP, and other core benefits for total health management.
4. External wellness programs provided off-site, such as smoking and weight loss programs.
5. Internal programs provided on District property, such as stress management and employee wellness education and communications.

Legal Reference: WAC 200-110-070 (Applies only if the Trust self-insures any Trust benefit.) Standards for operations—Standards for management—Wellness programs

Adopted: August 25, 2008
Revised: January 24, 2011
Revised: October 16, 2013

Everett School Employee Benefit Trust



ESEBT Program Investment Philosophy

The overall goal of the Trust's wellness program is to promote the overall health and well-being of the covered members. The foundation of the program is the Core Programs, which provide the basic level of protection to the members. The internal and external programs provide supplemental assistance to members, helping those that are healthy to continue to maintain their health, while also providing tools and resources to employees seeking to improve their health and reduce their health risks.

In certain years, dependent upon the financial status of the Trust reserves and the desired direction of the program by the trustees, the level of investment in the core, internal and external programs can be adjusted upward or downward accordingly.

COMPLIANCE AND RISK MANAGEMENT

Fees

If the Trust self-insures any Trust benefit, the Trust is subject to an expense and operating cost fee from the Washington State risk manager, and it is the policy of the Trustees to pay any such fee levied against the Trust within 60 days of the date of invoice.

Legal Reference:	WAC 200-110-160	Standards for operations—State risk manager—Expense and operating cost fees

Adopted: January 24, 2011
Revised: October 16, 2013

COMPLIANCE AND RISK MANAGEMENT

Open Public Meetings

The Trust is subject to the Open Public Meetings Act as described in Title 42, Chapter 30 RCW, and it is the policy of the Trustees to comply with those requirements.

Trust meetings will be scheduled in compliance with the law and as deemed by the Trust to be in the best interests of the employees. The Trust will conduct business through (1) regular meetings, (2) special meetings, and (3) emergency meetings. Public notice shall be properly given for any special meeting; whenever a regular meeting is adjourned to another time; or, when a regular meeting is to be held at a place other than the school district boardroom.

Regular meetings shall normally be held the third Wednesday of each month in the district boardroom or at other times and places as determined by the presiding officer or by majority vote of the Trust. If regular meetings are to be held at places other than the boardroom or are adjourned at times other than a regular meeting time, notice of the meeting shall be made in the same manner as provided for special meetings. All regular meetings of the Trust shall be held within the school district boundaries. The Trust shall adopt an annual regular meeting schedule by no later than June 30 of each year.

Matters that employees and citizens wish to have included on the agenda should be submitted to the chairperson one week prior to a scheduled Trust meeting. The chairperson shall make the decision to include or reject a request for an agenda item. The chairperson will notify the person(s) making the request of the decision.

When agenda presentations are made by more than one person, the leader or spokesperson should be identified. It should be understood that inclusion of a presentation on the agenda is not a commitment that the Trust will indicate its position or take any action on at that meeting.

Special meetings may be called by the chairperson or on a petition of a majority of the Trust members. A written notice of a special meeting, stating the purpose of the meeting, shall be sent to each Trustee not less than twenty-four (24) hours prior to the time of the meeting. Business transacted at a special meeting will be limited to that stated in the notice of the meeting.

All meetings shall be open to the public with the exception of executive sessions authorized by law. Final action resulting from executive session discussions will be taken during a meeting open to the public as required by law.

During the interim between meetings, the office of the Central Region Assistant Superintendent shall be the office of the Trust. The Trust's public records shall be open for inspection in the manner provided by and subject to the limitation of the law.

Legal References:	RCW 28A.330.070	Office of Board—Records available for public inspection
	RCW 28A.343.380	Meetings
	RCW 42.30	Open Public Meetings Act
	WAC 200-110-190	(Applies only if the Trust self-insures any Trust benefits.) Standards for Operations—Meetings

Adopted: January 24, 2011
Revised: September 25, 2013
Updated: October 16, 2013

COMPLIANCE AND RISK MANAGEMENT

Open Public Meetings

All meetings, including study sessions and retreats, must be advertised in the Benefit Trust section on the Everett Public Schools' web page as meetings that are open to the public. If the Trust wishes to devote all or most of a special meeting to an issue(s) to be discussed in executive session (Policy #491), the special meeting should be called to order and then recessed to an executive session. The purpose of the executive session should be announced and recorded in the minutes (e.g., personnel matters and litigation).

All regular meetings must be held within the District boundaries. Special meetings may be held outside the District with proper notice of the time and location.

Meeting Notices

A regular meeting does not require a public notice if held at the time and place provided by board policy. If the Trust does not meet at its regular location, the meeting should be treated as a special meeting. Each Trustee should receive a printed agenda twenty-four hours in advance of the meeting.

While other items of business may be discussed at a special meeting, no final action can be taken on topics, which have not been identified on the published agenda. If an item is to be discussed in executive session in accordance with policy #491, the item of business must also appear on the agenda if final action is to be taken following the executive session.

The Trust may recess a regular, special or recessed meeting to a specific future time. Notice of such a recess and continuation must be posted at or near the door of the meeting room.

Adopted: January 24, 2011

RESTATEMENT OF

EVERETT SCHOOL EMPLOYEE

BENEFIT TRUST

EFFECTIVE AS OF SEPTEMBER 1, 2005

CONTENTS

SECTION **PAGE**

RESTATEMENT

EVERETT SCHOOL EMPLOYEE

BENEFIT TRUST

THIS AGREEMENT is made and entered into effective as of September 1, 2005, by and among Everett School District ("District"), Everett Education Association ("Association"), and the undersigned who have been appointed by the District and the Association as trustees (collectively referred to as "Trustees").

RECITALS

A. The original Everett School Employee Benefit Trust (the "Trust") document was adopted as of July 1, 1985.

B On May 19, 1988, the Trust was approved by the Internal Revenue Service as a voluntary employees' beneficiary association ("VEBA") within the meaning of Section 501(c)(9) of the Internal Revenue Code of 1986, as amended (the "Code"), to provide for the payment of certain health, accident, disability, death and other benefits as described in Section 501(c)(9) of the Code.

C. On October 1, 1999, the Trust was approved as an individual self-insurance program under Title 48, Chapter 62 of the Revised Code of Washington ("RCW") by the state risk manager.

D. In order to effect certain changes and comply with applicable law, the District, Association, and Trustees wish to restate the trust document for the Everett School Employee Benefit Trust.

District, Association, and Trustees AGREE as follows:

1. ESTABLISHMENT OF TRUST

1.1 Name and Purpose: The Name of this Trust is the "Everett School Employee Benefit Trust". The purpose of the Trust is to provide payment for the benefits described in Section 1.4 to participating employees and their dependents.

1.2 Federal and State Law Compliance: The Trust is a VEBA trust within the meaning of Section 501(c)(9) of the Code and is intended to qualify for exemption from federal income taxation. The Trust is also an individual self-insurance program under Title 48, Chapter 62 RCW. The Trust shall be interpreted consistent with the intent of Section 501(c)(9) of the Code and Title 48, Chapter 62 RCW and administered for the exclusive benefit of participating employees and their dependents, in a non-discriminatory manner, solely to provide benefits in accordance with the Trust.

1.3 Trust Fund: The District delivered or caused to be delivered to the Trustees any assets required for 1984-85 school year pursuant to the collective bargaining agreement between the District and Association. These assets (if any) and contributions hereinafter made by the District and Participants to the Trust, together with the income therefrom, constitute the trust fund ("Fund"). The Trustees shall have exclusive authority and discretion to manage and control the Fund, except as hereinafter provided in Section 3.

1.4 Benefits: Any benefits designated by the Trustees may be funded through the Trust, provided the benefits are described in Section 501(c)(9) of the Code.

The Trust provides the following benefits:

(a) Medical and prescription drug benefits funded by the Trust and administered by a third party administrator selected by the Trustees to administer such benefits. Benefit provisions are contained in the documents identified in Appendix I.

(b) Medical benefits funded through insurance purchased by the Trust from an entity selected by the Trustees that is licensed or authorized by the State of Washington to transact insurance in the State of Washington. Benefit provisions are contained in the contract or contracts identified in Appendix I.

(c) Employee assistance benefits funded through insurance purchased by the Trust from an entity selected by the Trustees that is licensed or authorized by the State of Washington to transact insurance in the State of Washington. Benefit provisions are contained in the contract or contracts identified in Appendix I.

(d) Dental benefits funded through insurance purchased by the Trust from an entity selected by the Trustees that is licensed or authorized to transact insurance in the State of Washington. Benefit provisions are contained in the contract or contracts identified in Appendix I.

(e) Basic life and accidental death and dismemberment benefits funded through insurance purchased by the Trust from an entity selected by the Trustees that is licensed or authorized by the State of Washington to transact insurance in the State of Washington. Benefit provisions are contained in the policy identified in Appendix I.

(f) Long term disability benefits funded through insurance purchased by the Trust from an entity selected by the Trustees that is licensed or authorized by the State of Washington to transact insurance in the State of Washington. Benefit provisions are contained in the policy identified in Appendix I.

(g) Voluntary short-term disability, supplemental life and long-term care benefits funded through insurance purchased by the Trust from an entity selected by the Trustees that is licensed or authorized by the State of Washington to transact insurance in the State of Washington. Benefit provisions are contained in the policy identified in Appendix I.

Trustees may change the benefits described above and revise Appendix I at any time without amendment to the Trust so long as the benefits are described in Section 501(c)(9) of the Code.

1.5 Participation: The individuals entitled to benefits hereunder shall be:

(a) those employees of the District who are not covered by a collective bargaining agreement and who are employed on a full-time or part-time basis as determined by the District;

(b) those employees of the District who are designated as eligible employees in the collective bargaining agreement between the District and the Association;

(c) those employees of the District who are covered by a collective bargaining agreement between the District and a union, other than the Association, which provides for participation in Trust benefits; and

Any union or employee group which shall hereafter become parties to this Trust or receive benefits from same shall accept the terms of this Trust by written instrument, and shall agree to be represented by and be bound by the action of the Trust.

1.6 Administrator: The Administrator of the benefit provided hereunder shall be the Trustees.

1.7 Withdrawal from Trust; Forfeiture of Interest: In the event that any participating employee group, other than the District or Association, elects to terminate its participation in this trust and to withdraw from same, said withdrawing employee group shall forfeit its interest in any contingency reserves, initial deposits, refunds, surpluses, earnings, residual funds, dividends or other assets owned or held by the Trust and said property shall be used for the benefit of the remaining employees participating in the Trust for the purposes of this Trust.

2. CONTRIBUTIONS TO THE FUND

2.1 Time and Amount of Contributions: Contributions to the Fund by the District with respect to participants who are not covered by a collective bargaining agreement shall be made at such times and in such amounts as necessary to provide the benefits described herein. District contributions with respect to an association or union participant shall be determined by the collective bargaining agreement between the District and association or union which covers such participant, and

shall be made at such times as required by the collective bargaining agreement. The Trustees shall determine the amount of Participant contributions, if any, necessary to obtain each benefit. Participant contributions are voluntary.

2.2 Accountability of Trustees: The Trustees shall be accountable only for the contributions actually received. The Trustees shall be under no duty to see that the contribution made to the Fund comply with the provisions of the collective bargaining agreement or benefit contracts, and shall not be obligated to collect contributions from participants. The Trustees shall have all the authority necessary to take appropriate action for the purpose of collecting contributions to the Trust, including if necessary, the authority to institute legal proceedings for such purposes.

2.3 Return of Contributions: Contributions may be returned to a participant or the District as appropriate if the contribution is made by reason of a mistake of fact (or law if permitted by applicable federal law) and such contribution to the extent of the mistaken amount is returned within one year of its payment.

3. MANAGEMENT OF THE FUND

3.1 Investment of the Fund In Cash Equivalents: Such portion of the assets of the Fund as, in the opinion of the Trustees, are required for the payment of benefits shall be deposited in one or more bank accounts with such bank or banks as the Trustees shall designate. The remaining assets of the Fund shall be invested by the Trustees in accordance with section 4 below.

3.2 Distribution of Benefits: The Trustees shall distribute benefits under the Plan. The Trustees may delegate this duty to a third party administrator by authorizing such administrator to withdraw and distribute directly from the Trust's bank accounts, the benefits to which participants may be entitled. The Trustees need not see to the application of said distributions and shall not be liable for any payment made by them or a third party administrator in good faith, without actual notice or knowledge of a change in the condition or status of any person affecting his or her right to receive payments hereunder.

3.3 Correction of Errors: Any mistake in any direction, certificate, notice, or other document furnished or issued by the Trustees in connection herewith may be corrected when the mistake becomes known and the Trustees may direct any adjustment or action which they deem practicable under the circumstances to remedy the mistake.

4. POWERS AND DUTIES OF TRUSTEES

4.1 Investment: The Trustees shall invest and reinvest the portion of the assets of the Fund not designated under section 3.1 to be deposited in a bank account or accounts, and the income and earnings thereon. The Trustees are specifically authorized to invest a portion of the Fund in deposits which bear a reasonable interest rate in a bank or similar financial institution supervised by the United

States or a state, irrespective of whether such bank or similar financial institution is a fiduciary with respect to this Trust Agreement.

The Trustees may appoint an Investment Manager to manage, acquire and dispose of any asset in the Fund, provided that the party designated is either registered as an investment adviser under the Investment Advisers Act of 1940, or is a bank as defined in that Act, or is an insurance company qualified under the laws of more than one state of the United States to perform the duty of managing, acquiring and disposing of such assets. Such Investment Manager shall be required by the Trustees to acknowledge in writing that it is a Fiduciary with respect to this Benefit Trust. Neither the Trustees, District, Association nor any agent of any of them shall be liable for the acts or omissions of such Investment Manager so appointed or be under any obligation to invest or otherwise to manage any other of the assets of the Fund which are subject to the management of the Investment Manager. The Trustees shall have the power to remove and replace any Investment Manager whose performance they deem unsatisfactory.

All investment earnings and other passive income of the Fund shall be set aside as realized solely for the purpose of providing the benefits described herein and for payment of administrative costs of so providing such benefits. No part of the net earnings of the Fund shall inure, other than by payment of benefits, to the benefit of any private shareholder or individual.

4.2 Trustees' Powers: The powers and authority or the Trustees shall be exercised solely in a fiduciary capacity consistent with and in the furtherance of the purpose of this Trust and not otherwise. With respect to the assets of the Trust held hereunder, Trustees shall have the following powers and authority:

(a) To manage, acquire and dispose of such assets;

(b) To acquire securities or other property by purchase or subscription;

(c) To sell, exchange, convey, transfer or otherwise dispose of any securities or other property held by it by private contract or at public auction;

(d) To collect and reinvest the income of such assets;

(e) To cause any securities or other property unregistered to be registered in their own name or in the name of one or more of their nominees, and to hold any investment in bearer form, but the books and records of Trustees shall at all times show that all such investments are part of the Fund;

(f) To make, execute, acknowledge and deliver any and all documents of transfer and conveyance and any and all other instruments that may be necessary or appropriate to carry out their powers and duties hereunder;

(g) To vote any securities held in the Fund;

(h) To institute any legal action or to appear or participate in any legal action to which they may be made a party, but only on the undertaking of the Fund, or the District and Association to defray all expenses or losses incident thereto;

(i) To borrow money for purposes of the Trust and to execute and deliver notes, mortgages, pledges or other instruments as may be necessary in connection therewith;

(j) To do all such acts and exercise all such rights and privileges, although not specifically mentioned herein as Trustees deem necessary to administer the Fund and carry out the purposes of the Trust;

(k) To delegate and allocate by resolution specific responsibilities, obligations and duties imposed by the Trust to one or more Trustees or to committees composed of any number of Trustees;

(l) To review, adjust. and settle, in their discretion, any claims brought by or against them as Trustees.

No person dealing with Trustees shall be bound to see to the application of any money, or property paid or delivered to Trustees or to inquire into the validity or propriety of any transaction.

4.3 Expenses: Trustees shall be reimbursed from the Fund for expenses reasonably incurred but shall not be entitled to compensation for the performance of their duties as Trustees. All reasonable expenses which are necessary to operate and administer the Fund, including fees paid to persons employed pursuant to section 4.5 shall be paid from Trust assets.

4.4 Accounting: The Trustees, within a reasonable period following the close of the Trust Accounting Period and such other times as the Trustees may designate, shall render to the District and Association an account of its administration of the Trust Fund during the preceding Accounting Period or the period elapsed since their last accounting. The records of the Trustees and their designated administrators shall be open to inspection by representatives of the District and Association at all reasonable times.

4.5 Employment of Other: The Trustees are authorized to delegate and allocate ministerial duties to others, to engage such persons, counsel and agents, and to obtain such administrative, clerical, medical, legal, audit and actuarial services, as it may deem necessary in carrying out the provisions of the Trust.

4.6 Interpretation and Employment of Counsel: The interpretations placed on this agreement and its terms by the Trustees shall, in the absence of fraud, be conclusive, and in case any dispute or doubt arises as to the construction of this instrument or the rights, liabilities, or duties of the Trustees under it, the Trustees may employ counsel, who may not be counsel for the District or Association, and

take advice of such counsel as they may select and shall be fully protected in acting upon and following such advice. The Trustees shall be entitled to be reimbursed from the Fund for the expense so incurred.

4.7 Action by the Trustees: The decision or act of a majority of the Trustees upon any matters, whether with or without a meeting shall be controlling; provided, all such Trustees were given the opportunity to vote on such decision or act. The Trustees may by written instrument designate any one or more of them to execute on behalf of the Trustees any document to effectuate their actions and may, by written instruments, revoke or change any such designations. The following shall govern the decision making processes of the Trustees:

(a) Trustees shall meet as often as necessary to carry out the purpose and objectives of this Trust; provided, there shall be at least one meeting of the Trustees in each calendar year.

(b) The Chairperson may schedule meetings with seventy-two (72) hours notice. In cases of emergency, the seventy-two (72) hour notice is not required. Further, any two (2) Trustees may call a meeting of the Trustees at any time by giving at least ten (10) days written notice of the time and place of the meeting to each of the other Trustees. Meetings of the Trustees may also be hold at any time without notice if all of the Trustees consent thereto.

(c) Decisions or actions of the Trustees taken at any meeting shall be determined by majority vote of the Trustees present at the meeting, provided that a quorum is present. A quorum shall require four (4) Trustees be present with at least 50 percent of those Trustees present representing District. No proxy voting shall be allowed. In the event of a deadlock among the Trustees, no decision or action shall be taken by the Trustees.

(d) The Trustees shall select among themselves a Chairperson and Secretary who shall serve for terms of one fiscal year and until their successors are selected. For the first year of existence of this Trust the Chairperson position shall be filled from the District appointed Trustees and the Secretary position shall be filled from the Association appointed Trustees. For the second and all succeeding years, the position of Chairperson and Secretary shall alternate between the respective Trustee groups. Each Trustee group shall select the individual who will serve in the appropriate capacity from among its own members by majority vote.

4.8 Bonding: The Trustees shall be bonded as required by applicable law. The costs of premiums for such bonds shall be paid out of the Fund.

4.9 Determination of Rights: The Trustees shall have complete authority to determine, in accordance with the provisions of the Appendices the existence or

nonexistence, nature and amount of the rights and interest of all persons in the Fund and under the Appendices. The Trustees shall have authority to enforce the agreement on behalf of any and all, persons having or claiming any interest in the Fund. In any action or proceeding affecting the Fund the Trustees shall be the only necessary parties, and no employee or former employee of the District or any other person having or claiming to have an interest in the Fund shall be entitled to any notice or process. Any judgment which may be entered in any such action or proceeding shall be binding and conclusive on all persons having or claiming to have any interest in the Fund.

4.10 Evidence of District or Association Action: Any action by the District or Association pursuant to any of the provisions of this Trust shall be evidenced by a written instrument executed by the District or Association respectively or by any person or persons authorized from time to time by the District or Association respectively to take such action as its representative or representatives. The Trustees shall be fully protected in taking or omitting any action in accordance with written directions reasonably appearing to conform with the foregoing provision.

4.11 Records: The Trustees shall maintain records of participant contributions, District contributions, and benefits paid to or on behalf of participants. The exact nature of medical disabilities giving rise to claims shall be confidential to the provider and participant, unless disclosure is otherwise allowed by law.

4.12 Reports: The Trustees shall file or cause to be filed all annual reports, returns, and financial and other statements as required by any federal or state statute, including RCW 48.62.091, agency, or authority, within the time prescribed by law or regulation for filing said documents; and to furnish such reports, statements, or other documents to such participants and beneficiaries as required by federal or state statute or regulations, within the time prescribed for furnishing such documents.

4.16 Claims Procedures: Any person claiming a benefit, requesting an interpretation or ruling under a benefit plan offered through or by the Trust or requesting information under a benefit plan offered through or by the Trust shall follow the claims procedure established by the Trustees. The claims procedure shall conform with the requirements of applicable Washington law.

5. RESIGNATION, REMOVAL, AND SUCCESSION OF TRUSTEE

5.1 Removal of Trustee: The District may remove any Trustee appointed by the District at any time by delivery to such Trustee, and to the other Trustees then acting, an instrument signed by the District. Likewise, the Association may remove any Trustee appointed by the Association at any time by delivery to such Trustee and to the other Trustees then acting, an instrument signed by the Association.

5.2 Resignation of Trustee: Any Trustee may resign, without the permission of any court or judge and without first accounting for his actions as Trustee, by giving written notice to the District, Association and to the other Trustees then acting, but the foregoing shall not relieve any Trustee so resigning of the obligation ultimately to account for his or her actions as such Trustee.

5.3 Appointment of Successor Trustees: In the event of the death, resignation or removal for any reason of any Trustee, a successor Trustee may be appointed by an instrument signed by the District or Association, accepted in writing by such successor Trustee, copies of which shall be delivered by the District or Association to the other Trustees then acting. The District shall appoint the successor of a District Trustee and the Association shall appoint the successor of an Association Trustee. No vacancy or vacancies in the position of Trustee shall impair the power of the remaining Trustees to act in the manner herein provided for the purpose of administering the affairs of this Trust.

5.4 Change In number of Trustees: The number of Trustees may be changed from time to time by the District and Association; provided, however, that the number thereof (except for temporary vacancy periods created by death, resignation or removal from office) shall not be less than three District Trustees and three Association Trustees.

6. AMENDMENT OR TERMINATION

6.1 Amendment: The District and Association shall have the right at any, time, and from time to time, to amend this Trust, in whole or in part, retroactively or otherwise. In no event shall any such amendment cause this Trust to be used for any purpose other than the payment of benefits to participants and their dependents and beneficiaries or permit the net earnings of the Fund to inure other than by payment of benefits, to the benefit of any private shareholder or individual.

6.2 Termination: This agreement and the Trust hereunder may be terminated at any time by the District, Association, or both, upon written notice delivered to the Trustees and the other party. Upon termination of the Trust for any reason, the Trustees shall make such distributions as they deem appropriate, after reserving from the assets of the Fund such amount as they reasonably shall deem necessary to provide for any sums chargeable against the Fund for which the Trustees may be liable, or for payment of expenses in connection with the settlement of their accounts or otherwise, except the assets of the Fund upon such termination shall be used solely for providing benefits to participants and their dependents and beneficiaries and no part of the net earnings of the Fund shall inure, other than by payment of benefits, to the benefit of any private shareholder or individual. The Trustees, upon receipt of any direction from the District and Association upon termination, shall be under no duty to inquire into the propriety or validity thereof.

6.3 Continuation of Powers and Duties of Trustees: From and after the date of the termination of the Trust and until the final distribution of the assets of the Fund, the Trustees shall continue to have all the powers and duties provided under this agreement which are necessary and expedient for the orderly liquidation and distribution of the assets of the Fund.

6.4 Duration of the Trust: Unless sooner terminated in accordance with section 6.2, this agreement and the Trust created hereby, shall continue for such time as the benefits hereunder are to be provided and as long thereafter as may be necessary for liquidation and distribution of the assets of the Fund.

7. MISCELLANEOUS

7.1 Accounting Period: The annual accounting period for the Trust shall be the twelve month period commencing July 1 and ending June 30.

7.2 Applicable Law: This agreement shall be construed in accordance with applicable federal law and, to the extent otherwise applicable, the laws of the State of Washington.

7.3 Benefits Not Assignable: The Trust and the benefits provided through or by the Trust are for the personal protection of the covered employees and their dependents and beneficiaries. No vested or unvested interest of any covered employee, dependent or beneficiary may be assigned, seized by legal process, transferred or subjected to the claims of creditors in any way.

7.4 Nondiscrimination: The Trustees shall, to the fullest extent possible, treat alike all persons who are similarly situated.

IN WITNESS WHEREOF, the parties hereto have executed this agreement this ___ day of _____, 2005.

EVERETT SCHOOL DISTRICT	EVERETT EDUCATION ASSOCIATION
By:_____	By:_____
Its:_____	Its:_____
DISTRICT TRUSTEES	ASSOCIATION TRUSTEES
_____	_____
_____	_____
_____	_____

APPENDIX I

The terms conditions and limitations of the benefits described in 1.4 are contained in the written instruments listed from time to time in this Appendix I.

A. Insured medical benefits provided through the following insurance contract/policy:

1. Group Medical Coverage Agreement, Group Number 0026100, between Group Health Cooperative and the Trust.

B. Insured medical benefits provided by the following insurance carrier through Washington Education Association (the documents governing these benefits are the contracts between WEA and the below-listed insurance carrier):

1. Premera Blue Cross, Group Number 8000314-0001.

C. Insured dental benefits provided by the following insurance carriers through Washington Education Association (the documents governing these benefits are the contracts between WEA and the below-listed insurance carriers):

1. Washington Dental Service.
2. Willamette Dental Service.

D. Insured basic and voluntary term life and accidental death and dismemberment benefits provided through Metropolitan Life Insurance Company, Policy Number 74323-G.

E. Insured long term disability provided through Standard Insurance Company, Policy Number 135033-B.

F. Voluntary insured short term disability benefits provided through Standard Insurance Company, Policy Number 135033-A.

G. Voluntary insured long term care insurance provided by UNUM Life Insurance Company of America. Under this policy UNUM insures the employees of Everett School District (the Sponsoring Organization) under the Select Group Insurance Trust Policy Number 292000.

H. Employee assistance benefits provided through Magellan Behavioral Health, Inc., Customer Number ESEB00-01.

I. Wellness program benefits offered pursuant to the Wellness Program described in Trust Policy 470 of the Everett School Employee Benefit Trust Operations Manual for Trustees.

Revised: April 30, 2012

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."

Everett Public Schools

Human Resources Department
3715 Oakes Avenue
Everett, WA 98201
Telephone: (425) 388-4716

April 14, 2003

MEMORANDUM

To: All Employees of the Everett Public Schools

From: Molly Ringo
Executive Director of Human Resources

Re: **Health Insurance Portability and Accountability Act (HIPAA)**

The Health Insurance Portability and Accountability Act (HIPAA) requires the District to establish rules to protect the privacy of health information. Although in the past we have taken great care to maintain confidentiality with individual health plan information, this will require us to modify some of our practices.

Because the Everett School Employee Benefit Trust offers a variety of health plans to our employees and the District functions as the Plan Administrator, we are required to create Policies and Procedures for compliance with the HIPAA Privacy Rule by April 14, 2003.

One of these requirements is the distribution of a detailed Privacy Notice. This Notice explains:

- ✓ How the Trust/District may use or disclose your health plan information;
- ✓ Your rights with respect to your health plan information; and the
- ✓ Complaint process

Please take a moment to read this information. We apologize for the lengthiness of the Notice.

Again, please be assured that we will continue to honor the confidentiality of your health plan information.

MR/kms

Attachment

EVERETT PUBLIC SCHOOLS - PRIVACY NOTICE

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposes numerous requirements on employer health plans concerning the use and disclosure of individual health information. This information, known as protected health information, includes virtually all individually identifiable health information held by the Plan — whether received in writing, in an electronic medium, or as an oral communication. This notice describes the privacy practices of the following plans: Preferred Provider Organizations/First Choice Health Network and Flexible Spending Accounts. The plans covered by this notice may share health information with each other to carry out Treatment, Payment, or Health Care Operations. These plans are collectively referred to as the Plan in this notice, unless specified otherwise.

The Plan's duties with respect to health information about you

The Plan is required by law to maintain the privacy of your health information and to provide you with this notice of the Plan's legal duties and privacy practices with respect to your health information. If you participate in an insured plan option, you will receive a notice directly from the Insurer. Different policies may apply to other Everett School Employee Benefit Trust programs or to data unrelated to the health plan.

How the Plan may use or disclosure your health information

The privacy rules generally allow the use and disclosure of your health information without your permission (known as an authorization) for purposes of health care Treatment, Payment activities, and Health Care Operations. Here are some examples of what that might entail:

- **Treatment** includes providing, coordinating, or managing health care by one (1) or more health care providers or doctors. Treatment can also include coordination or management of care between a provider and a third party, and consultation and referrals between providers. *For example, the Plan may share health information about you with physicians who are treating you.*

- **Payment** includes activities by this Plan, other plans, or providers to obtain premiums, make coverage determinations and provide reimbursement for health care. This can include eligibility determinations, reviewing services for medical necessity or appropriateness, utilization management activities, claims management, and billing; as well as "behind the scenes" plan functions such as risk adjustment, collection, or reinsurance. *For example, the Plan may share information about your coverage or the expenses you have incurred with another health plan in order to coordinate payment of benefits.*

- **Health care operations** include activities by this Plan (and in limited circumstances other plans or providers) such as wellness and risk assessment programs, quality assessment and improvement activities, customer service, and internal grievance resolution. Health care operations also include vendor evaluations, credentialing, training, accreditation activities, underwriting, premium rating, arranging for medical review and audit activities, and business planning and development. *For example, the Plan may use information about your claims to review the effectiveness of wellness programs.*

The amount of health information used or disclosed will be limited to the "Minimum Necessary" for these purposes, as defined under the HIPAA rules. The Plan may also contact you to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you.

How the Plan may share your health information with Everett School Employee Benefit Trust

The Plan, or its health insurer or HMO, may disclose your health information without your written authorization to Everett School Employee Benefit Trust for plan administration purposes. Everett School Employee Benefit Trust may need your health information to administer benefits under the Plan. Everett School Employee Benefit Trust agrees not to use or disclose your health information other than as permitted or required by the Plan documents and by law. Human Resources administrators and benefits staff and Payroll staff are the only Everett School Employee Benefit Trust employees who will have access to your health information for plan administration functions.

Here's how additional information may be shared between the Plan and Everett School Employee Benefit Trust, as allowed under the HIPAA rules:

- The Plan, or its Insurer or HMO, may disclose "summary health information" to Everett School Employee Benefit Trust if requested, for purposes of obtaining premium bids to provide coverage under the Plan, or for modifying, amending, or terminating the Plan. Summary health information is information that summarizes participants' claims information, but from which names and other identifying information have been removed.

- The Plan, or its Insurer or HMO, may disclose to Everett School Employee Benefit Trust information on whether an individual is participating in the Plan, or has enrolled or disenrolled in an insurance option or HMO offered by the Plan.

In addition, you should know that Everett School Employee Benefit Trust cannot and will not use health information obtained from the Plan for any employment-related actions. However, health information collected by Everett School Employee Benefit Trust from other sources, for example under the Family and Medical Leave Act, Americans with Disabilities Act, or workers' compensation is *not* protected under HIPAA (although this type of information may be protected under other federal or state laws).

Other allowable uses or disclosures of your health information

In certain cases, your health information can be disclosed without authorization to a family member, close friend, or other person you identify who is involved in your care or payment for your care. Information describing your location, general condition, or death may be provided to a similar person (or to a public or private entity authorized to assist in disaster relief efforts). You'll generally be given the chance to agree or object to these disclosures (although exceptions may be made, for example if you're not present or if you're incapacitated). In addition, your health information may be disclosed without authorization to your legal representative.

The Plan also is allowed to use or disclose your health information without your written authorization for the following activities:

Workers' compensation	Disclosures to workers' compensation or similar legal programs that provide benefits for work-related injuries or illness without regard to fault, as authorized by and necessary to comply with such laws
Necessary to prevent serious threat to health or safety	Disclosures made in the good-faith belief that releasing your health information is necessary to prevent or lessen a serious and imminent threat to public or personal health or safety, if made to someone reasonably able to prevent or lessen the threat (including disclosures to the target of the threat); includes disclosures to assist law enforcement officials in identifying or apprehending an individual because the individual has made a statement admitting participation in a violent crime that the Plan reasonably believes may have caused serious physical harm to a victim, or where it appears the individual has escaped from prison or from lawful custody
Public health activities	Disclosures authorized by law to persons who may be at risk of contracting or spreading a disease or condition; disclosures to public health authorities to prevent or control disease or report child abuse or neglect; and disclosures to the Food and Drug Administration to collect or report adverse events or product defects
Victims of abuse, neglect, or domestic violence	Disclosures to government authorities, including social services or protected services agencies authorized by law to receive reports of abuse, neglect, or domestic violence, as required by law or if you agree or the Plan believes that disclosure is necessary to prevent serious harm to you or potential victims (you'll be notified of the Plan's disclosure if informing you won't put you at further risk)

Judicial and administrative proceedings	Disclosures in response to a court or administrative order, subpoena, discovery request, or other lawful process (the Plan may be required to notify you of the request, or receive satisfactory assurance from the party seeking your health information that efforts were made to notify you or to obtain a qualified protective order concerning the information)
Law enforcement purposes	Disclosures to law enforcement officials required by law or pursuant to legal process, or to identify a suspect, fugitive, witness, or missing person; disclosures about a crime victim if you agree or if disclosure is necessary for immediate law enforcement activity; disclosure about a death that may have resulted from criminal conduct; and disclosure to provide evidence of criminal conduct on the Plan's premises
Decedents	Disclosures to a coroner or medical examiner to identify the deceased or determine cause of death; and to funeral directors to carry out their duties
Organ, eye, or tissue donation	Disclosures to organ procurement organizations or other entities to facilitate organ, eye, or tissue donation and transplantation after death
Research purposes	Disclosures subject to approval by institutional or private privacy review boards, and subject to certain assurances and representations by researchers regarding necessity of using your health information and treatment of the information during a research project
Health oversight activities	Disclosures to health agencies for activities authorized by law (audits, inspections, investigations, or licensing actions) for oversight of the health care system, government benefits programs for which health information is relevant to beneficiary eligibility, and compliance with regulatory programs or civil rights laws
Specialized government functions	Disclosures about individuals who are Armed Forces personnel or foreign military personnel under appropriate military command; disclosures to authorized federal officials for national security or intelligence activities; and disclosures to correctional facilities or custodial law enforcement officials about inmates
HHS investigations	Disclosures of your health information to the Department of Health and Human Services (HHS) to investigate or determine the Plan's compliance with the HIPAA privacy rule

Except as described in this notice, other uses and disclosures will be made only with your written authorization. You may revoke your authorization as allowed under the HIPAA rules. However, you can't revoke your authorization if the Plan has taken action relying on it. In other words, you can't revoke your authorization with respect to disclosures the Plan has already made.

Your individual rights

You have the following rights with respect to your health information the Plan maintains. These rights are subject to certain limitations, as discussed below. This section of the notice describes how you may exercise each individual right. See the table at the end of this notice for information on how to submit requests.

Right to request restrictions on certain uses and disclosures of your health information and the Plan's right to refuse

You have the right to ask the Plan to restrict the use and disclosure of your health information for Treatment, Payment, or Health Care Operations, except for uses or disclosures required by law. You have the right to ask the Plan to restrict the use and disclosure of your health information to family members, close friends, or other persons you identify as being involved in your care or payment for your care. You also have the right to ask the Plan to restrict use and disclosure of health information to notify those persons of your location, general condition, or death — or to coordinate those efforts with entities assisting in disaster relief efforts. If you want to exercise this right, your request to the Plan must be in writing.

The Plan is not required to agree to a requested restriction. And if the Plan does agree, a restriction may later be terminated by your written request, by agreement between you and the Plan (including an oral agreement), or unilaterally by the Plan for health information created or received after you're notified that the Plan has removed the restrictions. The Plan may also disclose health information about you if you need emergency treatment, even if the Plan has agreed to a restriction.

Right to receive confidential communications of your health information

If you think that disclosure of your health information by the usual means could endanger you in some way, the Plan will accommodate reasonable requests to receive communications of health information from the Plan by alternative means or at alternative locations.

If you want to exercise this right, your request to the Plan must be in writing and you must include a statement that disclosure of all or part of the information could endanger you.

Right to inspect and copy your health information

With certain exceptions, you have the right to inspect or obtain a copy of your health information in a "Designated Record Set." This may include medical and billing records maintained for a health care provider; enrollment, payment, claims adjudication, and case or medical management record systems maintained by a plan; or a group of records the Plan uses to make decisions about individuals. However, you do not have a right to inspect or obtain copies of psychotherapy notes or information compiled for civil, criminal, or administrative proceedings. In addition, the Plan may deny your right to access, although in certain circumstances you may request a review of the denial.

If you want to exercise this right, your request to the Plan must be in writing Within 30 days of receipt of your request (60 days if the health information is not accessible onsite), the Plan will provide you with:

- The access or copies you requested;
- A written denial that explains why your request was denied and any rights you may have to have the denial reviewed or file a complaint; or
- A written statement that the time period for reviewing your request will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Plan expects to address your request.

The Plan may provide you with a summary or explanation of the information instead of access to or copies of your health information, if you agree in advance and pay any applicable fees. The Plan also may charge reasonable fees for copies or postage.

If the Plan doesn't maintain the health information but knows where it is maintained, you will be informed of where to direct your request.

Right to amend your health information that is inaccurate or incomplete

With certain exceptions, you have a right to request that the Plan amend your health information in a Designated Record Set. The Plan may deny your request for a number of reasons. For example, your request may be denied if the health information is accurate and complete, was not created by the Plan (unless the person or entity that created the information is no longer available), is not part of the Designated Record Set, or is not available for inspection (e.g., psychotherapy notes or information compiled for civil, criminal, or administrative proceedings).

If you want to exercise this right, your request to the Plan must be in writing, and you must include a statement to support the requested amendment. Within 60 days of receipt of your request, the Plan will:

- Make the amendment as requested;

- Provide a written denial that explains why your request was denied and any rights you may have to disagree or file a complaint; or
- Provide a written statement that the time period for reviewing your request will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Plan expects to address your request.

Right to receive an accounting of disclosures of your health information

You have the right to a list of certain disclosures the Plan has made of your health information. This is often referred to as an "accounting of disclosures." You generally may receive an accounting of disclosures if the disclosure is required by law, in connection with public health activities, or in similar situations listed in the table earlier in this notice, unless otherwise indicated below.

You may receive information on disclosures of your health information going back for six (6) years from the date of your request, but not earlier than April 14, 2003 (the general date that the HIPAA privacy rules are effective). You do not have a right to receive an accounting of any disclosures made:

- For Treatment, Payment, or Health Care Operations;
- To you about your own health information;
- Incidental to other permitted or required disclosures;
- Where authorization was provided;
- To family members or friends involved in your care (where disclosure is permitted without authorization);
- For national security or intelligence purposes or to correctional institutions or law enforcement officials in certain circumstances; or
- As part of a "limited data set" (health information that excludes certain identifying information).

In addition, your right to an accounting of disclosures to a health oversight agency or law enforcement official may be suspended at the request of the agency or official. If you want to exercise this right, your request to the Plan must be in writing. Within 60 days of the request, the Plan will provide you with the list of disclosures or a written statement that the time period for providing this list will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Plan expects to address your request. You may make one (1) request in any 12-month period at no cost to you, but the Plan may charge a fee for subsequent requests. You'll be notified of the fee in advance and have the opportunity to change or revoke your request.

Right to obtain a paper copy of this notice from the Plan upon request

You have the right to obtain a paper copy of this Privacy Notice upon request. Even individuals who agreed to receive this notice electronically may request a paper copy at any time.

Changes to the information in this notice

The Plan must abide by the terms of the Privacy Notice currently in effect. This notice takes effect on April 14, 2003. However, the Plan reserves the right to change the terms of its privacy policies as described in this notice at any time, and to make new provisions effective for all health information that the Plan maintains. This includes health information that was previously created or received, not just health information created or received after the policy is changed. If changes are made to the Plan's privacy policies described in this notice, you will be provided with a revised Privacy Notice via in-District mail or U.S. Mail.

Complaints

If you believe your privacy rights have been violated, you may complain to the Plan and to the Secretary of Health and Human Services. You won't be retaliated against for filing a complaint. To file a complaint, obtain a Complaint Form from the Complaint Manager by calling the Human Resources – Benefits Department at (425) 388-4710.

Contact

For more information on the Plan's privacy policies or your rights under HIPAA, contact Human Resources – Benefits Department at (425) 388-4710.

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)

4. Uses and Disclosures

4.01 Overview

4.02 Enrollment, Premium Bids, Amendment/Termination Activities

4.03 Treatment, Payment, and Health Care Operations

4.04 When Authorizations Are Needed

4.05 Disclosure to Participants, Beneficiaries, and Others Acting on Their Behalf

4.06 Use and Disclosure of De-Identified Information and Limited Data Sets

4.01 Overview

This Section 4.01 summarizes limits imposed by the HIPAA Privacy Rule on the Plan's uses and disclosures of PHI. Sections 4.02 through 4.06 describe Procedures the Plan's Administrator maintains to satisfy the standards when it uses PHI on behalf of the Plan. Insurers and Business Associates will also adopt procedures to meet those standards, and Business Associates will act as described in their Business Associate Agreement (see Section 7.05).

In general, a Participant's PHI can be used or disclosed for a variety of Plan administrative activities. Common examples include paying claims, resolving appeals, managing specialty vendors and helping Participants address problems. The HIPAA Privacy Rule does not prohibit these activities, but it imposes the following guidelines:

Uses and disclosures generally allowed without Authorization. A person's PHI can be used or disclosed without obtaining that person's Authorization as follows:

- If disclosed to the Plan's Administrator for enrollment activities and (where only summary health information is used) for premium bids and Plan Amendment/ termination activities;
- If requested by a Health Care Provider for Treatment;
- If needed for Payment activities such as claims, appeals, and bill collection;
- If needed for Health Care Operations such as audits and wellness and risk assessment programs;
- If disclosed to the Participant, and in certain circumstances, to family members and others acting on the Participant's behalf; and
- If required by law, in connection with public health activities, or in similar situations as listed in Section 10.10.

Details on the types of activities that constitute permissible Treatment, Payment, and Health Care Operations are included in Section 8. In some cases, the Plan will want to use or disclose PHI for other purposes, in which case Authorization will be required. In addition, except in certain limited circumstances, Authorization is required for the use and disclosure of Psychotherapy Notes and for the use and disclosure of PHI for Marketing.

Information is limited to the "Minimum Necessary." The Plan must limit uses and disclosures of PHI to the Minimum Necessary to accomplish the intended purpose. This requirement does not apply to:

- Uses or disclosures for Treatment purposes;
- Disclosures to the Department of Health and Human Services (HHS) for audits of the Plan's compliance with the HIPAA Privacy Rule;
- Disclosures to an individual of his or her own PHI;
- Uses or disclosures required by law;
- Uses or disclosures made pursuant to an Authorization; and
- Uses or disclosures otherwise required for compliance with the HIPAA Privacy Rule.

De-identified Information. The limits in this Manual apply only to health information that is individually identifiable. If information is de-identified, it can then be used or disclosed without restriction. In addition, information that has most of its de-identifiers removed can be disclosed to a person signing a Data Use Agreement (see Section 4.06).

a. Citations

45 CFR § 164.502(b)
45 CFR § 164.502(d)
45 CFR § 164.508
45 CFR § 164.514

4.02 Enrollment, Premium Bids, Amendment/ Termination Activities

The Plan's Administrator will process Participant enrollment and disenrollment elections and transmit the elections to the Plan, its Insurers, and its Business Associates. The Plan, its Insurers and its Business Associates will, without obtaining a Participant's Authorization, disclose certain types of PHI (enrollment/disenrollment information and summary health information) to the Plan's Administrator (or its agents) in the following circumstances:

PHI disclosed	Employer uses of PHI
Enrollment and disenrollment information	• Enrollment and disenrollment activities, including processing of annual enrollment elections, payroll processing of elected Participant contribution amounts, new-hire elections, enrollment changes, and responding to Participant questions related to eligibility for Plan enrollment.
Summary health information (see table below)	• To obtain premium bids for health insurance coverage under the Plan (if the Plan's Administrator requests the information). • To modify, amend, or terminate the Plan (if the Plan's Administrator requests the information).

Required deletions for Summary Health Information

Summary health information is information that summarizes claims history, expenses, or types of claims of individuals receiving benefits under the Plan from which the following information has been deleted.

- Names;
- Social Security numbers;
- Full face photographic and any comparable images;
- Telephone numbers;
- Specific dates such as dates of birth and death, and admission/discharge dates. *The Plan can use the year of the event, except for the birth year of persons over age eighty-nine (89)*
- Vehicle identifiers (serial number or license plate number);
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Fax numbers;
- E-mail address;
- Medical record number;
- Any other unique identifying numbers, or characteristics, or codes, including a particular subsidiaries, divisions, or work locations
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Internet Protocol (IP) address numbers;
- Biometric identifiers (e.g., finger, iris, or voice prints); and
- Geographic identifiers smaller than a state, including street address, city, county, and precinct; but the five (5)-digit zip code may be used.

a. Citations

45 CFR § 164.504(f)(1)

4.03 Treatment, Payment, and Health Care Operations

The HIPAA Privacy Rule permits the Plan's Administrator to receive PHI from the Plan without Authorization only after the Plan's Administrator has amended the Plan and certified that it will limit uses and disclosures of PHI to Plan administrative activities and will otherwise protect PHI as required by the law. The Plan's certification and Amendment are in Sections 7.03 and 7.04. This Section 4.03 describes the Plan's Administrator procedures for using or disclosing PHI for Plan administrative activities without Authorization. In general, the Plan's Administrator will:

- Identify the classes of employees with access to PHI and the categories of information they will use;
- Make reasonable efforts to limit disclosures of and requests for PHI to the Minimum Necessary to accomplish the intended purpose;
- Maintain procedures governing the storage of PHI; and
- If feasible, return or destroy PHI received from the Plan, and maintain procedures governing the retention and destruction of PHI not returned or destroyed.

Procedures governing disclosures and requests made on a routine and recurring basis are described in the following charts. For other disclosures and requests, the Plan's Administrator will review each situation on an individual basis by considering the importance of the request or disclosure; the costs of limiting the request or disclosure; and any other factors the Plan's Administrator believes to be relevant. Any uses or disclosures of PHI not included in these tables but permitted to be made without Authorization in the Notice of Privacy Practices (see Section 7.02) should be made upon consultation with the Privacy Official if feasible.

a. Appeals of Adverse Benefit Determinations

The Board of Trustees process final appeals to adverse benefit determinations for the self funded plans. Process includes collecting information relevant to benefit determination; review and analysis by the Board of Trustees; documenting decision; corresponding with Participant to apprise them of status and final determination; communicating with Business Associates as appropriate. This is a Payment activity.	
The Plan's Administrator staff permitted access to PHI	• Board of Trustees. • HR employees with responsibility for investigating appeals and recommending decisions to the Committee.
Parties to whom disclosures are permitted	• Participant who is the subject of the appeal, and associated individuals as permitted by Section 4.05. • Health care providers involved with treating the Participant. • Business Associates involved in the initial benefit determination. • Business Associates (including health care professionals) assisting with review and analysis of the benefit determination and appeal.
Categories of PHI	• Information relating to appeals, including: – copies of the denial letter. – documents submitted by the claimant, health care providers, etc. – benefit determinations of Participants receiving similar services. – documents/communications from the Plan's Administrator.
Protocols for meeting Minimum Necessary requirement	• Information received from the Plan will be de-identified (e.g., name and location removed) to the extent possible by Business Associates or, by HR employees before the claim is reviewed by the Board of Trustees.
Storage of PHI	• Paper records will be maintained in the HR file room and clearly labeled "Plan Appeals." • Electronic records will be retained on the HR file server. • Information will be protected using the procedures in Section 3.02.
Retention/ Destruction	• No redundant copies will be retained. • PHI will be destroyed six years after creation.

b. Customer Service

The Plan's Administrator will assist Participants with various eligibility and claims questions. Questions related solely to enrollment and disenrollment will be processed in accordance with Section 4.02. Process involves intake of questions from Participants, collecting information relevant to question; documenting decision; communicating with Participant to apprise them of status and resolution; communicating with Business Associates and Insurers as appropriate. This is a Payment activity.	
Individuals permitted access to PHI	• The Plan's Administrator is responsible for investigating questions and recommending decisions.
Parties to whom disclosures are permitted	• Participant who is the subject of a question, and associated individuals as permitted by Section 4.05. • Health care providers involved with treating the Participant. • Business Associates and Insurers involved in benefit determinations. • Business Associates Insurers assisting with review and analysis of benefit determinations.
Categories of PHI	• All PHI relevant to the claim.
Protocols for meeting Minimum Necessary requirement	• The Plan's Administrator will disclose only PHI that, in their judgment, is directly relevant to the resolution of the question. • Questions about the scope of requested disclosures should be directed to the Privacy Official.
Storage of PHI	• Paper records will be maintained in the HR file room and clearly labeled "Customer Service." • Electronic records will be retained on the HR file server. • Information will be protected using the procedures in Section 3.02.
Retention/ Destruction	• No redundant copies will be retained. • PHI will be destroyed six years after creation.

c. Data Analysis

The Plan's Administrator will perform plan auditing, rate setting and benefits planning and analysis using claims and appeals information obtained from Business Associates and Insurers. Business Associates perform claim data collection and warehousing services and provide quarterly reports to the Plan for the purpose of performing trending, forecasting, and cost calculations. These are both Health Care Operations activities and Payment activities.	
Individuals	• The Plan's Administrator is responsible for Plan management

permitted access to PHI	and quality assessment activities.
Parties to whom disclosures are permitted	• Business Associates involved in data aggregation. • Business Associates assisting with review and analysis of data.
Categories of PHI	• All claims data related to Participants, but excluding any physician notes and underlying claim records.
Protocols for meeting Minimum Necessary requirement	• Business Associate will remove obvious identifiers (e.g., name, location, ID number) before providing PHI to the Plan.
Storage of PHI	• Paper records will be maintained in the HR file room and clearly labeled "Data Analysis." • Electronic records will be retained on the HR file server. • Information will be protected using the procedures in Section 3.02.
Retention/ Destruction	• No redundant copies will be retained. • PHI will be destroyed six years after creation.

d. Citations

45 CFR § 164.506

4.04 When Authorizations are Needed

The Plan's Administrator will obtain a Participant's Authorization for any use or disclosure of PHI not identified in Section 4.01, including any uses for employment-related or non-Plan-related purposes.

PHI will not be used or disclosed on the basis of an Authorization, unless it is verified that the Authorization:

- Has not expired;
- Has not been revoked; and
- Includes all required information.

The requirements for Authorizations are described in Section 7.06.

A copy of each Authorization will be retained for six (6) years from the later of the date the Authorization was created or the last date the Authorization was effective.

a. Citations

45 CFR § 164.508

4.05 Disclosure to Participants, Beneficiaries, and Others Acting on Their Behalf

This Section 4.05 describes the Plans procedure for disclosing PHI to Participants, their personal representatives, and family members and others acting on their behalf. Insurers and Business Associates may adopt similar procedures for the PHI they use or disclose for the Plan. Before disclosing any PHI, the Plan's Administrator will verify the identity of the person requesting the information (see Section 3.03).

a. Participants

A Participant's own PHI may be disclosed to the Participant without Authorization.

b. Personal Representatives

A personal representative will be treated as the Participant and the Participant's PHI may be disclosed to the personal representative without Authorization. The Plan's Administrator will make reasonable efforts to limit disclosures with respect to PHI to the information relevant to such personal representation. A person will be treated as a personal representative in accordance with the following table and applicable state law. However, see the discussion following this table for important restrictions on personal representative status.

Participant	Person requesting PHI	Personal representative?
Minor child	Parent or guardian*	Yes, but must provide proof of relationship.
Adult child	Parent or guardian	Yes, but only upon proof of legal authority (e.g., court order) or voluntary agreement (e.g., power of attorney).
Adult	Spouse or other adult	Yes, but only upon proof of legal authority (e.g., court order) or voluntary agreement (e.g., power of attorney).
Deceased	Executor or Administrator	Yes, but only upon proof of legal authority (e.g., provisions of a will or power of attorney).

*This includes a person with the legal authority to make health care decisions.

Restrictions Regarding Minor Children

The Plan generally will treat the parent (or guardian or other person acting in the place of a parent) of a minor child as the child's personal representative, in accordance with applicable state law. However, the parent will not be treated as the personal representative for PHI related to health care services received by the minor if:

- The minor lawfully obtained the services 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 services and state law does not require the consent of anyone else; or
- The parent consents to a confidentiality agreement between the health care provider and the minor with respect to the services.

If a parent is not treated as a minor child's personal representative for a particular service, the parent may still receive access to the child's PHI under the individual right to inspect and copy PHI (Section 5.02) if the decision to provide access is made by a licensed health care professional, in the exercise of his or her professional judgment, and the decision is consistent with state law.

Restrictions Regarding Abuse or Endangerment

The Plans may elect not to treat a person as a Participant's personal representative if, in the exercise of professional judgment, the Plans decide that it is not in the best interest of the Participant because of a reasonable belief that:

- The Participant 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 Participant.

A Participant may request that the Plan limit communications with a personal representative by submitting a request for Confidential Communications (see Section 5.05).

c. Others Acting on a Participant's Behalf

The HIPAA Privacy Rule provides discretion to disclose a Participant's PHI to any individual without Authorization if necessary for Payment or Health Care Operations. This can include disclosures of a Participant's PHI to the Participant's family members. In making these

disclosures, the Plan's Administrator will make reasonable efforts to limit disclosures to the Minimum Necessary to accomplish the intended purpose. *(State law could limit these disclosures.)*

In certain additional cases, PHI can be disclosed without Authorization to a Participant's family members, friends, and others who are not personal representatives, if any of the following conditions applies:

- Information describing the Participant's location, general condition, or death is provided to a family member or other person responsible for the Participant's care (including PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts);
- PHI is disclosed to a family member, close friend or other person identified by the Participant who is involved in the Participant's care or Payment for that care, and the Participant had the opportunity to agree or object to the disclosure; or
- PHI is disclosed to a family member or friends involved in the Participant's care and it is impossible (due to incapacity or emergency) to obtain the Participant's agreement.

d. Citations

45 CFR § 164.502(g)
45 CFR § 164.510

4.06 Use and Disclosure of De-Identified Information and Data Use Agreements

Health information can be used without complying with the limits in this Manual if names, Social Security numbers and other data are removed so there is no reasonable basis to believe it can be used to identify a person. A Plan may choose to de-identify PHI and then use it without written Authorization from the persons to whom it pertains. A Plan can also remove most identifying data and disclose it without Authorization for selected purposes if the recipient agrees to protect the data through a Data Use Agreement.

Insurers and Business Associates acting on behalf of the Plan will adopt procedures for applying these De-identification rules and entering into Data Use Agreements. The Plans' procedures are described in this Section.

a. De-Identified Information

To de-identify Plan information, the specific data in the following list will be removed. However, if the Plan's Administrator knows that the information could still be used to identify a person, it will be protected as PHI.

- Names;
- Social Security number;
- Specific dates such as dates of birth and death, and admission/discharge dates. *The Plan can use the year of the event, except for the birth years of persons over age eighty-nine (89);*
- Telephone numbers;
- Fax numbers;
- E-mail addresses;
- Medical record numbers;
- Health plan beneficiary number;
- Geographic identifiers smaller than a state, including street address, city, county, precinct, and zip code. *The first three (3) numbers of the zip code can be used if more than 20,000 people are in any combination of zip codes with the same first three (3) numbers;*
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers (serial numbers or license plate numbers);
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers (e.g., finger, iris, or voice prints);
- Full-face photographic and any comparable images; and
- Any other unique identifying numbers or characteristics or codes, including a particular subsidiaries, divisions or work locations.

The Plan can retain a code (or other method) for re-identifying a person's information in the future, if the identification mechanism will not be used or disclosed and cannot be translated so as to identify the person. If the health information is re-identified, the Plan will treat it as PHI subject to this Manual.

As an alternative to removing all the items above, a case-by-case decision can be made about how much data needs to be removed in order to de-identify information. To do so, a written statement and analysis must be obtained from an appropriate expert in statistics and information de-identification. The statement must conclude that the risk is very small the information could be used (alone or in combination with other information) to identify an individual.

b. Data Use Agreements

In limited circumstances, PHI may be disclosed without Authorization under a data use agreement. This type of disclosure is permitted upon receipt of a request for health information needed for research purposes or public health activities, if the request fails to meet the requirements in Section 10.10. The same procedures can be used to disclose PHI without Authorization for certain types of Health Care Operations not specifically described in Section 8.

For example, a data use agreement may be used to disclose information for research that has not been approved by a review board; for public health activities undertaken by private organizations instead of public health authorities; and for Health Care Operations by providers or other health plans that do not have a prior or current relationship with the subject of the PHI.

To disclose PHI without Authorization in these circumstances, the Plan must:

- Create a "limited data set" by removing most of the identifying data listed in the table in Section 4.06(a). If all of the data is removed, the information is de-identified and can be used or disclosed without restriction. Key dates (birth date, admission/discharge date, date of death) and certain geographic information, such as city and zip code, may be retained; and

- Receive assurances from the recipient of the data that it will protect the information through a data use agreement. The agreement must establish the permitted uses and disclosures of the information, limit who can use or receive it, and promise that the recipient will safeguard the information.

The Plan's Administrator will review each request for disclosure of information that may qualify for data use agreements on an individual basis, in consultation with the Privacy Official, to determine whether the requirements in the HIPAA Privacy Rule are satisfied.

c. Citations

45 CFR § 164.514
45 CFR § 164.502(d)

5. Individual Rights

5.01 Overview

The HIPAA Privacy Rule provides individuals with certain rights associated with their PHI that the Plan (and all other Covered Entities) must follow. These include the rights to:

- Access, inspect, and copy certain PHI within a Designated Record Set (see Section 5.02);
- Request the Amendment of their PHI in a Designated Record Set (see Section 5.03);
- Request restriction of the use and disclosure of their PHI (see Section 5.04);
- Request the use of alternative means or alternative locations for receiving communications of their PHI (see Section 5.05); and
- Request an accounting of PHI disclosures (see Section 5.06).

Section 10.03 identifies the contact persons for processing Participants' requests to exercise these rights.

5.02 Inspect and Copy PHI

a. Participant's Right

A Participant has the right to access, inspect, and copy his or her PHI within a Designated Record Set for as long as the PHI is maintained in the Designated Record Set. The Plan must generally honor these rights, except in certain circumstances the Plan may deny the right to access. The Plan may provide a summary or explanation of the PHI instead of access or copies, if the Participant agrees in advance and pays any applicable fees.

A Designated Record Set is a group of records that the Plan maintains for enrollment, Payment, claims adjudication, case management or medical management, or that the Plan uses, in whole or in part, to make decisions about Participants. The Plan will require Business Associates to identify Designated Record Sets that they maintain and to make them available for inspection and copying. The Plan's Administrator maintains the following Designated Record Sets, which are available to be inspected or copied:

- Participant Files;
- Trust Appeal Files; and
- Subrogation Files.

b. Processing a Request

The Plan is responsible for receiving and processing requests for access, inspection, and copying of PHI maintained in Designated Record Sets. The Plan has assigned this responsibility to Inspection Contact (see Section 10.03). If the Plan does not maintain the PHI that is the subject of the Participant's request but knows where it is maintained, Inspection Contact will inform the Participant where to direct his or her request. The Plan will develop procedures with Business Associates to coordinate the inspection of Designated Record Sets in the Business Associates' custody.

Requests for access, inspection, and copying of PHI must be submitted on the Request for Access Form (Section 10.08(a)) and sent to Inspection Contact.

Inspection Contact will determine whether to approve or deny the request to access, inspect, or copy the PHI, in consultation with the Privacy Official, as needed.

Inspection Contact will respond to a Participant's request within thirty (30) days of the receipt

of the request. If the requested PHI is maintained offsite, Inspection Contact will respond within sixty (60) days of the request. If Inspection Contact is unable to respond within this timeframe, he or she will send the Participant written notice that the time period for reviewing the request will be extended for no longer than thirty (30) more days, along with the reasons for the delay and the date by which Inspection Contact expects to address the request.

c. Accepting a Request to Access, Inspect, or Copy

If Inspection Contact accepts the request, a copy of Form 10.08(a) indicating that the request has been accepted will be sent to the Participant and access will be provided within the thirty/sixty (30/60) day timeframe. A fee will be charged to the Participant for copying and mailing, based on the actual cost. Form 10.08(a) will inform the Participant of the fees in advance, and give the Participant an opportunity to withdraw the request if he or she does not agree to the fees.

d. Denying a Request to Access, Inspect, or Copy (Where Participant has Right to Review)

If Inspection Contact denies the request, a copy of Form 10.08(a) indicating that the request has been denied will be sent to the Participant within the thirty/sixty (30/60) day timeframe. Form 10.08(a) will indicate whether the Participant has the right to a review of the denial.

The Participant has the right to have the denial reviewed if Inspection Contact denies access to PHI for any of the following reasons:

- A licensed health care professional determines that the access is reasonably likely to endanger the life or physical safety of the Participant or another person;
- The PHI contains information about another person and a licensed health care professional determines that the access is reasonably likely to cause substantial harm to the other person; or
- The request is made by a personal representative, and a licensed health care professional determines that providing access to the personal representative is reasonably likely to cause substantial harm to the Participant or another person.

If Inspection Contact denies access on the basis of the risk of harm identified by a licensed health care professional, the Participant has the right to have the denial reviewed by a different licensed health care professional. Inspection Contact will promptly refer a request for review to a licensed health care professional who did not participate in the original denial decision. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access. Inspection Contact will provide or deny access in accordance with

the determination of the reviewing official.

If Inspection Contact denies access to any PHI, the Plan will, to the extent possible, continue to provide access to other PHI for which there are no grounds to deny access.

e. Denying a Request to Access, Inspect, or Copy (Where Participant has NO Right to Review)

If Inspection Contact denies the request, a copy of Form 10.08(a) indicating that the request has been denied will be sent to the Participant within the thirty/sixty (30/60) day timeframe. The copy will indicate whether the Participant has the right to a review of the denial.

The Participant has no right to have a denial reviewed if Inspection Contact denies a request to access, inspect, or copy PHI, for any of the following reasons:

- The PHI is Psychotherapy Notes;
- The PHI was compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative proceedings;
- The Plan maintains that the PHI is also subject to the Privacy Act (5 U.S.C. § 552a), and the Privacy Act allows the denial of access;
- The Plan received the PHI from someone other than a health care provider under a promise of confidentiality, and providing access to the PHI would be reasonably likely to reveal the source; or
- The Plan has temporarily suspended access to PHI created for research involving Treatment, if the Participant agreed to the suspension of access when agreeing to participate in the research.

f. Form for Denial

If the request for access is denied, Inspection Contact will within the timeframes, provide a written denial (see Section 10.08(a)) to the Participant in plain language which contains:

- The basis for the denial;
- A statement of the individual's review rights, if any; and

- A description of how the individual may complain to the Plan, pursuant to the complaint procedure in Section 6.03, or to HHS.

g. Documenting Requests

All requests, acceptances, and denials of PHI will be documented and retained for a period of six (6) years.

h. Citations

45 CFR § 164.524

5.03 Amend PHI

a. Participant's Rights

A Participant has the right to request that the Plan amend his or her PHI in a Designated Record Set. The Plan must generally honor these rights, except in certain circumstances. When the Plan amends PHI, it must communicate the Amendment to other persons to whom it has disclosed the PHI as described in Section 5.03(c). The Plan will require Business Associates to make Designated Record Sets that they maintain available for Amendment requests.

b. Processing a Request

The Plan is responsible for receiving and processing requests for Amendments to PHI. The Plan has assigned this responsibility to Amendment Contact (see Section 10.03). Requests must be submitted on the Request to Amend Form (see Section 10.08(b)) and sent to Amendment Contact. The Plan will develop procedures with Business Associates to coordinate the right to request Amendment of Designated Record Sets in the Business Associates' custody.

Amendment Contact will respond to a Participant's request within sixty (60) days after receipt. If Amendment Contact is unable to respond within this timeframe, he or she will send the Participant written notice that the time period for reviewing the request will be extended for no longer than thirty (30) more days, along with the reasons for the delay and the date by which Amendment Contact expects to address the request.

c. Amending PHI and Notifying Others

If Amendment Contact accepts a request for Amendment, in whole or in part, a copy of Form 10.08(b) indicating that the request has been accepted will be sent to the Participant within the sixty (60) day time frame. Amendment Contact will amend the PHI appropriately, and make reasonable efforts to inform and provide the Amendment to:

- Persons identified by the Participant as having received the PHI that is to be amended; and
- Persons, including Business Associates, who the Plan knows have the PHI that is the subject of the Amendment and who may have relied, or could forseeably rely, on the information to the detriment of the Participant.

d. Denying an Amendment

If Amendment Contact denies the request for Amendment, in whole or in part, a copy of Form 10.08(b) indicating that the request was denied will be sent to the Participant within the sixty (60) day time frame. Amendment Contact may deny a request to amend a Participant's PHI if he or she determines that the PHI:

- Was not created by the Plan (unless the Participant provides a reasonable basis to believe that the creator of the PHI is no longer available to amend the PHI);
- Is not part of the Designated Record Set;
- Is not available for inspection under the HIPAA Privacy Rule; or
- Is accurate and complete.

If Amendment Contact denies the request, it will permit the Participant to submit a statement of disagreement and the basis for the disagreement, limited to five (5) pages. In response, Amendment Contact may provide a rebuttal statement and send a copy to the Participant.

Amendment Contact will attach to each Designated Record Set that is subject to the request a completed copy of Form 10.08(b) (including any attached disagreement statements and rebuttals) indicating the denial of the Amendment request.

When the Plan makes subsequent disclosures of the disputed PHI, a copy of Form 10.08(b) (or a summary of the information included on Form 10.08(b)) will be attached to the PHI disclosed in the following circumstances:

- When the Participant has submitted a statement of disagreement;
- When the Participant has so requested.

e. Documenting Requests

All requests, acceptances, denials, and supporting statements regarding Amendment of PHI will be documented and retained for a period of six (6) years.

f. Citations

45 CFR § 164.526

5.04 Restricted Use of PHI

a. Participant's Rights

A Participant has the right to request that the Plan restrict the use and disclosure of his or her PHI. The Plan is not required to agree to a restriction, but it must abide by an agreed to restriction except in certain circumstances. The Plan will require Business Associates to make PHI that they maintain available for restriction requests.

b. Processing a Request

The Plan is responsible for processing requests for restricted use of PHI. The Plan has assigned this responsibility to Restriction Contact (see Section 10.03). Requests must be submitted on the Request for Restricted Use Form (see Section 10.08(c)) and sent to Restriction Contact. The Plan will develop procedures with Business Associates to coordinate the restricted use of PHI in the Business Associates' custody.

Restriction Contact will not agree to any requests for restricted use of PHI. Restriction Contact will send a copy of Form 10.08(c) to the Participant. The Form will indicate that the request was denied.

c. Documenting Requests

All restricted use of PHI requests will be documented and retained for a period of six (6) years.

d. Citations

45 CFR § 164.522(a)

5.05 Confidential Communications

a. Participant's Rights

A Participant has the right to request that the Plan use alternative means or alternative locations to communicate PHI to the Participant. The Plan must accommodate reasonable requests if the Participant clearly states that the disclosure of the PHI by the usual means could endanger the Participant. The Plan will require Business Associates that maintain PHI to reasonably honor a Participant's request for alternative means or locations to communicate the PHI to the Participant.

b. Processing a Request

The Plan is responsible for receiving and processing requests for Confidential Communication of PHI. The Plan has assigned this responsibility to Communications Contact (see Section 10.03). Requests must be submitted on the Request for Confidential Communications Form (see Section 10.08(d)) and sent to Communications Contact. The Plan will develop procedures with Business Associates to coordinate the Confidential Communications of PHI in Business Associates' custody.

Communications Contact will determine whether to approve or deny the request on the basis of its reasonableness. Reasonableness will be determined on the basis of the administrative difficulty in complying with the request and in consultation with the Privacy Official, as needed. If the payment of benefits is affected by this request, the Plan may also deny this request unless the Participant contacts the Communications Contact to discuss alternative payment means.

Communications Contact will provide notice of the decision to approve or deny the request.

- If approved, a copy of Form 10.08(d) indicating that the request has been approved will be sent to the Participant and each Business Associate that has access to that Participant's PHI.

- If denied, a copy of Form 10.08(d) indicating that the request has been denied will be sent to the Participant.

c. Documenting Requests

All requests for Confidential Communication of PHI will be documented and retained for a period of six (6) years.

d. Citations

45 CFR § 164.522(b)

5.06 Accounting of Non-Routine Disclosures

a. Participant's Rights

A Participant has the right to request an accounting of PHI disclosures made under Section 10.10 and disclosures not otherwise permitted by Section 4. However, an accounting is not available to the Participant in circumstances involving:

- National security or intelligence purposes;
- Correctional institutions or law enforcement officials;
- Limited data sets; and
- Disclosures occurring before the compliance date for the Covered Entity.

The Participant can request that the accounting include disclosures made on or after the later of:

- April 14, 2003; or
- The date that is six (6) years prior to the date of the request.

The Plan will require Business Associates that maintain PHI to reasonably honor a Participant's request for accountings of PHI disclosures.

b. Processing a Request

The Plan is responsible for receiving and processing requests for an accounting of PHI disclosures. The Plan has assigned this responsibility to Disclosure Contact (see Section 10.03). Requests must be submitted on the Request for Accounting of Non-Routine Disclosures Form (see Section 10.08(e)) and sent to Disclosure Contact. The Participant must indicate whether the requested accounting is for disclosures made within the past six (6) years or some shorter time period. The Plan will develop procedures with Business Associates that maintain PHI to coordinate the requests for accounting of PHI disclosures.

Disclosure Contact generally will respond to a request for an accounting within sixty (60) days after receipt. If Disclosure Contact is unable to respond within this timeframe, he or she will send the Participant written notice that the time period for reviewing the request will be extended for no longer than thirty (30) more days, along with the reasons for the delay and the date by which Disclosure Contact expects to address the request.

Disclosure Contact will send a copy of Form 10.08(e) to the Participant, with the accounting of PHI disclosures attached.

Disclosure Contact will provide a Participant with one accounting in any twelve (12)-month period free of charge. A reasonable fee will be charged for subsequent accountings within the same twelve (12)-month period.

Disclosure Contact may temporarily suspend a Participant's right to receive an accounting of disclosures to:

- A health oversight agency for health oversight purposes; or
- A law enforcement official for law enforcement purposes,

if the agency or official informs Disclosure Contact or the Plan in writing that the accounting would be reasonably likely to impede the agency's activities, and if it indicates the time for which the suspension is required.

Disclosure Contact will suspend a Participant's right to receive an accounting of these disclosures for up to thirty (30) days upon an oral request from the agency or official.

c. Content of the Accounting

Disclosure Contact will include the following information in an accounting of PHI disclosures:

- Date of disclosure;
- Name (and address, if known) of person or entity that received the PHI;
- Brief description of the PHI disclosed; and
- An explanation of the purpose of the disclosure or a copy of the request for disclosure.

The HIPAA Privacy Rule permits an abbreviated accounting of multiple PHI disclosures made to the same person or entity for a single purpose, and of certain disclosures for research purposes. Disclosure Contact will consult with the Privacy Official in deciding to abbreviate an accounting of these types of disclosures.

d. Documenting Requests

All requests for accounting of PHI disclosures will be documented and retained for a period of six (6) years.

e. Citations

45 CFR § 164.528

6. Risk Management Activities

6.01 Overview

6.02 Training

6.03 Complaints

6.04 Sanctions

6.05 Mitigation

6.06 Document Retention

6.01 Overview

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

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

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

6.02 Training

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

a. When Training will Occur

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

b. Contents of Training

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

The following topics are to be covered in the training:

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

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

c. Documentation

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

The documentation of privacy training will include:

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

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

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

d. Citations

45 CFR § 164.530(b)

6.03 Complaints

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

a. Filing Complaints

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

b. Processing Complaints and Complaint Resolution

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

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

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

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

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

c. Documentation

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

d. Citations

45 CFR § 164.530(d)

6.04 Sanctions

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

a. Determining Sanctions

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

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

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

b. Documentation

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

c. Citations

45 CFR § 164.530(e)

6.05 Mitigation

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

a. Mitigation Steps

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

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

The Privacy Official will conduct the mitigation activities.

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

b. Citations

45 CFR § 164.530(f)

6.06 Document Retention

The Plan must retain copies of its Policies and Procedures and all communications that the HIPAA Privacy Rule requires to be in writing. The Plan must also retain records of actions or designations that the HIPAA Privacy Rule requires to be documented. Materials can be maintained in written or electronic form. They must be retained for six (6) years from the date of their creation or when they were last in effect (whichever is later).

Business Associates and Insurers will retain documents in their possession as required by the HIPAA Privacy Rule and Business Associate Agreements.

a. Document Retention Checklists

The following are checklists of materials that the Plan's Administrator will retain under this rule:

Documents	
☐ Privacy Policies and Procedures (this Manual)	☐ Documentation that training has been provided to employees
☐ Authorizations	☐ Information in Designated Record Set to which Participants and similar persons have access (see Section 5.02)
☐ Plan Amendments	
☐ Plan Amendment certifications	☐ Data Use Agreements (used in certain cases involving summary data disclosed for research, public health, or Health Care Operations purposes)
☐ Business Associate Agreements	
☐ Notices of Privacy Practices	

Key person identification	
☐ Name of Privacy Official	☐ Titles of persons or offices responsible for receiving and processing requests to amend PHI
☐ Name of contact person or office responsible for receiving complaints and providing additional privacy information	☐ Titles of persons or offices responsible for receiving and processing requests for an accounting of non-routine disclosures made without Authorization, such as disclosures legally required or made for public health, law enforcement, judicial, and similar purposes
☐ Titles of persons or offices responsible for receiving and processing requests for access to their PHI	

Other materials relating to particular actions by the Plan	
☐ Complaints about the HIPAA Privacy Rule or this Manual and their disposition, if any	☐ Description of PHI disclosed
☐ Documentation of sanctions applied to employees for not complying with the HIPAA Privacy Rule, if any	☐ Copy of disclosure requests (or if made orally, statements describing the disclosures' purpose)
☐ Notices that deny a person's access to PHI	☐ Court orders, grand jury subpoenas, etc., where disclosure is required by law
☐ Notices that delay a person's access to PHI	☐ Written statements in connection with disclosures needed for other judicial/administrative processes, where the disclosure is not mandated by court order
☐ Notices that explain whether the Plan will overturn a decision to deny a person access to PHI	☐ Institutional or privacy board approvals for research-related disclosures
☐ Notices that deny a person's request to amend PHI	☐ Copies of written accountings
☐ Notices that delay amendments to PHI	☐ Plan's notice terminating a restriction on uses or disclosures of PHI previously agreed to by the Plan
☐ Statements of persons disagreeing with the Plan's decision to deny a request to amend PHI and any rebuttals of the statements	☐ Person's agreement or request to
☐ Disclosures of PHI for which a person is entitled to an accounting	
☐ Written statements or other documentation in	

Other materials relating to particular actions by the Plan	
support of verifications made prior to disclosures ☐ Written statements by agencies or officials supporting suspension of an accounting of PHI disclosures (including oral statements documented by the Plan) ☐ Conclusion and supporting analysis from an expert that health information is de-identified	terminate a restriction on uses or disclosures of PHI previously agreed to by the Plan ☐ Other communications required by the Plan to be in writing, including requests for Confidential Communications

b. Citations

45 CFR § 164.530(j)

7. Required Legal Documents

7.01 Overview

7.02 Privacy Notice

7.03 Amendments to Plan Documents

7.04 Plan Sponsor Certifications

7.05 Business Associate Agreements

7.06 Authorization

7.01 Overview

The HIPAA Privacy Rule requires Covered Entities to use specific documents to accomplish certain tasks.

- A Privacy Notice describes the Plan's practices concerning its uses and disclosures of PHI and informs Participants of their rights and of the Plan's legal duties, with respect to PHI (see Section 7.02);
- An Amendment to the Plan document describes the Plan's permitted uses and disclosures of PHI (see Section 7.03);
- A plan sponsor certification certifies that the Plan Sponsor has adopted the Plan Amendment and agrees to the restrictions on the uses and disclosures of PHI (see Section 7.04);
- A Business Associate Agreement describes the permitted uses and disclosures of PHI by the Business Associate (see Section 7.05); and
- A Participant's Authorization permits the Plan to use and disclose the Participant's PHI for purposes not otherwise permitted or required by the HIPAA Privacy Rule (see Section 7.06).

7.02 Privacy Notice

The Plan's Administrator will provide a Privacy Notice in Section 10.07 to satisfy the notice obligation for the Plan's self-funded benefits. Each health insurance issuer or HMO will provide its own Privacy Notice to those Participants who receive insured Plan benefits, in accordance with the requirements of the HIPAA Privacy Rule.

a. Identifying the Recipients

The Plan's Administrator will provide the Privacy Notice (see Section 10.07) to Participants (including both active and former employees) who are covered under a self-funded Plan benefit, no later than April 14, 2003. The Plan's Administrator will not provide a separate Privacy Notice to spouses or dependents, except for qualified beneficiaries who made independent COBRA elections (e.g., following a divorce or the death of an employee). The Plan's Administrator will also provide the Privacy Notice to new enrollees under a self-funded Plan benefit at the time of enrollment.

In addition, the Plan's Administrator will provide the Privacy Notice to all Business Associates.

b. Distributing the Notice

The Plan's Administrator will provide the Privacy Notice by in-District mail or first-class mail.

The Plan's Administrator will prominently post the Privacy Notice on any web sites that it maintains that provide information about the Plan's services or benefits.

c. Revising the Notice

The Plan's Administrator will revise the Privacy Notice if its terms are affected by a change to the Plan's Policies and Procedures.

If the change is material (as determined by the Privacy Official), the Plan's Administrator will provide the revised Privacy Notice to Participants covered under a self-funded Plan benefit within sixty (60) days of the change. No material change will be implemented before the effective date of the revised Privacy Notice (except where required by law). In addition, the Plan's Administrator will promptly provide revised Privacy Notices to Business Associates and Everett School District employees and Board of Trustees who perform Plan functions.

d. Informing Participants of the Availability of the Notice

Once every three (3) years, the Plan's Administrator will inform all Participants of the Privacy Notice's availability and how to obtain a copy. The Plan's Administrator will send this reminder via in-District mail or first-class mail.

e. Documenting Notices

All Privacy Notices will be documented and retained for a period of six (6) years from the date of creation or when last in effect, whichever is later.

f. Citations

45 CFR § 164.520(d)

7.03 Amendment to Plan Documents

The HIPAA Privacy Rule permits the Plan to share PHI with the Plan's Administrator after the Board of Trustees has amended its Plan documents, as described. The Plan's Administrator must restrict its use of the PHI to Payment and Health Care Operations activities.

a. Required Plan Amendments

The Board of Trustees will amend its Plan Documents (see Section 10.06(a)) to include provisions that:

- Describe the Plan's Administrator permitted uses and disclosures of PHI;
- Provide that the Plan can disclose PHI to the Plan's Administrator only upon receipt of a written certification from the Board of Trustees that the Plan Documents have been amended to include specific restrictions on the use and disclosure of PHI and that the Board of Trustees have agreed to those restrictions; and
- Provide adequate firewalls, such as identifying the employees (by name or by function) who will have access to PHI, restricting access solely to the identified employees for Plan administration functions, and providing a mechanism for resolving issues of noncompliance.

b. Documenting Plan Amendments

The Plan's Administrator will retain the amended Plan Documents for a period of at least six (6) years from the date when last in effect.

c. Citations

45 CFR § 164.504(f)(2)

7.04 Plan Sponsor Certifications

The HIPAA Privacy Rule requires the Board of Trustees to certify to the Plan that it has amended the Plan document in order for the Plan to share PHI with the Plan's Administrator. The Plan will disclose PHI to the Plan's Administrator only after the Board of Trustees provides the Plan with that written certification.

a. Written Certification Requirements

The Board of Trustees written certification (see Section 10.06(b)) provides that Everett School Employee Benefit Trust will take the following actions:

Required elements of the Board of Trustee's written certification

- Not use or further disclose PHI other than as permitted or required by the Plan documents or as required by law;
- Ensure that any subcontractors or agents to whom the Plan's Administrator provides PHI agree to the same restrictions;
- Not use or disclose the PHI for employment-related actions or in connection with any other benefit program of the Plan;
- Report to the Plan any use or disclosure of which the Plan's Administrator becomes aware that is inconsistent with the Plan documents or the HIPAA Privacy Rule;
- Make PHI accessible to individuals in accordance with Section 4.02;
- Allow individuals to amend their information in accordance with Section 4.03;
- Provide an accounting of its disclosures in accordance with Section 4.06;
- Make its practices available to HHS for determining compliance;
- Return and destroy all PHI when no longer needed, if feasible; and
- Ensure that adequate separation exists between the Plan's Administration activities and all other activities.

b. Documenting Certifications

All certifications will be retained for a period of six (6) years.

c. Citations

45 CFR § 164.504(f)(2)(ii)

7.05 Business Associate Agreements

The HIPAA Privacy Rule requires each Business Associate of the Plan to enter into a written contract (a Business Associate Agreement) with the Plan before the Plan can disclose PHI to it, except as indicated below. The Business Associate can use and disclose PHI only for the purposes provided in the Business Associate Agreement. A Business Associate not yet required to enter into a Business Associate Agreement must still comply with the HIPAA Privacy Rule. The Privacy Official will monitor how PHI maintained by the Business Associate is handled at the termination of the Business Associate Agreement and will, while the agreement is in force, act upon complaints of privacy violations and breaches.

a. Identifying Business Associates

The Plan's Administrator will determine which service providers are Business Associates. The log of Business Associate Agreements is at Section 10.04.

b. Signing Business Associate Agreements

The Plan will require each Business Associate to sign a Business Associate Agreement (see Section 10.04) or a contract that contains the required terms, as determined by the Privacy Official.

c. Timing of Business Associate Agreements

A Business Associate must sign a Business Associate Agreement no later than April 14, 2003, except as indicated below. After that date, the Plan will not disclose PHI to a Business Associate unless a Business Associate Agreement has been signed.

The Plan will have up to an additional year to enter into a Business Associate Agreement with a Business Associate if before, October 15, 2002, an existing written contract governed the arrangement and the Plan has not renewed or modified the contract before April 14, 2003. The deadline to amend such a contract is the earlier of the date the contract is amended or April 14, 2004.

The Plan will send a letter to each Business Associate whose contract is eligible for an extension of time, detailing the Business Associate's responsibilities to comply with the HIPAA Privacy Rule as of April 14, 2003.

d. Responsibilities of the Privacy Official

The Privacy Official will monitor the PHI that a Business Associate must return to the 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.

The Privacy Official will ensure that all complaints about privacy violations by a Business Associate are reviewed according to the Plan's procedures, as described in Section 6.03.

If the Privacy Official knows of acts or a pattern of activity by a Business Associate that are a material violation 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 the Plan's Administrator whether termination of the Business Associate Agreement is feasible. If not feasible (i.e., there are no viable business alternatives for the Plan), the Privacy Official will report the violation to HHS.

e. Documenting Business Associate Agreements

All Business Associate Agreements will be retained for a period of six (6) years from the date they were last in effect.

f. Citations

45 CFR § 164.502(e)(1)
45 CFR § 164.504(e)

7.06 Authorization

The HIPAA Privacy Rule requires the Plan to receive an Authorization from a Participant before using or disclosing PHI for purposes other than Treatment, Payment, Health Care Operations, or as otherwise permitted or required by the HIPAA Privacy Rule. The Plan may act on an Authorization only to the extent consistent with the terms of such Authorization.

a. Providing the Authorization Form to Participants

The Plan's Administrator will provide an Authorization Form (see Section 10.08(f)) to Participant who requests that his or her PHI be disclosed to a third party (other than a personal representative).

The Plan's Administrator will provide each Participant with an Authorization Form if the Plan's Administrator wants to use or disclose the Plan's PHI for a purpose that requires Authorization (see Section 4.04).

b. Signing of the Authorization Form

The signing of an Authorization Form is voluntary. Participants may refuse to authorize use of their PHI.

c. Receiving the Signed Authorization Form

The Plan must have a signed Authorization Form from the Participant, before it can take an action that requires Authorization.

d. Determining the Validity of Authorization

Before the use or disclosure of PHI, the Plan will confirm that the Authorization is valid by verifying that:

- The expiration date or event triggering expiration has not passed;
- The Authorization was filled out completely;
- The Authorization has not been revoked; and
- The Authorization Form contains all the required elements.

e. Revocation of Authorization

At any time, the Participant may revoke the Authorization, provided that a revocation will not be effective if the Authorization was relied on as described in the Form. Requests for revocation of Authorizations must be submitted in writing to Authorization Contact (see Section 10.03). The Plan will not act upon an Authorization that has been revoked.

f. Documentation Requirement

All Authorizations and revocations of Authorizations will be documented and retained for a period of six (6) years from the date the Authorization is created or when it last was in effect, whichever is later.

g. Citations

45 CFR § 164.508

8. Definitions

8.01 Definitions

Authorization: A person's permission to use PHI for purposes *other* than Treatment, Payment, or Health Care Operations, or as otherwise permitted or required by the HIPAA Privacy Rule (see Section 4). Authorizations require specific contents described in Section 7.06.

Business Associate: A person or entity that performs a function or activity regulated by HIPAA on behalf of the Plan and involving individually identifiable health information. Examples of such functions or activities are claims processing, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services. A Business Associate may be a Covered Entity. However, Insurers and HMOs are not Business Associates of the plans they insure. The HIPAA Privacy Rule requires that each Business Associate of the Plan enter into a written contract (Business Associate Agreement) with the Plan before the Plan can disclose PHI to it, as described in Section 7.05.

Covered Entity: A health plan (including an employer plan, Insurer, HMO, and government coverage such as Medicare); a health care provider (such as a doctor, hospital, or pharmacy) that electronically transmits any health information in connection with a transaction for which HHS has established an EDI (electronic data interchange) standard; and a health care clearinghouse (an entity that translates electronic information between nonstandard and HIPAA standard transactions).

De-identification: The removal of personal information (such as name, Social Security number, address) that could identify an individual. The HIPAA Privacy Rule lists eighteen (18) identifiers that must generally be stripped for data to meet the De-identification safe harbor described in Section 4.06.

Designated Record Set: A group of records that the Plan (or its Business Associate) maintains that relates to enrollment, Payment, claims adjudication, and case or medical management records, or that the Plan (or its Business Associate) uses, in whole or in part, to make decisions about Participants. The Plan has identified specific Designated Record Sets for particular uses (see Section 5.02).

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of PHI outside of the Plan.

ERISA: The Employee Retirement Income Security Act of 1974, as amended.

Fiduciary: A person or entity that exercises any discretionary authority or discretionary control respecting management of the Plan or disposition of its assets; renders investment advice for a fee or other compensation, direct or indirect, with respect to any moneys or other property of the Plan, or has authority or responsibility to do so; or has discretionary authority or discretionary responsibility in the administration of the Plan. A Fiduciary can be an individual, partnership,

joint venture, corporation, mutual company, joint-stock company, trust, estate, association, unincorporated organization, or employee organization. A person can be deemed a Fiduciary by performing the acts described above with or without authority to do so, by holding certain positions with duties and responsibilities similar to the acts described above, or by being expressly designated or named as a Fiduciary in the Plan Document.

Health Care Operations: Activities related to a Covered Entity's functions as a health plan, health provider, or health care clearinghouse. They include quality assessment and improvement activities, credentialing, training, accreditation activities, underwriting, premium rating, arranging for medical review and audit activities, business planning and development (such as cost management), customer service, grievance and appeals resolution, vendor evaluations, legal services.

HHS: The United States Department of Health and Human Services.

HIPAA Privacy Rule: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes "administrative simplification" rules that will affect the way group health plans and their vendors use, disclose, transmit, and secure health information. The administrative simplification rules include: privacy protections; rules governing transmission of electronic health care data (electronic data interchange or "EDI" rules); and rules that apply new security standards to health information. The "HIPAA Privacy Rule" refers to the new privacy protections of HIPAA.

Insurer: An underwriter, insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a state and is subject to state law that regulates insurance. This term does not include a group health plan.

Marketing: A communication about a product or service that encourages recipients of the communication to purchase or use the product or service, except for communication made:

- To describe a health-related product or service (or payment for such product or service) that is provided by, or included in the benefits of, the Plan, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, the Plan; and health-related products or services available only to a Plan enrollee that add value to, but are not part of, the Plan's benefits;

- For Treatment; or

- For case management or care coordination for the person, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the person.

In addition, marketing includes an arrangement between a Covered Entity and any other entity whereby the Covered Entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product

or service that encourages recipients of the communication to purchase or use that product or service.

Minimum Necessary: To the extent practical, individually identifiable health information should be disclosed only to the extent needed to support the purpose of disclosure. Covered Entities are expected to make a reasonable effort to limit use, disclosure of, and requests for PHI to the *Minimum Necessary*. HIPAA requires Covered Entities to make their own assessment of what health information is reasonably necessary.

Participant: Persons who are or were eligible for benefits under the Plan. Participant refers to both active employees who are members of the Plan and other beneficiaries, unless the context clearly indicates otherwise.

Payment: Activities by a plan to obtain premiums or determine or fulfill its responsibility for coverage and the provision of benefits under the Plan. Also, activities by a plan or provider to obtain or provide reimbursement for the provision of health care. These activities include determinations of eligibility or coverage, adjudication or subrogation or health benefit claims, billing, claims management, collection activities, reinsurance payment, review of health care services with respect to medical necessity, review of coverage under a health plan, review appropriateness of care or justification of charges, and utilization review activities.

Plan: The health plan for which these Policies and Procedures were written.

Plan Sponsor: The employer, employee organization, or the association, committee, joint board of trustees, or other similar group of representatives, that established or maintain the Plan.

Policies and Procedures: Descriptions of the Plan's intentions and process for complying with the HIPAA Privacy Rule, as codified in this Manual.

Privacy Official: A designated individual responsible for the development and implementation of the Plan's privacy Policies and Procedures.

Privacy Notice: A description, provided to Participants at specific times, and to other persons upon a request of the Plan's practices concerning its uses and disclosures of PHI, which also informs Participants of their rights and of the Plan's legal duties, with respect to PHI.

Protected Health Information (PHI): Individually identifiable health information created or received by a Covered Entity. Information is "individually identifiable" if it names the individual person or there is a reasonable basis to believe components of the information could be used to identify the individual. "Health information" means information, whether oral or recorded in any form or medium, that (i) is created by a health care provider, 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.

Psychotherapy Notes: Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. It excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Treatment: The provision, coordination, or management of health care by one (1) or more health care providers. It includes health care coordination or management between a provider and a third party, as well as consultation and referrals between providers.

9. HIPAA Privacy Rule

Standards for Privacy of Individually Identifiable Health Information
Regulation Text, as amended
Table of Contents

PART 160 – GENERAL ADMINISTRATIVE REQUIREMENTS

Authority: Sec. 1171 through 1179 of the Social Security Act, (42 U.S.C. 1320d- 1329d-8) as added by sec. 262 of Pub. L. No. 104-191, 110 Stat. 2021-2031 and sec. 264 of Pub. L. No. 104-191 (42 U.S.C. 1320d- 2(note)).

Subpart A - General Provisions

§ 160.101 Statutory basis and purpose.

The requirements of this subchapter implement sections 1171 through 1179 of the Social Security Act (the Act), as added by section 262 of Public Law 104-191, and section 264 of Public Law 104-191.

§ 160.102 Applicability.

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:
(1) A health plan.
(2) A health care clearinghouse.
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
(b) To the extent required under the Social Security Act, 42 U.S.C. 1320a-7c(a)(5), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

§ 160.103 Definitions.

Except as otherwise provided, the following definitions apply to this subchapter:.
Act means the Social Security Act.
ANSI stands for the American National Standards Institute.
Business associate:
(1) Except as provided in paragraph (2) of this definition, *business associate* means, with respect to a covered entity, a person who:
(i) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:
(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
(B) Any other function or activity regulated by this subchapter; or
(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.
(3) A covered entity may be a business associate of another covered entity.
Compliance date means the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.
Covered entity means:
(1) A health plan.
(2) A health care clearinghouse.
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
EIN stands for the employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury. The EIN is the taxpayer identifying number of an individual or other entity (whether or not an employer) assigned under one or the following:
(1) 26 U.S.C. 6011(b), which is the portion of the Internal Revenue Code dealing with identifying the taxpayer in tax returns and statements, or corresponding provisions of prior law.
(2) 26 U.S.C. 6109, which is the portion of the Internal Revenue Code dealing with identifying numbers in tax returns, statements, and other required documents.
Employer is defined as it is in 26 U.S.C. 3401(d).
Group health plan (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C.

300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:
(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or
(2) Is administered by an entity other than the employer that established and maintains the plan.
HCFA stands for Health Care Financing Administration within the Department of Health and Human Services.
HHS stands for the Department of Health and Human Services.
Health care means care, services, or supplies related to the health of an individual.
Health care includes, but is not limited to, the following:
(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:
(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.
Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, whether oral or recorded in any form or medium, that:
(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
(2) 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.
Health insurance issuer (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of *health plan* in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.
Health maintenance organization (HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of *health plan* in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.
Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).
(1) *Health plan* includes the following, singly or in combination:
(i) A group health plan, as defined in this section.
(ii) A health insurance issuer, as defined in this section.
(iii) An HMO, as defined in this section. (iv) Part A or Part B of the Medicare program under title XVIII of the Act.
(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.
(vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).
(vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.
(viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.
(ix) The health care program for active military personnel under title 10 of the United States Code.
(x) The veterans health care program under 38 U.S.C. chapter 17.
(xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)(as defined in 10 U.S.C. 1072(4)).
(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq. (xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.
(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.
(xv) The Medicare + Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28. (xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.
(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).
(2) *Health plan* excludes:
(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg- 91(c)(1); and
(ii) A government-funded program (other than one listed in paragraph (1)(i)-(xvi)of this definition):
(A) Whose principal purpose is other than providing, or paying the cost of, health care; or
(B) Whose principal activity is:
(*1*) The direct provision of health care to persons; or
(*2*) The making of grants to fund the direct provision of health care to persons.

Implementation specification means specific requirements or instructions for implementing a standard.
Individually identifiable health

information is information that is a subset of health information, including demographic information collected from an individual, and:
(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) 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; and
(i) That identifies the individual; or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
Modify or *modification* refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.
Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.
Small health plan means a health plan with annual receipts of $5 million or less.
Standard means a rule, condition, or requirement:
(1) Describing the following information for products, systems, services or practices: (i) Classification of components.
(ii) Specification of materials, performance, or operations; or
(iii) Delineation of procedures; or
(2) With respect to the privacy of individually identifiable health information.
Standard setting organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.
State refers to one of the following:
(1) For a health plan established or regulated by Federal law, *State* has the meaning set forth in the applicable section of the United States Code for such health plan.
(2) For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.
Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)
Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:
(1) Health care claims or equivalent encounter information.
(2) Health care payment and remittance advice.
(3) Coordination of benefits.
(4) Health care claim status.
(5) Enrollment and disenrollment in a health plan.
(6) Eligibility for a health plan.
(7) Health plan premium payments.
(8) Referral certification and authorization.
(9) First report of injury.
(10) Health claims attachments.
(11) Other transactions that the Secretary may prescribe by regulation.
Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

§ 160.104 Modifications.
(a) Except as provided in paragraph (b) of this section, the Secretary may adopt a modification to a standard or implementation specification adopted under this subchapter no more frequently than once every 12 months.

(b) The Secretary may adopt a modification at any time during the first year after the standard or implementation specification is initially adopted, if the Secretary determines that the modification is necessary to permit compliance with the standard or implementation specification.
(c) The Secretary will establish the compliance date for any standard or implementation specification modified under this section.
(1) The compliance date for a modification is no earlier than 180 days after the effective date of the final rule in which the Secretary adopts the modification.
(2) The Secretary may consider the extent of the modification and the time needed to comply with the modification in determining the compliance date for the modification.
(3) The Secretary may extend the compliance date for small health plans, as the Secretary determines is appropriate.

Subpart B - Preemption of State Law
§ 160.201 Applicability.

The provisions of this subpart implement section 1178 of the Act, as added by section 262 of Public Law 104-191.

§ 160.202 Definitions. For purposes of this subpart, the following terms have the following meanings:
Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:
(1) A covered entity would find it impossible to comply with both the State and federal requirements; or
(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act or section 264 of Pub. L. 104-191, as applicable.
More stringent means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:
(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:
(i) Required by the Secretary in connection with determining whether a covered entity is in compliance with this subchapter; or
(ii) To the individual who is the subject of the individually identifiable health information.
(2) With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable

health information, permits greater rights of access or amendment, as applicable.
(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.
(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.
(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.
(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

§ 160.203 General rule and exceptions.

A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:
(a) A determination is made by the Secretary under § 160.204 that the provision of State law:
(1) Is necessary:
(i) To prevent fraud and abuse related to the provision of or payment for health care;
(ii) To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;
(iii) For State reporting on health care delivery or costs; or
(iv) For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or
(2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.
(b) The provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.
(c) The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.
(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

§ 160.204 Process for requesting exception determinations.

(a) A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:
(1) The State law for which the exception is requested;
(2) The particular standard, requirement, or implementation specification for which the exception is requested;
(3) The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;
(4) How health care providers, health plans, and other entities would be affected by the exception;
(5) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and
(6) Any other information the Secretary may request in order to make the determination.
(b) Requests for exception under this section must be submitted to the Secretary at an address that will be published in the Federal Register. Until the Secretary's determination is made, the standard, requirement, or implementation specification under this subchapter remains in effect.
(c) The Secretary's determination under this section will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met.

§ 160.205 Duration of effectiveness of exception determinations.

An exception granted under this subpart remains in effect until:
(a) Either the State law or the federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or
(b) The Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

Subpart C - Compliance and Enforcement

§ 160.300 Applicability.

This subpart applies to actions by the Secretary, covered entities, and others with respect to ascertaining the compliance by covered entities with and the enforcement of the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.302 Definitions.

As used in this subpart, terms defined

in § 164.501 of this subchapter have the same meanings given to them in that section.

§ 160.304 Principles for achieving compliance.
(a) *Cooperation.* The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.
(b) *Assistance.* The Secretary may provide technical assistance to covered entities to help them comply voluntarily with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.306 Complaints to the Secretary.
(a) *Right to file a complaint.* A person who believes a covered entity is not complying with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter may file a complaint with the Secretary.
(b) *Requirements for filing complaints.* Complaints under this section must meet the following requirements:
(1) A complaint must be filed in writing, either on paper or electronically.
(2) A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.
(3) A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.
(4) The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.
(c) *Investigation.* The Secretary may investigate complaints filed under this section. Such investigation may include a review of the pertinent policies, procedures, or practices of the covered entity and of the circumstances regarding any alleged acts or omissions concerning compliance.

§ 160.308 Compliance reviews.
The Secretary may conduct compliance reviews to determine whether covered entities are complying with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

§ 160.310 Responsibilities of covered entities.
(a) *Provide records and compliance reports.* A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.
(b) *Cooperate with complaint investigations and compliance reviews.* A covered entity must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of a covered entity to determine whether it is complying with the applicable requirements of this part 160 and the standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.
(c) *Permit access to information.*
(1) A covered entity must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity must permit access by the Secretary at any time and without notice.
(2) If any information required of a covered entity under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity must so certify and set forth what efforts it has made to obtain the information.
(3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter, or if otherwise required by law.

§ 160.312 Secretarial action regarding complaints and compliance reviews.
(a) *Resolution where noncompliance is indicated.*
(1) If an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates a failure to comply, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant, in writing and attempt to resolve the matter by informal means whenever possible.
(2) If the Secretary finds the covered entity is not in compliance and determines that the matter cannot be resolved by informal means, the Secretary may issue to the covered entity and, if the matter arose from a complaint, to the complainant written findings documenting the non-compliance.
(b) *Resolution when no violation is found.* If, after an investigation or compliance review, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity and, if the matter arose from a complaint, the complainant in writing.

PART 164 – SECURITY AND PRIVACY

Subpart A – General Provisions
164.102 Statutory basis.
164.104 Applicability.
164.106 Relationship to other parts.

Subparts B-D – [Reserved]

Subpart E – Privacy of Individually Identifiable Health Information

Authority: 42 U.S.C. 1320d-2 and 1320d-4, sec. 264 of Pub. L. No. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2(note)).

Subpart A–General Provisions

§ 164.102 Statutory basis.

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act and section 264 of Public Law 104-191.

§ 164.104 Applicability.

Except as otherwise provided, the provisions of this part apply to covered entities: health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with any transaction referred to in section 1173(a)(1) of the Act.

§ 164.106 Relationship to other parts.

In complying with the requirements of this part, covered entities are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

Subpart B-D–[Reserved]

Subpart E - Privacy of Individually Identifiable Health Information

§ 164.500 Applicability.

(a) Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.

(b) Health care clearinghouses must comply with the standards, requirements, and implementation specifications as follows:

(1) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, the clearinghouse must comply with:

(i) Section 164.500 relating to applicability;

(ii) Section 164.501 relating to definitions;

(iii) Section 164.502 relating to uses and disclosures of protected health information, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(iv) Section 164.504 relating to the organizational requirements for covered entities, including the designation of health care components of a covered entity;

(v) Section 164.512 relating to uses and disclosures for which individual authorization or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(vi) Section 164.532 relating to transition requirements; and

(vii) Section 164.534 relating to compliance dates for initial implementation of the privacy standards.

(2) When a health care clearinghouse creates or receives protected health information other than as a business associate of a covered entity, the clearinghouse must comply with all of the standards, requirements, and implementation specifications of this subpart.

(c) The standards, requirements, and implementation specifications of this subpart do not apply to the Department of Defense or to any other federal agency, or nongovernmental organization acting on its behalf, when providing health care to overseas foreign national beneficiaries.

§ 164.501 Definitions.

As used in this subpart, the following terms have the following meanings:

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons held in lawful custody* includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Designated record set means:
(1) A group of records maintained by or for a covered entity that is:
(i) The medical records and billing records about individuals maintained by or for a covered health care provider;
(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.
(2) For purposes of this paragraph, the term *record* means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.
Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:
(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;
(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
(6) Business management and general administrative activities of the entity, including, but not limited to:
(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
(ii) Customer service, including the provision of data analyses for policy holders, Plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, Plan sponsor, or customer.
(iii) Resolution of internal grievances;
(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
(v) Consistent with the applicable requirements of § 164.514, creating deidentified health information or a limited data set, and fundraising for the benefit of the covered entity.
Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.
Indirect treatment relationship means a relationship between an individual and a health care provider in which:
(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and
(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.
Individual means the person who is the subject of protected health information.
Inmate means a person incarcerated in or otherwise confined to a correctional institution.
Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:
(1) Investigate or conduct an official inquiry into a potential violation of law; or
(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.
Marketing means:
(1) To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:
(i) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.
(ii) For treatment of the individual; or
(iii) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the

individual.
(2) An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.
Organized health care arrangement means: (1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
(2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
(i) Hold themselves out to the public as participating in a joint arrangement; and
(ii) Participate in joint activities that include at least one of the following:
(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;
(4) A group health plan and one or more other group health plans each of which are maintained by the same Plan sponsor; or
(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.
Payment means:
(1) The activities undertaken by:
(i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and
(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:
(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;
(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
(A) Name and address;
(B) Date of birth;
(C) Social security number;
(D) Payment history;
(E) Account number; and
(F) Name and address of the health care provider and/or health plan.
Plan Sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).
Protected health information means individually identifiable health information:
(1) Except as provided in paragraph (2) of this definition, that is:
(i) Transmitted by electronic media;
(ii) Maintained in any medium described in the definition of *electronic media* at § 162.103 of this subchapter; or
(iii) Transmitted or maintained in any other form or medium.
(2) *Protected health information* excludes individually identifiable health information in:
(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
(iii) Employment records held by a covered entity in its role as employer.
Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.
Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.
Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.
Required by law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law.
Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or

summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

§ 164.502 Uses and disclosures of protected health information: general rules.

(a) *Standard.* A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) *Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of § 164.502(b), § 164.514(d), and § 164.530(c) with respect to such otherwise permitted or required use or disclosure;

(iv) Pursuant to and in compliance with an authorization that complies with § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

(vi) As permitted by and in compliance with this section, § 164.512, or § 164.514(e), (f), or (g).

(2) *Required disclosures.* A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and as required by §§ 164.524 or 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.

(b) *Standard: minimum necessary.*

(1) *Minimum necessary applies.* When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) *Minimum necessary does not apply.* This requirement does not apply to:

(i) Disclosures to or requests by a health care provider for treatment;

(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;

(iii) Uses or disclosures made pursuant to an authorization under § 164.508;

(iv) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;

(v) Uses or disclosures that are required by law, as described by § 164.512(a); and

(vi) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

(c) *Standard: uses and disclosures of protected health information subject to an agreed upon restriction.* A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

(d) *Standard: uses and disclosures of deidentified protected health information.*

(1) *Uses and disclosures to create deidentified information.* A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) *Uses and disclosures of de-identified information.* Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is reidentified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

(e)(1) *Standard: disclosures to business associates.*

(i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

(ii) This standard does not apply:

(A) With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual;

(B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the Plan sponsor, to the extent that the requirements of § 164.504(f) apply and are met; or

(C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency

other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.
(iii) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.504(e).
(2) *Implementation specification: documentation.* A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).
(f) *Standard: deceased individuals.* A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual.
(g)(1) *Standard: personal representatives.* As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.
(2) *Implementation specification: adults and emancipated minors.* If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.
(3) *Implementation specification: unemancipated minors.*
(i) If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:
(A) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;
(B) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or
(C) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.
(ii) Notwithstanding the provisions of paragraph (g)(3)(i) of this section:
(A) If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*;
(B) If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*; and
(C) Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative under paragraph (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under § 164.524 to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.
(4) *Implementation specification: deceased individuals.* If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.
(5) *Implementation specification: abuse, neglect, endangerment situations.* Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:
(i) The covered entity has a reasonable belief that:
(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or
(B) Treating such person as the personal representative could endanger the individual; and
(ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.
(h) *Standard: confidential communications.* A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.
(i) *Standard: uses and disclosures consistent with notice.* A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.
(j) *Standard: disclosures by whistleblowers and workforce member crime victims.*
(1) *Disclosures by whistleblowers.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or

a business associate discloses protected health information, provided that:
(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and
(ii) The disclosure is to:
(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or
(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.
(2) *Disclosures by workforce members who are victims of a crime.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:
(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and
(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

§ 164.504 Uses and disclosures: organizational requirements.
(a) *Definitions.* As used in this section:
Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.
Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.
Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with paragraph (c)(3)(iii) of this section.
Hybrid entity means a single legal entity:
(1) That is a covered entity;
(2) Whose business activities include both covered and non-covered functions; and
(3) That designates health care components in accordance with paragraph (c)(3)(iii) of this section.
Plan administration functions means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.
Summary health information means information, that may be individually identifiable health information, and:
(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a Plan sponsor has provided health benefits under a group health plan; and
(2) From which the information described at § 164.514(b)(2)(i) has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.
(b) *Standard: health care component.* If a covered entity is a hybrid entity, the requirements of this subpart, other than the requirements of this section, apply only to the health care component(s) of the entity, as specified in this section.
(c)(1) *Implementation specification: application of other provisions.* In applying a provision of this subpart, other than this section, to a hybrid entity:
(i) A reference in such provision to a "covered entity" refers to a health care component of the covered entity;
(ii) A reference in such provision to a "health plan," "covered health care provider," or "health care clearinghouse" refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable; and
(iii) A reference in such provision to "protected health information" refers to protected health information that is created or received by or on behalf of the health care component of the covered entity.
(2) *Implementation specifications: safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this subpart. In particular, and without limiting this requirement, such covered entity must ensure that:
(i) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which this subpart would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;
(ii) A component that is described by paragraph (c)(3)(iii)(B) of this section does not use or disclose protected health information that it creates or receives from or on behalf of the health care component in a way prohibited by this subpart; and
(iii) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by this subpart.
(3) *Implementation specifications: responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities:
(i) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility to comply with this subpart.
(ii) The covered entity has the responsibility for complying with § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with this subpart, including the safeguard requirements in paragraph (c)(2) of this section.
(iii) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation as required by § 164.530(j), provided that, if the covered entity designates a health care component or components, it must include any component that would meet the definition of covered entity if

it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs:
(A) Covered functions; or
(B) Activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.
(d)(1) *Standard: affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this subpart.
(2) *Implementation specifications: requirements for designation of an affiliated covered entity.*
(i) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this subpart, if all of the covered entities designated are under common ownership or control.
(ii) The designation of an affiliated covered entity must be documented and the documentation maintained as required by § 164.530(j).
(3) *Implementation specifications: safeguard requirements.* An affiliated covered entity must ensure that:
(i) The affiliated covered entity's use and disclosure of protected health information comply with the applicable requirements of this subpart; and
(ii) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with paragraph (g) of this section.
(e)(1) *Standard: business associate contracts.*
(i) The contract or other arrangement between the covered entity and the business associate required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable.
(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (e) of this section, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:
(A) Terminated the contract or arrangement, if feasible; or
(B) If termination is not feasible, reported the problem to the Secretary.
(2) *Implementation specifications: business associate contracts.* A contract between the covered entity and a business associate must:
(i) Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:
(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and
(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.
(ii) Provide that the business associate will:
(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;
(B) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;
(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;
(D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;
(E) Make available protected health information in accordance with § 164.524;
(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;
(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;
(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and
(I) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.
(3) *Implementation specifications: other arrangements.*
(i) If a covered entity and its business associate are both governmental entities:
(A) The covered entity may comply with paragraph (e) of this section by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section.
(B) The covered entity may comply with paragraph (e) of this section, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section.
(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of *business associate* in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without

meeting the requirements of this paragraph (e), provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(3)(i) of this section, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.
(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.
(4) *Implementation specifications: other requirements for contracts and other arrangements.*
(i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary:
(A) For the proper management and administration of the business associate; or
(B) To carry out the legal responsibilities of the business associate.
(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:
(A) The disclosure is required by law; or
(B)*(1)* The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and
(2) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.
(f)(1) *Standard: Requirements for group health plans.*
(i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.
(ii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of:
(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or (B) Modifying, amending, or terminating the group health plan.
(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.
(2) *Implementation specifications: requirements for plan documents.* The plan documents of the group health plan must be amended to incorporate provisions to:
(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.
(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:
(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;
(B) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;
(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;
(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;
(E) Make available protected health information in accordance with § 164.524;
(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;
(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;
(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;
(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor 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; and
(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.
(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:
(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;
(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration

functions that the plan sponsor performs for the group health plan; and
(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.
(3) *Implementation specifications: uses and disclosures.* A group health plan may:
(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;
(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;
(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and
(iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.
(g) *Standard: requirements for a covered entity with multiple covered functions.*

(1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.
(2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.
(a) *Standard: Permitted uses and disclosures.* Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.
(b) *Standard: Consent for uses and disclosures permitted.*
(1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.
(2) Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under § 164.508, is required or when another condition must be met for such use or disclosure to be permissible under this subpart.
(c) *Implementation specifications: Treatment, payment, or health care operations.*
(1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.
(2) A covered entity may disclose protected health information for treatment activities of a health care provider.
(3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.
(4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:
(i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or
(ii) For the purpose of health care fraud and abuse detection or compliance.
(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

§ 164.508 Uses and disclosures for which an authorization is required.
(a) *Standard: authorizations for uses and disclosures.*
(1) *Authorization required: general rule.* Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.
(2) *Authorization required: psychotherapy notes.* Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:
(i) To carry out the following treatment, payment, or health care operations:
(A) Use by the originator of the psychotherapy notes for treatment;
(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or
(C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and
(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).
(3) *Authorization required: Marketing.*
(i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:
(A) A face-to-face communication

made by a covered entity to an individual; or
(B) A promotional gift of nominal value provided by the covered entity.
(ii) If the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.
(b) *Implementation specifications: general requirements.*
(1) *Valid authorizations.*
(i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (c)(1), and (c)(2) of this section, as applicable.
(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.
(2) *Defective authorizations.* An authorization is not valid, if the document submitted has any of the following defects:
(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;
(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable;
(iii) The authorization is known by the covered entity to have been revoked;
(iv) The authorization violates paragraph (b)(3) or (4) of this section, if applicable;
(v) Any material information in the authorization is known by the covered entity to be false.
(3) *Compound authorizations.* An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:
(i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of protected health information for such research or a consent to participate in such research;
(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;
(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations.
(4) *Prohibition on conditioning of authorizations.* A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:
(i) A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;
(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:
(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and
(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and
(iii) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.
(5) *Revocation of authorizations.* An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:
(i) The covered entity has taken action in reliance thereon; or
(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.
(6) *Documentation.* A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).
(c) *Implementation specifications: Core elements and requirements.*
(1) *Core elements.* A valid authorization under this section must contain at least the following elements:
(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.
(iv) A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
(v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.
(vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.
(2) *Required statements.* In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:
(i) The individual's right to revoke the authorization in writing, and either:
(A) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or
(B) To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.
(ii) The ability or inability to condition

treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:
(A) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or
(B) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.
(iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.
(3) *Plain language requirement.* The authorization must be written in plain language.
(4) *Copy to the individual.* If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.
A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.
(a) *Standard: use and disclosure for facility directories.*
(1) *Permitted uses and disclosure.* Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:
(i) Use the following protected health information to maintain a directory of individuals in its facility:
(A) The individual's name;
(B) The individual's location in the covered health care provider's facility;
(C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and
(D) The individual's religious affiliation; and
(ii) Disclose for directory purposes such information:
(A) To members of the clergy; or
(B) Except for religious affiliation, to other persons who ask for the individual by name.
(2) *Opportunity to object.* A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.
(3) *Emergency circumstances.*
(i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:
(A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and
(B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.
(ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.
(b) *Standard: uses and disclosures for involvement in the individual's care and notification purposes.*
(1) *Permitted uses and disclosures.*
(i) A covered entity may, in accordance with paragraphs (b)(2) or (3) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.
(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (3), or (4) of this section, as applicable.
(2) *Uses and disclosures with the individual present.* If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:
(i) Obtains the individual's agreement;
(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
(iii) Reasonably infers from the circumstances, based the exercise of professional judgment, that the individual does not object to the disclosure.
(3) *Limited uses and disclosures when the individual is not present.* If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

(4) *Use and disclosures for disaster relief purposes.* A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

A covered entity may use or disclose protected health information without the written authorization of the individual, as described in § 164.508, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally.

(a) *Standard: uses and disclosures required by law.*

(1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

(b) *Standard: uses and disclosures for public health activities.*

(1) *Permitted disclosures.* A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(iii) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

(A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

(B) To track FDA-regulated products;

(C) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or

(D) To conduct post marketing surveillance;

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides health care to the individual at the request of the employer:

(*1*) To conduct an evaluation relating to medical surveillance of the workplace; or

(*2*) To evaluate whether the individual has a work-related illness or injury;

(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

(*1*) By giving a copy of the notice to the individual at the time the health care is provided; or

(*2*) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

(2) *Permitted uses.* If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) *Standard: disclosures about victims of abuse, neglect or domestic violence.*

(1) *Permitted disclosures.* Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;

(ii) If the individual agrees to the disclosure; or

(iii) To the extent the disclosure is expressly authorized by statute or regulation and:

(A) The covered entity, in the exercise of professional judgment, believes the

disclosure is necessary to prevent serious harm to the individual or other potential victims; or
(B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
(2) *Informing the individual.* A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if: (i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
(ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.
(d) *Standard: uses and disclosures for health oversight activities.*
(1) *Permitted disclosures.* A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:
(i) The health care system;
(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;
(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.
(2) *Exception to health oversight activities.* For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:
(i) The receipt of health care;
(ii) A claim for public benefits related to health; or
(iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.
(3) *Joint activities or investigations.* Notwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.
(4) *Permitted uses.* If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.
(e) *Standard: disclosures for judicial and administrative proceedings.*
(1) *Permitted disclosures.* A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:
(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or
(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:
(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or
(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.
(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protecting health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:
(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);
(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and
(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:
(*1*) No objections were filed; or
(*2*) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.
(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:
(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.
(v) For purposes of paragraph (e)(1) of this section, a *qualified protective order* means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and
(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.
(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.
(2) *Other uses and disclosures under this section.* The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.
(f) *Standard: disclosures for law enforcement purposes.* A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.
(1) *Permitted disclosures: pursuant to process and as otherwise required by law.* A covered entity may disclose protected health information:
(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or
(ii) In compliance with and as limited by the relevant requirements of:
(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
(B) A grand jury subpoena; or
(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
(*1*) The information sought is relevant and material to a legitimate law enforcement inquiry;
(*2*) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
(*3*) De-identified information could not reasonably be used.
(2) *Permitted disclosures: limited information for identification and location purposes.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:
(i) The covered entity may disclose only the following information:
(A) Name and address;
(B) Date and place of birth;
(C) Social security number;
(D) ABO blood type and rh factor;
(E) Type of injury;
(F) Date and time of treatment;
(G) Date and time of death, if applicable; and
(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.
(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.
(3) *Permitted disclosure: victims of a crime.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:
(i) The individual agrees to the disclosure; or
(ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:
(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.
(4) *Permitted disclosure: decedents.* A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.
(5) *Permitted disclosure: crime on premises.* A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.
(6) *Permitted disclosure: reporting crime in emergencies.*
(i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:
(A) The commission and nature of a crime; (B) The location of such crime or of the victim(s) of such crime; and
(C) The identity, description, and location of the perpetrator of such crime.
(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to

paragraph (c) of this section.
(g) *Standard: uses and disclosures about decedents.*
(1) *Coroners and medical examiners.* A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.
(2) *Funeral directors.* A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.
(h) *Standard: uses and disclosures for cadaveric organ, eye or tissue donation purposes.* A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.
(i) *Standard: uses and disclosures for research purposes.*
(1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:
(i) *Board approval of a waiver of authorization.* The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either:
(A) An Institutional Review Board (IRB), established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or
(B) A privacy board that:
(*1*) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;
(*2*) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and
(*3*) Does not have any member participating in a review of any project in which the member has a conflict of interest.
(ii) *Reviews preparatory to research.* The covered entity obtains from the researcher representations that:
(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;
(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and
(C) The protected health information for which use or access is sought is necessary for the research purposes.
(iii) *Research on decedent's information.* The covered entity obtains from the researcher:
(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;
(B) Documentation, at the request of the covered entity, of the death of such individuals; and
(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.
(2) *Documentation of waiver approval.* For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:
(i) *Identification and date of action.* A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved; (ii) *Waiver criteria.* A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:
(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;
(*1*) An adequate plan to protect the identifiers from improper use and disclosure;
(*2*) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
(*3*) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;
(B) The research could not practicably be conducted without the waiver or alteration; and
(C) The research could not practicably be conducted without access to and use of the protected health information.
(iii) *Protected health information needed.* A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board has determined, pursuant to paragraph (i)(2)(ii)(C) of this section;
(iv) *Review and approval procedures.* A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:
(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR

46.110, 45 CFR 690.110, or 49 CFR 11.110);
(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(*2*) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;
(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and
(v) *Required signature.* The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.
(j) *Standard: uses and disclosures to avert a serious threat to health or safety.*
(1) *Permitted disclosures.* A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:
(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and
(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or
(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:
(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or
(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.
(2) *Use or disclosure not permitted.* A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:
(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or
(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.
(3) *Limit on information that may be disclosed.* A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.
(4) *Presumption of good faith belief.* A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.
(k) *Standard: uses and disclosures for specialized government functions.*
(1) *Military and veterans activities.*
(i) *Armed Forces personnel.* A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the **Federal Register** the following information:
(A) Appropriate military command authorities; and
(B) The purposes for which the protected health information may be used or disclosed.
(ii) *Separation or discharge from military service.* A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.
(iii) *Veterans.* A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.
(iv) *Foreign military personnel.* A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the **Federal Register** pursuant to paragraph (k)(1)(i) of this section.
(2) *National security and intelligence activities.* A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (e.g., Executive Order 12333).
(3) *Protective services for the President and others.* A covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879.
(4) *Medical suitability determinations.* A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the

Department of State who need access to such information for the following purposes:
(i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12698;
(ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or
(iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.
(5) *Correctional institutions and other law enforcement custodial situations.*
(i) *Permitted disclosures.* A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:
(A) The provision of health care to such individuals;
(B) The health and safety of such individual or other inmates;
(C) The health and safety of the officers or employees of or others at the correctional institution;
(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
(E) Law enforcement on the premises of the correctional institution; and
(F) The administration and maintenance of the safety, security, and good order of the correctional institution.
(ii) *Permitted uses.* A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.
(iii) *No application after release.* For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.
(6) *Covered entities that are government programs providing public benefits.*
(i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.
(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.
(l) *Standard: disclosures for workers' compensation.* A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

§ 164.514 Other requirements relating to uses and disclosures of protected health information.
(a) *Standard: de-identification of protected health information.* 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 is not individually identifiable health information.
(b) *Implementation specifications: requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:
(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
(ii) Documents the methods and results of the analysis that justify such determination; or
(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:
(A) Names;
(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
(*1*) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
(*2*) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
(D) Telephone numbers;
(E) Fax numbers;
(F) Electronic mail addresses;
(G) Social security numbers;
(H) Medical record numbers;
(I) Health plan beneficiary numbers;
(J) Account numbers;
(K) Certificate/license numbers;
(L) Vehicle identifiers and serial numbers, including license plate numbers;
(M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs);
(O) Internet Protocol (IP) address numbers;
(P) Biometric identifiers, including finger and voice prints;
(Q) Full face photographic images and any comparable images; and
(R) Any other unique identifying

number, characteristic, or code, except as permitted by paragraph (c) of this section; and
(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.
(c) *Implementation specifications: reidentification.* A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:
(1) *Derivation.* The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
(2) *Security.* The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for reidentification.
(d)(1) *Standard: minimum necessary requirements.* In order to comply with § 164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.
(2) *Implementation specifications: minimum necessary uses of protected health information.*
(i) A covered entity must identify:
(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and
(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.
(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.
(3) *Implementation specification: minimum necessary disclosures of protected health information.*
(i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.
(ii) For all other disclosures, a covered entity must:
(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and
(B) Review requests for disclosure on an individual basis in accordance with such criteria.
(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:
(A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);
(B) The information is requested by another covered entity;
(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or
(D) Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.
(4) *Implementation specifications: minimum necessary requests for protected health information.*
(i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.
(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.
(iii) For all other requests, a covered entity must:
(A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and
(B) Review requests for disclosure on an individual basis in accordance with such criteria.
(5) *Implementation specification: other content requirement.* For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.
(e) (1) *Standard: Limited data set.* A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.
(2) *Implementation specification: Limited data set:* A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:
(i) Names;
(ii) Postal address information, other than town or city, State, and zip code;
(iii) Telephone numbers;
(iv) Fax numbers;
(v) Electronic mail addresses;
(vi) Social security numbers;
(vii) Medical record numbers;
(viii) Health plan beneficiary numbers;
(ix) Account numbers;
(x) Certificate/license numbers;
(xi) Vehicle identifiers and serial numbers, including license plate numbers;
(xii) Device identifiers and serial numbers;
(xiii) Web Universal Resource Locators (URLs);
(xiv) Internet Protocol (IP) address numbers;
(xv) Biometric identifiers, including finger and voice prints; and
(xvi) Full face photographic images and any comparable images.

(3) *Implementation specification: Permitted purposes for uses and disclosures.*
(i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.
(ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.
(4) *Implementation specifications: Data use agreement.*
(i) *Agreement required.* A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.
(ii) *Contents.* A data use agreement between the covered entity and the limited data set recipient must:
(A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;
(B) Establish who is permitted to use or receive the limited data set; and
(C) Provide that the limited data set recipient will:
(*1*) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
(*2*) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
(*3*) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
(*4*) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
(*5*) Not identify the information or contact the individuals.
(iii) *Compliance.*
(A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:
(*1*) Discontinued disclosure of protected health information to the recipient; and
(*2*) Reported the problem to the Secretary.
(B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.
(f)(1) *Standard: uses and disclosures for fundraising.* A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:
(i) Demographic information relating to an individual; and
(ii) Dates of health care provided to an individual.
(2) *Implementation specifications: fundraising requirements.*
(i) The covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by §164.520(b)(1)(iii)(B) is included in the covered entity's notice;
(ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications.
(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.
(g) *Standard: uses and disclosures for underwriting and related purposes.* If a health plan receives protected heath information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other purpose, except as may be required by law.
(h)(1) *Standard: verification requirements.* Prior to any disclosure permitted by this subpart, a covered entity must:
(i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and
(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.
(2) *Implementation specifications: verification.*
(i) *Conditions on disclosures.* If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.
(A) The conditions in § 164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.
(B) The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).
(ii) *Identity of public officials.* A covered entity may rely, if such reliance is reasonable under the

circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:
(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
(B) If the request is in writing, the request is on the appropriate government letterhead; or
(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority 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.
(iii) *Authority of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:
(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;
(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.
(iv) *Exercise of professional judgment.* The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).

§ 164.520 Notice of privacy practices for protected health information.
(a) *Standard: notice of privacy practices.*
(1) *Right to notice.* Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.
(2) *Exception for group health plans.*
(i) An individual enrolled in a group health plan has a right to notice:
(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or
(B) From the health insurance issuer or HMO with respect to the group health plan though which such individuals receive their health benefits under the group health plan.
(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:
(A) Maintain a notice under this section; and
(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.
(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.
(3) *Exception for inmates.* An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.
(b) *Implementation specifications: content of notice.*
(1) *Required elements.* The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph.
(i) *Header.* The notice must contain the following statement as a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."
(ii) *Uses and disclosures.* The notice must contain:
(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.
(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization.
(C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202.
(D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.
(E) A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by § 164.508(b)(5).
(iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement, as applicable, that:
(A) The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other heath-related benefits and services that may be of interest to the individual;
(B) The covered entity may contact the individual to raise funds for the covered entity; or
(C) A group health plan, or a health

insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.
(iv) *Individual rights.* The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:
(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction;
(B) The right to receive confidential communications of protected health information as provided by § 164.522(b), as applicable;
(C) The right to inspect and copy protected health information as provided by § 164.524;
(D) The right to amend protected health information as provided by § 164.526;
(E) The right to receive an accounting of disclosures of protected health information as provided by § 164.528; and
(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.
(v) *Covered entity's duties.* The notice must contain:
(A) A statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information;
(B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and
(C) For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.
(vi) *Complaints.* The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.
(vii) *Contact.* The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by § 164.530(a)(1)(ii).
(viii) *Effective date.* The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.
(2) *Optional elements.*
(i) In addition to the information required by paragraph (b)(1) of this section, if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i).
(ii) For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.
(3) *Revisions to the notice.* The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.
(c) *Implementation specifications: provision of notice.* A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.
(1) *Specific requirements for health plans.*
(i) A health plan must provide notice:
(A) No later than the compliance date for the health plan, to individuals then covered by the plan;
(B) Thereafter, at the time of enrollment, to individuals who are new enrollees; and
(C) Within 60 days of a material revision to the notice, to individuals then covered by the plan.
(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.
(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.
(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.
(2) *Specific requirements for certain covered health care providers.* A covered health care provider that has a direct treatment relationship with an individual must:
(i) Provide the notice:
(A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or
(B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.
(ii) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;
(iii) If the covered health care provider maintains a physical service delivery site:
(A) Have the notice available at the service delivery site for individuals to request to take with them; and
(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health

care provider to be able to read the notice; and
(iv) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.
(3) *Specific requirements for electronic notice.*
(i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.
(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.
(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.
(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.
(d) *Implementation specifications: joint notice by separate covered entities.* Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:
(1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;
(2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and
(i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;
(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and
(iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.
(3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.
(e) *Implementation specifications: Documentation.* A covered entity must document compliance with the notice requirements, as required by § 164.530(j), by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with paragraph (c)(2)(ii) of this section.

§ 164.522 Rights to request privacy protection for protected health information.
(a)(1) *Standard: right of an individual to request restriction of uses and disclosures.*
(i) A covered entity must permit an individual to request that the covered entity restrict:
(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and
(B) Disclosures permitted under § 164.510(b).
(ii) A covered entity is not required to agree to a restriction.
(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.
(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.
(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.
(2) *Implementation specifications: terminating a restriction.* A covered entity may terminate its agreement to a restriction, if:
(i) The individual agrees to or requests the termination in writing;
(ii) The individual orally agrees to the termination and the oral agreement is documented; or
(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual.
(3) *Implementation specification: documentation.* A covered entity that agrees to a restriction must document the restriction in accordance with § 164.530(j).
(b)(1) *Standard: confidential communications requirements.*
(i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.
(ii) A health plan must permit individuals to request and must

accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.
(2) *Implementation specifications: conditions on providing confidential communications.*
(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.
(ii) A covered entity may condition the provision of a reasonable accommodation on:
(A) When appropriate, information as to how payment, if any, will be handled; and
(B) Specification of an alternative address or other method of contact.
(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.
(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

§ 164.524 Access of individuals to protected health information.
(a) *Standard: access to protected health information.*
(1) *Right of access.* Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:
(i) Psychotherapy notes;
(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
(iii) Protected health information maintained by a covered entity that is:
(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or
(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).
(2) *Unreviewable grounds for denial.* A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.
(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.
(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.
(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.
(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.
(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
(3) *Reviewable grounds for denial.* A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:
(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.
(4) *Review of a denial of access.* If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.
(b) *Implementation specifications: requests for access and timely action.*
(1) *Individual's request for access.* The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.
(2) *Timely action by the covered entity.*
(i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.
(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.
(B) If the covered entity denies the

request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.
(ii) If the request for access is for protected health information that is not maintained or accessible to the covered entity on-site, the covered entity must take an action required by paragraph (b)(2)(i) of this section by no later than 60 days from the receipt of such a request.
(iii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) or (ii) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:
(A) The covered entity, within the time limit set by paragraph (b)(2)(i) or (ii) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and
(B) The covered entity may have only one such extension of time for action on a request for access.
(c) *Implementation specifications: provision of access.* If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.
(1) *Providing the access requested.* The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.
(2) *Form of access requested.*
(i) The covered entity must provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.
(ii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:
(A) The individual agrees in advance to such a summary or explanation; and
(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.
(3) *Time and manner of access.* The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.
(4) *Fees.* If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:
(i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual;
(ii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
(iii) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.
(d) *Implementation specifications: denial of access.* If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.
(1) *Making other information accessible.* The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.
(2) *Denial.* The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:
(i) The basis for the denial;
(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and
(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).
(3) *Other responsibility.* If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.
(4) *Review of denial requested.* If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.
(e) *Implementation specification: documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):
(1) The designated record sets that are subject to access by individuals; and
(2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

§ 164.526 Amendment of protected health information.

(a) *Standard: right to amend.*

(1) *Right to amend.* An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) *Denial of amendment.* A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

(i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment

(ii) Is not part of the designated record set;

(iii) Would not be available for inspection under § 164.524; or

(iv) Is accurate and complete.

(b) *Implementation specifications: requests for amendment and timely action.*

(1) *Individual's request for amendment.* The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

(2) *Timely action by the covered entity.*

(i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) *Implementation specifications: accepting the amendment.* If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Making the amendment.* The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) *Informing the individual.* In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) *Informing others.* The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) *Implementation specifications: denying the amendment.* If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Denial.* The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).

(2) *Statement of disagreement.* The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) *Rebuttal statement.* The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) *Recordkeeping.* The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) *Future disclosures.*

(i) If a statement of disagreement has

been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.
(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.
(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.
(e) *Implementation specification: actions on notices of amendment.* A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.
(f) *Implementation specification: documentation.* A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).

§ 164.528 Accounting of disclosures of protected health information.
(a) *Standard: right to an accounting of disclosures of protected health information.*
(1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:
(i) To carry out treatment, payment and health care operations as provided in § 164.506;
(ii) To individuals of protected health information about them as provided in § 164.502;
(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;
(iv) Pursuant to an authorization as provided in § 164.508;
(v) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510;
(vi) For national security or intelligence purposes as provided in § 164.512(k)(2);
(vii) To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);
(viii) As part of a limited data set in accordance with § 164.514(e); or
(ix) That occurred prior to the compliance date for the covered entity.
(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.
(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:
(A) Document the statement, including the identity of the agency or official making the statement;
(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and
(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.
(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.
(b) *Implementation specifications: content of the accounting.* The covered entity must provide the individual with a written accounting that meets the following requirements.
(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.
(2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure:
(i) The date of the disclosure;
(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;
(iii) A brief description of the protected health information disclosed; and
(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.
(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, the accounting may, with respect to such multiple disclosures, provide:
(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;
(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and
(iii) The date of the last such disclosure during the accounting period.
(4)(i) If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with § 164.512(i) for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:
(A) The name of the protocol or other research activity;
(B) A description, in plain language, of the research protocol or other research activity, including the purpose of the

research and the criteria for selecting particular records;
(C) A brief description of the type of protected health information that was disclosed;
(D) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
(E) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
(F) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.
(ii) If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.
(c) *Implementation specifications: provision of the accounting.*
(1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.
(i) The covered entity must provide the individual with the accounting requested; or
(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:
(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and
(B) The covered entity may have only one such extension of time for action on a request for an accounting.
(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.
(d) *Implementation specification: documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):
(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;
(2) The written accounting that is provided to the individual under this section; and
(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

§ 164.530 Administrative requirements. (a)(1) *Standard: personnel designations.*
(i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.
(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.
(2) *Implementation specification: personnel designations.* A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.
(b)(1) *Standard: training.* A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.
(2) *Implementation specifications: training.*
(i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:
(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;
(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and
(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.
(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.
(c)(1) *Standard: safeguards.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.
(2) *Implementation specification: safeguards.*
(i) A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.
(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.
(d)(1) *Standard: complaints to the covered entity.* A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of this subpart.
(2) *Implementation specification: documentation of complaints.* As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.
(e)(1) *Standard: sanctions.* A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that

meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.
(2) *Implementation specification: documentation.* As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.
(f) *Standard: mitigation.* A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.
(g) *Standard: refraining from intimidating or retaliatory acts.* A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:
(1) *Individuals.* Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section;
(2) *Individuals and others.* Any individual or other person for:
(i) Filing of a complaint with the Secretary under subpart C of part 160 of this subchapter;
(ii) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or
(iii) Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.
(h) *Standard: waiver of rights.* A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter or this subpart as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.
(i)(1) *Standard: policies and procedures.* A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.
(2) *Standard: changes to policies or procedures.*
(i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart;
(ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or
(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.
(3) *Implementation specification: changes in law.* Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.
(4) *Implementation specifications: changes to privacy practices stated in the notice.*
(i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:
(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;
(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and
(C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.
(ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:
(A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)-(C) of this section; and
(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.
(5) *Implementation specification: changes to other policies or procedures.* A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:
(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and
(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.
(j)(1) *Standard: documentation.* A covered entity must:
(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;
(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and
(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action,

activity, or designation.
(2) *Implementation specification: retention period.* A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.
(k) *Standard: group health plans.*
(1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:
(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and
(ii) The group health plan does not create or receive protected health information, except for:
(A) Summary health information as defined in § 164.504(a); or
(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.
(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).

§ 164.532 Transition provisions.
(a) *Standard: Effect of prior authorizations.* Notwithstanding §§ 164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, or a waiver of informed consent by an IRB.
(b) *Implementation specification: Effect of prior authorization for purposes other than research.* Notwithstanding any provisions in § 164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this subpart, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with § 164.522(a).
(c) *Implementation specification: Effect of prior permission for research.* Notwithstanding any provisions in §§ 164.508 and 164.512(i), a covered entity may, to the extent allowed by one of the following permissions, use or disclose, for research, protected health information that it created or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with § 164.522(a), and the covered entity has obtained, prior to the applicable compliance date, either:
(1) An authorization or other express legal permission from an individual to use or disclose protected health information for the research;
(2) The informed consent of the individual to participate in the research; or
(3) A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with § 164.508 if, after the compliance date, informed consent is sought from an individual participating in the research.
(d) *Standard: Effect of prior contracts or other arrangements with business associates.* Notwithstanding any other provisions of this subpart, a covered entity, other than a small health plan, may disclose protected health information to a business associate and may allow a business associate to create, receive, or use protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§ 164.502(e) and 164.504(e) consistent with the requirements, and only for such time, set forth in paragraph (e) of this section.
(e) *Implementation specification: Deemed compliance.*
(1) *Qualification.* Notwithstanding other sections of this subpart, a covered entity, other than a small health plan, is deemed to be in compliance with the documentation and contract requirements of §§ 164.502(e) and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:
(i) Prior to October 15, 2002, such covered entity has entered into and is operating pursuant to a written contract or other written arrangement with a business associate for such business associate to perform functions or activities or provide services that make the entity a business associate; and
(ii) The contract or other arrangement is not renewed or modified from October 15, 2002, until the compliance date set forth in § 164.534.
(2) *Limited deemed compliance period.* A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section, shall be deemed compliant until the earlier of:
(i) The date such contract or other arrangement is renewed or modified on or after the compliance date set forth in § 164.534; or
(ii) April 14, 2004.
(3) *Covered entity responsibilities.* Nothing in this section shall alter the requirements of a covered entity to comply with Part 160, Subpart C of this subchapter and §§ 164.524, 164.526, 164.528, and 164.530(f) with respect to protected health information held by a business associate.

§ 164.534 Compliance dates for initial implementation of the privacy standards. (a) *Health care providers.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 14, 2003.
(b) *Health plans.* A health plan must comply with the applicable requirements of this subpart no later than the following date, as applicable:
(1) *Health plans other than small health plans* – April 14, 2003.
(2) *Small health plans* – April 14, 2004.
(c) *Health care clearinghouses.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 14, 2003.

10. Key Resources and Forms

10.01 Covered Plans

10.02 Privacy Official

10.03 Other Contacts

10.04 Business Associate Agreements

10.05 Insurers

10.06 Plan Sponsor Documentation

10.07 Notice of Privacy Practices

10.08 Participant Forms

10.09 Documentation Logs

10.10 List of Legally Required Uses, Public Health Activities, Other Situations not Requiring Authorization

10.11 License Agreement for HIPAA Compliance Requests Database

10. Key Resources and Forms

10.01 Covered Plans

10.02 Privacy Official

10.03 Other Contacts

10.04 Business Associate Agreements

10.05 Insurers

10.06 Plan Sponsor Documentation

10.07 Notice of Privacy Practices

10.08 Participant Forms

10.09 Documentation Logs

10.10 List of Legally Required Uses, Public Health Activities, Other Situations not Requiring Authorization

10.11 License Agreement for HIPAA Compliance Requests Database

10.01 Covered Plans

The Board of Trustees sponsors through Everett School Employee Benefit Trust the following HIPAA covered benefit options:

- Preferred Provider Organizations/First Choice Health Network
- Flexible Spending Accounts

10.02 Privacy Official

a. Privacy Official Designation

The following person is designated as the Privacy Official:

Name:	Molly Ringo
Address:	3715 Oakes Avenue, Everett, Washington 98201
Phone:	(425) 388-4716
Fax:	(425) 388-4713
Email:	Mringo@everett.wednet.edu
Other relevant contact information:	Privacy Official Designee is Dottie Cainion, Benefits Supervisor, (425) 388-4722

b. Sample Privacy Official Job Description

The Privacy Official shall be responsible for coordinating employer's policies and procedures under HIPAA's privacy rules, as revised from time-to-time, monitoring compliance with those rules, and making decisions with respect to any issues that arise under such rules. The Privacy Official shall report to the Superintendent.

c. Essential Duties - General

- *Serve as the leader of Everett School Employee Benefit Trust's HIPAA privacy workgroup and focal point for privacy compliance-related activities*
- *Implement HIPAA privacy policies and procedures for Everett School Employee Benefit Trust's group health plan arrangement*
- *Assist in the interpretation of the state and federal privacy rules and act as the designated decision-maker for issues and questions, in coordination with legal counsel*
- *Oversee training programs*
- *Ensure compliance with privacy practices and consistent application of sanctions for failure to comply within employer's workforce and all Business Associates, in cooperation with human resources, administration, and legal counsel as applicable*
- *Audit and administer privacy program reviews*
- *Serve as internal and external liaison and resource between the employer group health plan and other entities (employer's officers, vendors, Office of Civil Rights, other legal entities) for purposes of any compliance reviews or investigations and to ensure that employer's privacy practices are implemented, consistent, and coordinated*
- *Periodically revise the HIPAA privacy policies and procedures in light of changes to the rules, or changes in group health plan practices or in the flow of PHI*

d. Essential Duties – Specific

- *Develop a procedure to inventory and document the uses and disclosures of protected health information (PHI)*
- *Assist in the development, implementation, negotiation, and compliance monitoring of Business Associate contracts to ensure all privacy concerns, requirements, and responsibilities are addressed*
- *Develop and implement overall privacy policies and procedures as applicable for the employer group health plan arrangement*
- *Develop and implement appropriate firewalls between employer functions and the functions of the group health plan arrangement*
- *Draft and distribute the HIPAA privacy notice*
- *Appoint or serve as the designated contact person in the privacy notice and receive questions and complaints related to the protection of PHI, participant privacy, and violations of employer's privacy procedures*
- *Establish mechanisms and monitor processes to ensure participants' rights to restrict, amend, have access to, and receive an accounting of their health information*
- *Establish and administer a process to receive, document, track, investigate, and take action (including developing sanctions) on all complaints regarding employer's privacy policies and procedures*
- *Ensure that employer develops and maintains appropriate privacy authorization forms*
- *Ensure that amendments to plan documents are addressed*
- *Ensure that all documentation required by the privacy rule is maintained and retained for six (6) years from the date it was created or was last in effect, whichever is later*
- *Oversee and ensure delivery of privacy training and orientation to staff*
- *Establish programs to audit and monitor Business Associates*

- *Monitor changes to the HIPAA privacy and security rules, including federal and state laws and regulations*

- *Establish programs to audit and monitor internal privacy compliance, perform initial and periodic privacy risk assessments, and conduct related ongoing compliance monitoring activities*

- *Review system-related information security plans as necessary throughout employer's network to ensure alignment between security and privacy practices, and act as a liaison to the information systems department*

The Privacy Official shall have the sole authority and discretion to delegate the above tasks or portions thereof to other individuals within employer or to consultants, contractors or other specialists, as appropriate, provided that the Privacy Official monitors such activities in good faith for purposes of achieving compliance with HIPAA.

10.03 Other Contacts

The following is a list of key contacts (persons or offices) responsible for responding to Participants exercising their rights described in Section 5; for receiving complaints concerning 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.

- Inspection Contact

Name:	Human Resources – Benefits Department
Address:	3715 Oakes Avenue, Everett, WA 98201
Phone:	(425) 388-4710
Fax:	(425) 388-4713
Email:	

- Amendment Contact

Name:	Human Resources – Benefits Department
Address:	3715 Oakes Avenue, Everett, WA 98201
Phone:	(425) 388-4710
Fax:	(425) 388-4713
Email:	

- Restriction Contact

Name:	Human Resources – Benefits Department
Address:	3715 Oakes Avenue, Everett, WA 98201
Phone:	(425) 388-4710
Fax:	(425) 388-4713
Email:	

- Communications Contact

Name:	Human Resources – Benefits Department
Address:	3715 Oakes Avenue, Everett, WA 98201
Phone:	(425) 388-4710
Fax:	(425) 388-4713
Email:	

- Disclosure Contact

Name:	Human Resources – Benefits Department
Address:	3715 Oakes Avenue, Everett, WA 98201
Phone:	(425) 388-4710
Fax:	(425) 388-4713
Email:	

- Complaint Manager

Name:	Human Resources – Benefits Department
Address:	3715 Oakes Avenue, Everett, WA 98201
Phone:	(425) 388-4710
Fax:	(425) 388-4713
Email:	

- Authorization Contact

Name:	Human Resources – Benefits Department
Address:	3715 Oakes Avenue, Everett, WA 98201
Phone:	(425) 388-4710
Fax:	(425) 388-4713
Email:	

10.04 Business Associate Agreements

a. Model Business Associate Agreement

Directions to the Plan's Administrator for Using Model Business Associate Agreement

General Comments. This model HIPAA Business Associate Agreement is designed to be an addendum to an existing contract between Everett School Employee Benefit Trust and its third party vendor. It should be modified if it will be used as a stand-alone contract (i.e., there is no existing contract), or for insertion into the body of a contract.

Select Instructions:

Section 3.0(b). This section is optional. Most vendors will likely request the authority to engage in the specific uses and disclosures discussed therein.

Section 4.0(a) and (b). The Plan's Administrator will need to modify this subsection if it delegated to the Business Associate its obligation to produce and provide Privacy Notices.

Section 6.0(a). For written contracts (i) in effect before October 15, 2002, and (ii) not renewed or modified before April 14, 2003, Everett School Employee Benefit Trust has until the earlier of the date of renewal or modification, or April 14, 2004, to amend such contracts. If conditions (i) and (ii) are not satisfied, then the contract must be amended by April 14, 2003.

Section 7.0(f). Conform this section to the existing contract with this vendor unless that contract does not specify the law of which state will govern the contract.

Section 7.0(g). Modify this section if the existing contract does not include any provision regarding indemnification or performance guarantees, or if application of those provisions requires additional statements in this section.

SAMPLE HIPAA PRIVACY BUSINESS ASSOCIATE AGREEMENT

This Agreement is entered into this _____ day of _____, _____, between **the Board of Trustees (Plan Sponsor), acting on behalf of Everett School Employee Benefit Trust** (the "Plan") and **[Name of Vendor]** ("Business Associate"). The Agreement is incorporated into the **[Name of Vendor Contract]** between the Plan and Business Associate, dated **[Date of Contract]** (the "Contract"). The parties intend to use this Amendment to satisfy the Business Associate contract requirements in the regulations at 45 CFR 164.502(e) and 164.504(e), issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

1.0 Definitions

Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in 45 CFR 160.103 and 164.501. Notwithstanding the above, "Covered Entity" shall mean **[Name of Covered Entity/Plan]**; "Individual" shall have the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g); "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his designee; and "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

2.0 Obligations and Activities of Business Associate

(a) Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by Section 3.0 of this Agreement, or as Required by Law.

(b) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

(c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

(d) Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

(e) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

(f) Business Associate agrees to provide access, at the request of Covered Entity or an Individual, and in a prompt and reasonable manner consistent with the HIPAA regulations, to Protected Health Information in a Designated Record Set, to the Covered Entity or directly to an Individual in order to meet the requirements under 45 CFR 164.524.

(g) Business Associate agrees to make any Amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity or an Individual directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in a prompt and reasonable manner consistent with the HIPAA regulations.

(h) Business Associate agrees to make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity, to the Secretary in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

(i) Business Associate agrees to document disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

(j) Business Associate agrees to provide to Covered Entity or an Individual an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528, in a prompt and reasonable manner consistent with the HIPAA regulations.

(k) Business Associate agrees to satisfy all applicable provisions of HIPAA standards for electronic transactions and code sets, also known as the Electronic Data Interchange (EDI) Standards, at 45 CFR Part 162 no later than October 16, 2003. Business Associate further agrees to ensure that any agent, including a subcontractor, that conducts standard transactions on its behalf will comply with the EDI Standards.

(l) Business Associate agrees to determine the Minimum Necessary type and amount of PHI required to perform its services and will comply with 45 CFR 164.502(b) and 514(d).

3.0 Permitted or Required Uses and Disclosures by Business Associate

(a) General Use and Disclosure. Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Contract and

in this Agreement, provided that such use or disclosure of Protected Health Information would not violate the Privacy Rule, including the Minimum Necessary requirement, if done by Covered Entity. **[If not specified in the Contract, consider adding provisions clearly obligating Business Associate to share Protected Health Information for permitted purposes, such as for audits performed by Business Associates or Everett School Employee Benefit Trust.]**

(b) Additional use and disclosure.

(i) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(ii) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that such disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(iii) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR 164.504(e)(2)(i)(B).

(iv) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

4.0 Obligations of Covered Entity to Inform Business Associate of Covered Entity's Privacy Practices, and any Authorization or Restrictions.

(a) Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

(b) Covered Entity shall provide Business Associate with any changes in, or revocation of, Authorization by Individual or his or her personal representative to use or disclose Protected Health Information, if such changes affect Business Associate's uses or disclosures of Protected Health Information.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, if such changes affect Business Associate's uses or disclosures of Protected Health Information.

5.0 Permissible Requests by Covered Entity.

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

6.0 Term and Termination

(a) *Term.* The Term of this Agreement shall be effective as of April 14, 2003 **[there may be a different date depending on when Everett School Employee Benefit Trust renews it's contract],** and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

(b) *Termination for Cause.* Without limiting the termination rights of the parties pursuant to the Contract, and upon Covered Entity's knowledge of a material breach by Business Associate of a provision under this Agreement, Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Contract if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, or immediately terminate the Contract if Business Associate has breached a material term of this Agreement and cure is not possible. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

(c) *Effect of Termination.* The parties mutually agree that it is essential for Protected Health Information to be maintained after the expiration of the Agreement for regulatory and other business reasons. The parties further agree that it would be infeasible for Covered Entity to maintain such records because Covered Entity lacks the necessary system and expertise. Accordingly, Covered Entity hereby appoints Business Associate as its custodian for the safe keeping of any record-containing Protected Health Information that Business Associate may determine it is appropriate to retain. Notwithstanding the expiration or termination of the Contract, Business Associate shall extend the protections of this Addendum to such Protected Health Information, and limit further use or disclosure of the Protected Health Information to those purposes that make the return or destruction of the Protected Health Information infeasible.

7.0 Miscellaneous

(a) *Regulatory References.* A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended, and for which compliance is required.

(b) *Amendment.* Upon the enactment of any law or regulation affecting the use or disclosure of Protected Health Information, or the publication of any decision of a court of the United States or any state relating to any such law or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, either party may, by written notice to the other party, amend the Contract and this Agreement in such manner as such party determines necessary to comply with such law or regulation. If the other party disagrees with such Amendment, it shall so notify the first party in writing within thirty (30) days of the notice. If the parties are unable to agree on an Amendment within thirty (30) days thereafter, then either of the parties may terminate the Contract on thirty (30) days written notice to the other party. **[May be modified to fit parties' wishes.]**

(c) *Survival.* The respective rights and obligations of Business Associate under Section 6.0 of this Agreement shall survive the termination of this Addendum.

(d) *Interpretation.* Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rule.

(e) *No third party beneficiary.* Nothing expressed or implied in this Agreement or in the Contract is intended to confer, nor shall anything herein confer, upon any person other than the parties and the respective successors or assignees of the parties, any rights, remedies, obligations, or liabilities whatsoever.

(f) *Governing Law.* This Agreement shall be governed by and construed in accordance with the laws of the state of aWashington to the extent not preempted by the Privacy Rules or other applicable federal law.

(g) *Indemnification and performance guarantees.* The indemnification and performance guarantee provisions contained in the Contract shall also apply to this Agreement.

By:_____
Chairperson, Board of Trustees on behalf of
Everett School Employee Benefit Trust

By:_____
[Name of Vendor]

b. Log of Business Associate Agreements

Vendor name	Agreement date	Expiration date	Storage location	Description of agreement (including Plan names)
Everett School District No. 2	April 14, 2003	Evergreen	Human Resources Benefits Department	Requires all HIPAA compliance as outlined under HIPAA privacy requirements.
Flex-Plan Services, Inc.	April 14, 2003	Evergreen	Human Resources Benefits Department	Requires all HIPAA compliance as outlined under HIPAA privacy requirements.
Mercer Human Resources Consulting	April 14, 2003	Evergreen	Human Resources Benefits Department	Requires all HIPAA compliance as outlined under HIPAA privacy requirements.
Safeco	April 14, 2003	Evergreen	Human Resources Benefits Department	Requires all HIPAA compliance as outlined under HIPAA privacy requirements.
Margaret Templeton	April 14, 2003	Evergreen	Human Resources Benefits Department	Requires all HIPAA compliance as outlined under HIPAA privacy requirements.
Zenith Administrators	April 14, 2003	Evergreen	Human Resources Benefits Department	Requires all HIPAA compliance as outlined under HIPAA privacy requirements.

10.05 Insurers

The following is a list of the Plan(s) Insurers:

Insurer	Policy identifying information	Storage location
Ceridian Corporation (EAP LifeBalance Program)	Services Agreement	Copy of Agreement held in Human Resources
Willamette Dental of Washington (formerly Columbia Dental Plan)	Group Plan #W002	Copy of Policy held in Human Resources
Group Health Corporation	Group Plan #0026100	Copy of Policy held in Human Resources
PacifiCare HMO	Group Plan #804139	Copy of Policy held in Human Resources
UNUM (Long Term Care Program)	Policy #220302	
Washington Dental Service	Group Plan #0186	Copy of Policy held in Human Resources

10.06 Plan Sponsor Documentation

a. Amendment to Existing Plan Documents

Instructions for Completing Plan Amendment

General & Introductory Paragraphs. In order to receive PHI from a HIPAA covered plan, the Board of Trustees will need to amend the Plan Document to comply with HIPAA's Privacy requirements and certify to the Plan that the appropriate Amendments have been made. The process for amending each plan will usually be described in the document creating the Plan.

Selected Line Instructions

1. If Everett School Employee Benefit Trust sponsors one (1) or more small group health plans in addition to other covered plans, a separate Amendment might be appropriate as an alternative to stating a separate effective date for the small plan Amendment.

2.a. & b. Refer to Section 4.03 to determine the extent to which Everett School Employee Benefit Trust's Plan administrative activities should be described. (Note that changes to these provisions should be reflected in the Notice of Privacy Practices.)

5.i.(1) Refer to Section 4.03 for a description of persons that may have access to PHI. This description may need to distinguish among various plans if the persons with access to PHI vary by plan.

5.i.(3) Coordinate disciplinary measures with those in Section 6.04 .

HIPAA PRIVACY
MASTER GROUP HEALTH PLAN AMENDMENT
FOR GROUP HEALTH PLANS OF
EVERETT SCHOOL EMPLOYEE BENEFIT TRUST

WHEREAS, the Health Insurance Portability and Accountability Act of 1996, ("HIPAA"), and the regulations issued thereunder at 45 CFR Parts 160 and 164 ("the HIPAA regulations"), impose privacy obligations on group health plans that restrict the use and disclosure of protected health information ("PHI");

WHEREAS, the Board of Trustees sponsors and maintains the following group health plans that are subject to the HIPAA regulations: Preferred Provider Organizations/First Choice Health Network and Flexible Spending Accounts;

WHEREAS, the Plan's Administrator representing the Plan intend to receive PHI from the Plan (including its Business Associates, health insurance issuers, HMOs, and their agents) from time to time;

WHEREAS, the HIPAA regulations require Board of Trustees to amend the Plan to incorporate provisions specified in 45 CFR 164.504(f)(2) prior to the receipt of such PHI; and

WHEREAS, Chairperson of Board of Trustees is authorized on behalf of the Plans offered by Everett Public School Employee Benefit Trust to approve Amendments to the Plan;

NOW, THEREFORE, each respective Plan is hereby amended, as set forth below, to implement appropriate protections required under the HIPAA regulations.

1. **Effective Date**. This Amendment is effective as of April 14, 2003.

2. **Uses and Disclosures of PHI.** The Plan's Administrator may disclose a Plan Participant's PHI to Everett School Employee Benefit Trust and Business Associate(s) for the following Plan administration functions under 45 CFR 164.504(a), to the extent not inconsistent with the HIPAA regulations:

   - Identify the classes of employees with access to PHI and the categories of information they will use;
   - Make reasonable efforts to limit disclosures of and requests for PHI to the Minimum Necessary to accomplish the intended purpose;
   - Maintain procedures governing the storage of PHI; and
   - If feasible, return or destroy PHI received from the Plan, and maintain procedures governing the retention and destruction of PHI not returned or destroyed.

3. **Restriction on Plan Disclosure to Everett School Employee Benefit Trust.** Neither the Plan nor any of its Business Associates, health insurance issuers, or HMOs, will disclose

PHI to the Plan except upon receipt of Everett School Employee Benefit Trust certification that the Plan has been amended to incorporate the agreements of Everett School Employee Benefit Trust under paragraph 4, except as otherwise permitted or required by law.

4. **Privacy Agreements of Everett School Employee Benefit Trust.** As a condition for obtaining PHI from the Plan, its Business Associates, Insurers, and HMOs, the Plan's Administrator agrees it will:

   a. Not use or further disclose such PHI other than as permitted by paragraph 2 of this Amendment, as permitted by 45 CFR 164.508, 45 CFR 164.512, and other sections of the HIPAA regulations, or as required by law;

   b. Ensure that any of its agents, including a subcontractor, to whom it provides the PHI agree to the same restrictions and conditions that apply to the Plan with respect to such information;

   c. Not use or disclose the PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of Everett School Employee Benefit Trust;

   d. Report to the Plan any use or disclosure of the PHI that is inconsistent with the uses or disclosures provided for of which the Plan's Administrator becomes aware;

   e. Make the PHI of a particular Participant available for purposes of the Participant's requests for inspection, copying, and Amendment, and carry out such requests in accordance with HIPAA regulation 45 CFR 164.524 and 164.526;

   f. Make the PHI of a particular Participant available for purposes of required accounting of disclosures by Everett School Employee Benefit Trust pursuant to the Participant's request for such an accounting in accordance with HIPAA regulation 45 CFR §164.528;

   g. Make Everett School Employee Benefit Trust's internal practices, books, and records relating to the use and disclosure of PHI received from the Plan available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining compliance by the Plan with HIPAA;

   h. If feasible, return or destroy all PHI received from the Plan that the Plan's Administrator 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, Everett School Employee Benefit Trust agrees to limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

i. Ensure that there is adequate separation between the Plan and the Plan's Administrator by implementing the terms of subparagraphs 5.i. (1) through (3), below:

(1) *Employees With Access to PHI*: Trustees working with appeals and designated employees in Human Resources, Information Systems and Technology and Payroll are the only individuals that may access PHI received from the Plan.

(2) *Use Limited to Plan Administration*: The access to and use of PHI by the individuals described in (1), above, is limited to Plan Administration functions as defined in HIPAA regulation 45 CFR §164.504(a) that are performed by the Plan's Administrator for the Plan.

(3) *Mechanism for Resolving Noncompliance*. If the Plan's Administrator or person(s) responsible for monitoring compliance determines that any person described in (1), above, has violated any of the restrictions of this Amendment, then such individual shall be disciplined in accordance with the policies of Everett School Employee Benefit Trust established for purposes of privacy compliance, up to and including dismissal from employment. The Plan's Administrator shall arrange to maintain records of such violations along with the persons involved, as well as disciplinary and corrective measures taken with respect to each incident.

5. **PHI not Subject to this Amendment**. Notwithstanding the foregoing, the terms of this Amendment shall not apply to uses or disclosures of Enrollment, Disenrollment, and Summary Health Information made pursuant to 45CFR 164.504 (f)(l)(ii) or (iii); of PHI released pursuant to an Authorization that complies with 45 CFR 164.508; or in other circumstances as permitted by the HIPAA regulations.

6. **Definitions.** All capitalized terms within this Amendment not otherwise defined by the provisions of this Amendment shall have the meaning given them in the respective Plan or, if no other meaning is provided in the Plan, the term shall have the meaning provided under HIPAA.

7. **Copies Effective as Originals.** A copy of the signed and dated original of this Amendment shall be as effective as the original, and either an original or such copy shall be appended to the governing instruments of each Plan and shall be deemed to be a part of such governing instruments.

IN WITNESS WHEREOF, this Amendment was executed by the following duly authorized individual on behalf of Everett School Employee Benefit Trust this ___ day of _____, 2003.

Everett School Employee Benefit Trust

By: _____

_____

(print name)

Date: _____

Title: _____

SAMPLE
PLAN SPONSOR CERTIFICATION OF
HIPAA PRIVACY PLAN AMENDMENTS FOR
EVERETT SCHOOL EMPLOYEE BENEFIT TRUST
[GROUP HEALTH PLAN]

The undersigned duly authorized representative of the Board of Trustees, Plan Sponsor of the Everett School Employee Benefit Trust (the "Plan"), certifies by this instrument that the Plan was amended, effective **[date HIPAA Privacy Amendment was effective for Plan],** by adoption of the "HIPAA Privacy Master Group Health Plan Amendment for Group Health Plans of Everett School Employee Benefit Trust" attached to this certificate. The undersigned further certifies that Everett School Employee Benefit Trust agrees to the provisions in such Amendment.

Everett School Employee Benefit Trust

By: _____

_____
(print name)

Date: _____

Title: _____

(Plan Amendment attached)

b. Certification

Instructions for Completing Plan Sponsor Certification
General. Everett School Employee Benefit Trust may choose to provide a brief certificate (the "Alternative Form") that references Everett School Employee Benefit Trust's detailed HIPAA Privacy Amendment.
Certain vendors will require a complete copy of the HIPAA Privacy Amendment. If so, the "Alternative Form" may be the more appropriate form to use because attached will be a copy of the complete HIPAA Privacy Plan Amendment, as adopted. If Everett School Employee Benefit Trust uses the Alternative Form, it should consider whether any provisions of the Amendment are inappropriate to furnish to the particular vendor. **[Bracketed text]** — Each form of certificate contains bracketed text indicating where information should be specific to Everett School Employee Benefit Trust.

10.07 Notice of Privacy Practices

Instructions for Privacy Notice

This sample was designed as a joint Privacy Notice for all group health plan self-insured benefits. If appropriate, indicate which components of the plans are covered by this notice (self-funded? insured? which options?). Employers may choose to send multiple notices for different benefits, in which case the notices should be modified accordingly.

Note that if a use or disclosure is prohibited or materially limited by another law — e.g., a more stringent state law — the notice must reflect the more stringent requirements (45 CFR 164.520(b)(1)(ii)).

The notice must describe how the individual may exercise each individual right and should indicate where to submit requests (e.g., Plan Contact, Insurer, Business Associate?).

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposes numerous requirements on employer health plans concerning the use and disclosure of individual health information. This information, known as protected health information, includes virtually all individually identifiable health information held by the Plan — whether received in writing, in an electronic medium, or as an oral communication. This notice describes the privacy practices of the following plans: Preferred Provider Organizations/First Choice Health Network and Flexible Spending Accounts. The plans covered by this notice may share health information with each other to carry out Treatment, Payment, or Health Care Operations. These plans are collectively referred to as the Plan in this notice, unless specified otherwise.

The Plan's duties with respect to health information about you

The Plan is required by law to maintain the privacy of your health information and to provide you with this notice of the Plan's legal duties and privacy practices with respect to your health information. If you participate in an insured plan option, you will receive a notice directly from the Insurer. It's important to note that these rules apply to the Plan, not Everett School District as an employer — that's the way the HIPAA rules work. Different policies may apply to other Everett School Employee Benefit Trust programs or to data unrelated to the health plan.

How the Plan may use or disclosure your health information

The privacy rules generally allow the use and disclosure of your health information without your permission (known as an authorization) for purposes of health care Treatment, Payment activities, and Health Care Operations. Here are some examples of what that might entail:

- **Treatment** includes providing, coordinating, or managing health care by one (1) or more health care providers or doctors. Treatment can also include coordination or management of care between a provider and a third party, and consultation and referrals between providers. *For example, the Plan may share health information about you with physicians who are treating you.*

- **Payment** includes activities by this Plan, other plans, or providers to obtain premiums, make coverage determinations and provide reimbursement for health care. This can include eligibility determinations, reviewing services for medical necessity or appropriateness, utilization management activities, claims management, and billing; as well as "behind the scenes" plan functions such as risk adjustment, collection, or reinsurance. *For example, the Plan may share information about your coverage or the*

expenses you have incurred with another health plan in order to coordinate payment of benefits.

- **Health care operations** include activities by this Plan (and in limited circumstances other plans or providers) such as wellness and risk assessment programs, quality assessment and improvement activities, customer service, and internal grievance resolution. Health care operations also include vendor evaluations, credentialing, training, accreditation activities, underwriting, premium rating, arranging for medical review and audit activities, and business planning and development. *For example, the Plan may use information about your claims to review the effectiveness of wellness programs.*

The amount of health information used or disclosed will be limited to the "Minimum Necessary" for these purposes, as defined under the HIPAA rules. The Plan may also contact you to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you.

How the Plan may share your health information with Everett School Employee Benefit Trust

The Plan, or its health insurer or HMO, may disclose your health information without your written authorization to Everett School Employee Benefit Trust for plan administration purposes. Everett School Employee Benefit Trust may need your health information to administer benefits under the Plan. Everett School Employee Benefit Trust agrees not to use or disclose your health information other than as permitted or required by the Plan documents and by law. Trustees working with appeals and designated employees in Human Resources, Information Systems and Technology and Payroll are the only Everett School Employee Benefit Trust employees who will have access to your health information for plan administration functions.

Here's how additional information may be shared between the Plan and Everett School Employee Benefit Trust, as allowed under the HIPAA rules:

- The Plan, or its Insurer or HMO, may disclose "summary health information" to Everett School Employee Benefit Trust if requested, for purposes of obtaining premium bids to provide coverage under the Plan, or for modifying, amending, or terminating the Plan. Summary health information is information that summarizes participants' claims information, but from which names and other identifying information have been removed.

- The Plan, or its Insurer or HMO, may disclose to Everett School Employee Benefit Trust information on whether an individual is participating in the Plan, or has enrolled or disenrolled in an insurance option or HMO offered by the Plan.

In addition, you should know that Everett School Employee Benefit Trust cannot and will not use health information obtained from the Plan for any employment-related actions. However,

health information collected by Everett School Employee Benefit Trust from other sources, for example under the Family and Medical Leave Act, Americans with Disabilities Act, or workers' compensation is *not* protected under HIPAA (although this type of information may be protected under other federal or state laws).

Other allowable uses or disclosures of your health information

In certain cases, your health information can be disclosed without authorization to a family member, close friend, or other person you identify who is involved in your care or payment for your care. Information describing your location, general condition, or death may be provided to a similar person (or to a public or private entity authorized to assist in disaster relief efforts). You'll generally be given the chance to agree or object to these disclosures (although exceptions may be made, for example if you're not present or if you're incapacitated). In addition, your health information may be disclosed without authorization to your legal representative.

The Plan also is allowed to use or disclose your health information without your written authorization for the following activities:

Workers' compensation	Disclosures to workers' compensation or similar legal programs that provide benefits for work-related injuries or illness without regard to fault, as authorized by and necessary to comply with such laws
Necessary to prevent serious threat to health or safety	Disclosures made in the good-faith belief that releasing your health information is necessary to prevent or lessen a serious and imminent threat to public or personal health or safety, if made to someone reasonably able to prevent or lessen the threat (including disclosures to the target of the threat); includes disclosures to assist law enforcement officials in identifying or apprehending an individual because the individual has made a statement admitting participation in a violent crime that the Plan reasonably believes may have caused serious physical harm to a victim, or where it appears the individual has escaped from prison or from lawful custody
Public health activities	Disclosures authorized by law to persons who may be at risk of contracting or spreading a disease or condition; disclosures to public health authorities to prevent or control disease or report child abuse or neglect; and disclosures to the Food and Drug Administration to collect or report adverse events or product defects
Victims of abuse, neglect, or domestic violence	Disclosures to government authorities, including social services or protected services agencies authorized by law to receive reports of abuse, neglect, or domestic violence, as required by law or if you agree or the Plan believes that disclosure is necessary to prevent serious harm to you or potential victims (you'll be notified of the Plan's disclosure if informing you won't put you at further risk)
Judicial and administrative proceedings	Disclosures in response to a court or administrative order, subpoena, discovery request, or other lawful process (the Plan may be required to notify you of the request, or receive satisfactory assurance from the party seeking your health information that efforts were made to notify you or to obtain a qualified protective order concerning the information)
Law enforcement purposes	Disclosures to law enforcement officials required by law or pursuant to legal process, or to identify a suspect, fugitive, witness, or missing person; disclosures about a crime victim if you agree or if disclosure is necessary for immediate law enforcement activity; disclosure about a death that may have resulted from criminal conduct; and disclosure to provide evidence of criminal conduct on the Plan's premises

Decedents	Disclosures to a coroner or medical examiner to identify the deceased or determine cause of death; and to funeral directors to carry out their duties
Organ, eye, or tissue donation	Disclosures to organ procurement organizations or other entities to facilitate organ, eye, or tissue donation and transplantation after death
Research purposes	Disclosures subject to approval by institutional or private privacy review boards, and subject to certain assurances and representations by researchers regarding necessity of using your health information and treatment of the information during a research project
Health oversight activities	Disclosures to health agencies for activities authorized by law (audits, inspections, investigations, or licensing actions) for oversight of the health care system, government benefits programs for which health information is relevant to beneficiary eligibility, and compliance with regulatory programs or civil rights laws
Specialized government functions	Disclosures about individuals who are Armed Forces personnel or foreign military personnel under appropriate military command; disclosures to authorized federal officials for national security or intelligence activities; and disclosures to correctional facilities or custodial law enforcement officials about inmates
HHS investigations	Disclosures of your health information to the Department of Health and Human Services (HHS) to investigate or determine the Plan's compliance with the HIPAA privacy rule

Except as described in this notice, other uses and disclosures will be made only with your written authorization. You may revoke your authorization as allowed under the HIPAA rules. However, you can't revoke your authorization if the Plan has taken action relying on it. In other words, you can't revoke your authorization with respect to disclosures the Plan has already made.

Your individual rights

You have the following rights with respect to your health information the Plan maintains. These rights are subject to certain limitations, as discussed below. This section of the notice describes how you may exercise each individual right. See the table at the end of this notice for information on how to submit requests.

Right to request restrictions on certain uses and disclosures of your health information and the Plan's right to refuse

You have the right to ask the Plan to restrict the use and disclosure of your health information for Treatment, Payment, or Health Care Operations, except for uses or disclosures required by law. You have the right to ask the Plan to restrict the use and disclosure of your health information to family members, close friends, or other persons you identify as being involved in your care or payment for your care. You also have the right to ask the Plan to restrict use and disclosure of health information to notify those persons of your location, general condition, or death — or to coordinate those efforts with entities assisting in disaster relief efforts. If you want to exercise this right, your request to the Plan must be in writing.

The Plan is not required to agree to a requested restriction. And if the Plan does agree, a restriction may later be terminated by your written request, by agreement between you and the Plan (including an oral agreement), or unilaterally by the Plan for health information created

or received after you're notified that the Plan has removed the restrictions. The Plan may also disclose health information about you if you need emergency treatment, even if the Plan has agreed to a restriction.

Right to receive confidential communications of your health information

If you think that disclosure of your health information by the usual means could endanger you in some way, the Plan will accommodate reasonable requests to receive communications of health information from the Plan by alternative means or at alternative locations.

If you want to exercise this right, your request to the Plan must be in writing and you must include a statement that disclosure of all or part of the information could endanger you.

Right to inspect and copy your health information

With certain exceptions, you have the right to inspect or obtain a copy of your health information in a "Designated Record Set." This may include medical and billing records maintained for a health care provider; enrollment, payment, claims adjudication, and case or medical management record systems maintained by a plan; or a group of records the Plan uses to make decisions about individuals. However, you do not have a right to inspect or obtain copies of psychotherapy notes or information compiled for civil, criminal, or administrative proceedings. In addition, the Plan may deny your right to access, although in certain circumstances you may request a review of the denial.

If you want to exercise this right, your request to the Plan must be in writing Within 30 days of receipt of your request (60 days if the health information is not accessible onsite), the Plan will provide you with:

- The access or copies you requested;
- A written denial that explains why your request was denied and any rights you may have to have the denial reviewed or file a complaint; or
- A written statement that the time period for reviewing your request will be extended for no more than 30 more days, along with the reasons for the delay and the date ~~by~~ which the Plan expects to address your request.

The Plan may provide you with a summary or explanation of the information instead of access to or copies of your health information, if you agree in advance and pay any applicable fees. The Plan also may charge reasonable fees for copies or postage.

If the Plan doesn't maintain the health information but knows where it is maintained, you will be informed of where to direct your request.

Right to amend your health information that is inaccurate or incomplete

With certain exceptions, you have a right to request that the Plan amend your health information in a Designated Record Set. The Plan may deny your request for a number of reasons. For example, your request may be denied if the health information is accurate and complete, was not created by the Plan (unless the person or entity that created the information is no longer available), is not part of the Designated Record Set, or is not available for inspection (e.g., psychotherapy notes or information compiled for civil, criminal, or administrative proceedings).

If you want to exercise this right, your request to the Plan must be in writing, and you must include a statement to support the requested amendment. Within 60 days of receipt of your request, the Plan will:

- Make the amendment as requested;
- Provide a written denial that explains why your request was denied and any rights you may have to disagree or file a complaint; or
- Provide a written statement that the time period for reviewing your request will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Plan expects to address your request.

Right to receive an accounting of disclosures of your health information

You have the right to a list of certain disclosures the Plan has made of your health information. This is often referred to as an "accounting of disclosures." You generally may receive an accounting of disclosures if the disclosure is required by law, in connection with public health activities, or in similar situations listed in the table earlier in this notice, unless otherwise indicated below.

You may receive information on disclosures of your health information going back for six (6) years from the date of your request, but not earlier than April 14, 2003 (the general date that the HIPAA privacy rules are effective). You do not have a right to receive an accounting of any disclosures made:

- For Treatment, Payment, or Health Care Operations;
- To you about your own health information;
- Incidental to other permitted or required disclosures;
- Where authorization was provided;
- To family members or friends involved in your care (where disclosure is permitted without authorization);

- For national security or intelligence purposes or to correctional institutions or law enforcement officials in certain circumstances; or

- As part of a "limited data set" (health information that excludes certain identifying information).

In addition, your right to an accounting of disclosures to a health oversight agency or law enforcement official may be suspended at the request of the agency or official. If you want to exercise this right, your request to the Plan must be in writing. Within 60 days of the request, the Plan will provide you with the list of disclosures or a written statement that the time period for providing this list will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Plan expects to address your request. You may make one (1) request in any 12-month period at no cost to you, but the Plan may charge a fee for subsequent requests. You'll be notified of the fee in advance and have the opportunity to change or revoke your request.

Right to obtain a paper copy of this notice from the Plan upon request

You have the right to obtain a paper copy of this Privacy Notice upon request. Even individuals who agreed to receive this notice electronically may request a paper copy at any time.

Changes to the information in this notice

The Plan must abide by the terms of the Privacy Notice currently in effect. This notice takes effect on April 14, 2003. However, the Plan reserves the right to change the terms of its privacy policies as described in this notice at any time, and to make new provisions effective for all health information that the Plan maintains. This includes health information that was previously created or received, not just health information created or received after the policy is changed. If changes are made to the Plan's privacy policies described in this notice, you will be provided with a revised Privacy Notice via in-District mail or U.S. Mail.

Complaints

If you believe your privacy rights have been violated, you may complain to the Plan and to the Secretary of Health and Human Services. You won't be retaliated against for filing a complaint. To file a complaint, obtain a Complaint Form from the Complaint Manager by contacting the Everett Public Schools Human Resources Department.

Contact

For more information on the Plan's privacy policies or your rights under HIPAA, contact the Everett Public Schools, Human Resources Department.

10.08 Participant Forms

The following forms are included in this section:

10.08(a) Request for Access to Inspect and Copy

10.08(b) Request to Amend

10.08(c) Request for Restricted Use

10.08(d) Request for Confidential Communications

10.08(e) Request for Accounting of Non-Routine Disclosures

10.08(f) Authorization to Use and/or Disclosure

a. Request for Access to Inspect and Copy

Instructions for Responding to a Request for Access to Inspect and Copy

Directions for Plan's Administrator:

Providing Form. If any person wishes to request access to inspect and copy Personal health plan information, Inspection Contact should provide the person with this Form.

Receiving a Completed Form. Upon receipt of this Form Inspection Contact should initial and date top right corner and must verify that Part I (Request for Access to Inspect and Copy Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in sections A and B must be marked, and the form must be signed and dated. If the person requesting Personal health plan information is not the subject of the information, Inspection Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.

If Part I is incomplete, Inspection Contact should return it to the person for completion.

Determination of Request. Upon receipt of this Form with Part I properly completed, Inspection Contact will respond by completing Part II (Determination of Request for Access to Inspect and Copy Personal Health Plan Information, within the timeframes detailed in Section 5.02.

Note that although a Designated Record Set includes the Plan's enrollment and Payment information, it does not include Everett School Employee Benefit Trust's enrollment and Payment records.

Part I - Request for Access to Inspect and Copy Personal Health Plan Information

Form Received By _____ Date _____

With certain exceptions, you have the right to inspect or obtain a copy of your health information in a "Designated Record Set" maintained by the Everett School Employee Benefit Trust (the "Plan"). This may include medical and billing records maintained for a health care provider; enrollment, payment, claims adjudication, and case or medical management record systems maintained by a plan; or a group of records the Plan uses to make decisions about individuals. However, you do not have a right to inspect or obtain copies of psychotherapy notes or information compiled for civil, criminal, or administrative proceedings. In addition, the Plan may deny your right to access, although in certain circumstances you may request a review of the denial.

The Plan may provide you with a summary or explanation of the information in your health plan records instead of access to or copies of your records, if you agree in advance and pay any applicable fees. The Plan may also charge reasonable fees for copies or postage.

1. Employee Name:	**1a. Employee Health Plan ID Number:**
1b. Employee Date of Birth:	
2. Name of Person Whose Records You Are Requesting:	**2a. Relationship to Employee** Employee ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name:	**3a. Your Relationship to Person in Box 2** Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ **Other (please describe relationship):**
4. Mailing Address for Records:	**4a. City, State, Zip Code:**

Section A: Requested Personal Records.

Please identify the personal health plan information in your health plan records you are requesting access to, including the time period to which the information relates:

Section B: Methods of Access.

I wish to inspect and copy the personal health plan information described in Section A using the following method(s):

☐ I wish to inspect the records requested in Section A in person. I will arrange a mutually agreeable time to come to the Plan by contacting Human Resources – Benefits Department.

☐ I wish to copy the records requested in Section A in person. I will arrange a mutually agreeable time to come to the Plan by contacting Human Resources – Benefits Department. I understand that I will be charged and I agree to pay the cost of copying at _____ per page.

☐ I wish to have copies of the records requested in Section A sent directly to me, at the address in Box 4. I understand that I will be charged and I agree to pay the cost of copying at _____ per page plus postage.

☐ I wish to have the information requested in Section A summarized (instead of receiving the entire record) and sent to me at the address in Box 4. I understand that I will be charged for the summary provided and I agree to pay the cost of preparing the summary, any copying at _____ per page, and postage.

Please return completed form to: Human Resources – Benefits Department
3715 Oakes Avenue
Everett, WA 98201
(425) 388-4710

_____ _____

Signature **Date**

Part II – Determination of Request for Access to Inspect and Copy Personal Health Plan Records

Form Part II Prepared By	Date Part II Issued

After reviewing your request for access to inspect and/or copy personal health plan records, Inspection Contact has made the following determination [check one of the following]:

☐ Request granted (see Section A below).

☐ Request partially granted and partially denied (see Section A and B or C below).

☐ Request denied with no right to review (see Section B below).

☐ Request denied with right to review (see Section C below).

Section A: Request Granted

Your request for access to inspect and/or copy personal health plan records is granted in full / in part. All / Some of the health information you requested is available to you for inspection or copying, or both. If you requested to review the records in person, please contact Human Resources – Benefits Department at (425) 388-4710 to coordinate this request. If you requested that the records or a summary be sent to you, a copy is attached.

Section B: Request Denied with No Right to Review

Your request for access to inspect and copy personal health plan records is denied in full / in part for the following reasons [check all that apply]:

☐ The information requested is psychotherapy notes.

☐ The information is for civil, criminal, or administrative proceedings.

☐ The information is created for research and you agreed to forgo access while the research is in progress.

☐ The information was obtained from someone other than a health care provider under a promise of confidentiality and access would reveal the source.

☐ The information requested is not maintained by the Plan. Inspection Contact does not know who maintains the specific information requested.

☐ The information requested is not maintained by the Plan. The information is maintained by _____. Please contact them for access to the information.

Section C: Request Denied with Right to Review

Your request for access to inspect and/or copy personal health plan records has been denied in full / in part because a licensed health care professional has determined that the access is reasonably likely to endanger an individual. You have a right to ask the Plan to have the denial reviewed by another licensed health care professional.

If you wish to ask the Plan to review this denial, please send a written request to Human Resources – Benefits Department at 3715 Oakes Avenue, Everett, WA 98201. For more information, please contact Human Resources – Benefits Department at (425) 388-4710.

If you have been denied access to inspect and copy PHI, you may complain to the Plan or to the Secretary of the U.S. Department of Health and Human Services according to the procedures at http://www.hhs.gov/ocr/hipaa2.html For more information, please contact Human Resources – Benefits Department at (425) 388-4710.

Name of Plan Representative	Signature of Plan Representative	Date of Determination

b. Request to Amend

Instructions for Responding to a Request for Access to Inspect and Copy

Directions for the Plan's Administrator:

Providing Form. If any person wishes to request that the Plan amend his or her personal health plan information, Amendment Contact should provide the person with this Form.

Receiving a Completed Form. Upon receipt of this Form, Amendment Contact must verify that Part I (Request to Amend Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the Form must be signed and dated. If the person requesting personal health plan information is not the subject of the information, Amendment Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03

If Part I of the Form is incomplete, Amendment Contact should return it to the person for completion.

Determination of Request. Upon receipt of this Form with Part I properly completed, Amendment Contact will respond by completing Part II (Determination of Request to Amend Personal Health Plan Information), within the timeframes detailed in Section 5.03.

Part I - Request to Amend Personal Health Plan Information

Form Received By _____ Date _____

With certain exceptions, you have a right to request that the Plan amend your health information in a "Designated Record Set." The Plan may deny your request for a number of reasons. For example, your request may be denied if the health information is accurate and complete; was not created by the Plan (unless the person or entity that created the information is no longer available); is not part of the Designated Record Set; or would not be available for inspection (e.g., psychotherapy notes or information compiled for civil, criminal or administrative proceedings).

1. Employee Name:	**1a. Employee Health Plan ID Number:**
1b. Employee Date of Birth:	
2. Name of Person Whose Records You Are Requesting:	**2a. Relationship to Employee** Employee ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name:	**3a. Your Relationship to Person in Box 2** Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ **Other (please describe relationship):**
4. Mailing Address for Records:	**4a. City, State, Zip Code:**

I request that the Plan amend the following information in a personal health plan record [describe the information that is the subject of the Amendment request]:

_____

_____

_____

_____

The identified information should be amended because:

_____

_____

_____

I understand that if the Plan approves my request to amend a health plan record, the Plan will not necessarily delete the original information in the Designated Record Set, but instead may choose to identify the information in the Designated Record Set(s) that is the subject of my request for Amendment and provide a link to the location of the Amendment

_____ _____

Signature **Date**

Part II – Determination of Request to Amend Personal Health Plan Information

Form Part II Prepared By	Date Part II Issued

☐ Request Approved

☐ Request Denied for the following reasons [check all that apply]:

- ☐ The PHI or record was not created by the Plan.
- ☐ The PHI or record is not part of one of the Plan's Designated Record Sets.
- ☐ The PHI or record is not available for inspection under the HIPAA Privacy Rule.
- ☐ The PHI or record is accurate and complete referring.

If your request has been denied, you have the right to submit a statement of disagreement and the basis for such disagreement (limited to five (5) pages) to Human Resources – Benefits Department at 3715 Oakes Avenue, Everett, WA 98201. In response, Human Resources – Benefits Department will send you a copy of any rebuttal statement that is prepared. If you submit a statement of disagreement, when the Plan makes future disclosures of your disputed PHI or record, a copy of your request, the denial, and any disagreement and rebuttal will be attached to the disclosed PHI or record.

If your request has been denied and you choose not to submit a statement of disagreement, you may still ask the Plan to include a copy of your Amendment and the denial along with any future disclosures of the health information that is the subject of the Amendment request.

If you have been denied access to inspect and copy PHI, you may complain to the Plan or to the Secretary of the U.S. Department of Health and Human Services according to the procedures at http://www.hhs.gov/ocr/hipaa2.html For more information, please contact Human Resources – Benefits Department at (425) 388-4710.

Name of Plan Representative	Signature of Plan Representative	Date of Determination

c. Restricted Access

Instructions for Responding to a Request for Restricted Use of PHI

Directions for the Plan's Administrator:

Providing Form. If any person wishes to request that the Plan restrict or terminate a restriction on the Plan's use and disclosure of his or her PHI, Restriction Contact should provide the person with this Form.

Receiving a Completed Form. Upon receipt of this Form, Restriction Contact must verify that Part I (Request for Restricted Use Personal Heath Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the form must be signed and dated. If the person requesting the restricted use of PHI is not the subject of the PHI, Restrictions Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.

If Part I of the Form is incomplete, Restriction Contact should return it to the person for completion.

Determination of Request for Restricted Use of PHI. When Part I, Section A has been completed, Restriction Contact will respond by completing Part II (Determination of Request for Restricted Use of Personal Heath Plan Information), within the timeframes detailed in Section 5.04.

Terminating a Restriction. *Agreed Upon by a Participant (Part I, Section B).* When Part I, Section B, of the Form has been completed, Restriction Contact will not send a completed Part II (Determination of Request for Restricted Use of Personal Heath Plan Information), as detailed in Section 5.04.

Terminating a Restriction. *Not Agreed Upon by a Participant (Part III).* The Plan will only complete Part III of the Form to provide notice to a person (or the person's representative) that the Plan will terminate a previously agreed upon restriction, without the person's approval. The Plan will complete Part III on the original Form (where the restriction was requested and approved), as detailed in Section 5.04. Such restriction is effective only with respect to PHI created or received after the Plan has provided notice of the termination to the person.

Part I - Request for Restricted Use of Personal Health Plan Information

Form Received By _____ Date _____

You have the right to ask the Plan to restrict the use and disclosure of your health information for Treatment, Payment, or Health Care Operations, except for uses or disclosures required by law. You have the right to ask the Plan to restrict the use and disclosure of your health information to family members, close friends, or other persons you identify as being involved in your care or Payment for your care. You also have the right to ask the Plan to restrict use and disclosure of health information to notify those persons of your location, general condition, or death — or to coordinate those efforts with entities assisting in disaster relief efforts. If you want to exercise this right, your request to the Plan must be in writing.

The Plan is not required to agree to a requested restriction. And if the Plan does agree, a restriction may later be terminated by your written request, by agreement between you and the Plan (including an oral agreement), or unilaterally by the Plan for health information created or received after you're notified that the Plan has removed the restrictions. The Plan may also disclose health information about you if you need emergency Treatment, even if the Plan has agreed to a restriction.

1. Employee Name:	**1a. Employee Health Plan ID Number:**
1b. Employee Date of Birth:	
2. Name of Person Whose Records You Are Requesting:	**2a. Relationship to Employee** Employee ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name:	**3a. Your Relationship to Person in Box 2** Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ **Other (please describe relationship):**
4. Mailing Address for Records:	**4a. City, State, Zip Code:**

ection A: Request to Restrict Use and Disclosure of Personal Heath Plan Information

request that the use and disclosure of personal health plan information for the person in Box 2 be restricted in the manner described below:

_____

_____

_____

understand that the Plan may deny this request. I also understand that the Plan may remove this restriction in the future if I am notified in advance.

ection B: Request to Terminate Restricted Use and Disclosure of Personal Heath Plan Information

☐ I request that the restriction on the use and disclosure of personal health plan information made on _____ [Date Initial Request Made] be terminated. I understand that upon receipt of this form, the Plan will terminate the previously accepted restriction. Once a restriction has been terminated, the Plan will use and disclose personal health plan information as permitted or required by law.

☐ I agreed orally to terminate the restricted use and disclosure of personal health plan information belonging to the person in Box 2 made on _____ [Date Initial Request Made]. This serves as formal documentation of that oral agreement.

_____ _____

ignature **Date**

Part II – Determination of Request for Restricted Use of Personal Health Plan Information

Form Part II Prepared By	Date Part II Issued

After reviewing your request to restrict use of personal health plan information, the Plan has made the following determination [check one of the following]:

☐ Request Approved

☐ Request Denied

Name of Plan Representative	Signature of Plan Representative	Date of Determination

Part III – Termination of a Request for Restricted Use of Personal Health Plan Information

Form Part III Prepared by	Date Part III Issued

The Plan is providing you with notice that it is terminating its agreement to restrict its use and disclosure of personal health plan information as documented above in Part II of this Form. Any personal health plan information created or received on or after _____ [Date of Mailing] will not be subject to the restriction. The Plan may use and disclose your personal health plan information as permitted by law.

Name of Plan Representative	Signature of Plan Representative	Date of Determination

d. Request for Confidential Communications

Instructions for Responding to a Request for Confidential Communications

Directions for the Plan's Adminsitrator:

Providing Form. If any person wishes to request that the Plan use an alternative means to communicate his or her personal health plan information or that he or she receive personal health plan information at an alternate location, Communication Contact should provide the person with this Form. Examples of alternative means could include mail instead of fax, phone instead of mail, etc.

Receiving a Completed Form. Upon receipt of this Form, Communication Contact must verify that Part I (Request for Confidential Communications of Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the form must be signed and dated. If the person requesting the Confidential Communications of personal health plan information is not the subject of the information, Restrictions Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.

If Part I of the Form is incomplete, Communication Contact should return it to the person for completion.

Determination of Request. Upon receipt of this Form with Part I properly completed, Communication Contact will respond by completing Part II (Determination of Request for Confidential Communications of Personal Health Plan Information), within the timeframes detailed in Section 5.05 of the Manual.

Part I - Request for Confidential Communications of Personal Health Plan Information

Form Received By _____ Date _____

If you think that disclosure of your health information by the usual means could endanger you in some way, the Plan will accommodate reasonable requests to receive communications of health information from the Plan by alternative means or at alternative locations. If the Payment of benefits is affected by this request, the Plan may also deny this request unless you contact the Communication Contact to discuss alternative Payment means.

1. Employee Name:	**1a. Employee Health Plan ID Number:**
1b. Employee Date of Birth:	
2. Name of Person Whose Records You Are Requesting:	**2a. Relationship to Employee:** Employee ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name:	**3a. Your Relationship to Person in Box 2:** Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ **Other (please describe relationship):**
4. Mailing Address for Records:	**4a. City, State, Zip Code:**

I am requesting that communication of personal health plan information for the person in Box 2be provided by alternative means or at alternative locations. I [check one] ☐ am ☐ am not making this request because disclosure of all or part of the information to which the request pertains could endanger me, or the person I represent.

Please send the information by the following alternative means:

_____

_____

Please send the information to the following alternative address, if different than address above:

Street address _____

City, State and Zip code _____

Phone _____

Other _____

If this request relates to communication regarding Payment for health care services, please indicate how we can reach you to discuss alternative Payment means.

_____

Signature _____ **Date** _____

Part II – Determination of Request for Confidential Communications of Personal Health Plan Information

Form Part II Prepared By	Date Part II Issued

After reviewing your request for Confidential Communications of personal health plan information, the Plan has made the following determination [check one of the following]:

☐ Request Approved (see section A below)

☐ Request Denied (see section B below)

Section A: Request Approved

The Plan accepts your written request for the use of alternative means or alternative locations for Confidential Communications of personal health plan information The Plan will send personal health plan information [check all that apply]:

☐ By the alternative means you specified in Part I; and/or

☐ To the alternative address you specified in Part I.

Section B: Request Denied

The Plan denies your written request for the use of alternative means or alternative locations for Confidential Communications of personal health plan information for the following reasons [check all that apply]:

☐ The Plan has determined that the request is incomplete.

☐ The Plan has determined that the request is not reasonable

☐ The request does not clearly state that the Plan's usual means or locations of disclosure of personal health plan information poses a danger to you (or to the person in Box 2).

Name of Plan Representative	Signature of Plan Representative	Date of Determination

e. Accounting of Non-Routine Disclosures

Instructions for Responding for Accounting of Non-Routine Disclosures of PHI

Directions for the Plan's Administrator:

Providing Form. If any person wishes to request an accounting of non-routine PHI disclosures, Disclosure Contact should provide the person with this Form and a copy of the Privacy Notice detailing the non-routine disclosures.

Receiving a Completed Form. Upon receipt of this Form, Disclosure Contact must verify that Part I (Request for Accounting of Non-Routine Disclosures of Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the form must be signed and dated. If the person requesting personal health plan information is not the subject of the information, Disclosure Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.

If part I of the Form is incomplete, Disclosure Contact should return it to the person for completion.

Determination of Request. Upon receipt of the Form with Part I properly completed, Disclosure Contact will respond by completing Part II (Determination of Request for Accounting of Non-Routine Disclosures of Personal Health Plan Information), within the timeframes detailed in Section 5.06 of the Manual.

If the Plan is required to temporarily suspend a person's right to receive an accounting, as detailed in Section 5.06, Disclosure Contact must provide the person requesting the accounting with the appropriate information after the suspension of this person's right to receive the accounting has been lifted.

Part I - Request for Accounting of Non-Routine Disclosures of Personal Health Plan Information

Form Received By _____ Date _____

You have the right to a list of certain disclosures the Everett School Employee Benefit Trust (the "Plan") has made of your health information. This is often referred to as an "accounting of disclosures." You generally may receive an accounting of disclosures if the disclosure is required by law, in connection with public health activities, or in similar situations as described in more detail in the Plan's Privacy Notice.

1. Employee Name:	**1a. Employee Health Plan ID Number:**
1b. Employee Date of Birth:	
2. Name of Person Whose Accounting You Are Requesting:	**2a. Relationship to Employee:** Employee ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name:	**3a. Your Relationship to Person in Box 2:** Self ☐ Spouse ☐ Parent ☐ Child ☐ ☐ **Other (please describe relationship):**
4. Mailing Address for Records:	**4a. City, State, Zip Code:**

I understand that I can request an accounting of non-routine disclosures of personal health plan information once within any twelve (12)-month period, free of charge. If I request accountings more frequently, I understand the Plan will charge me a reasonable, cost-based fee for each subsequent request.

The accounting of non-routines disclosures of PHI will include the following information:

- The date of disclosure;
- The name of the person or entity to whom information was made and the person's or entity's address (if known);
- A brief description of the information disclosed; and
- The reason for the disclosure.

I hereby request an accounting of any non-routine disclosures of personal health plan information of the person named in Box 2 made by the Plan for the following time period _____ [Enter time period (disclosures can be requested for a time period of up six (6) years, beginning no earlier than April 14, 2003)].

Signature _____ **Date** _____

Part II - Determination of Request for Accounting of Non-Routine Disclosures of Personal Health Plan Information

Form II Prepared By	Date Form II Issued

After reviewing your request for an accounting of non-routine disclosures of personal health plan information, the Plan has made the following determination [check one of the following]:

☐ Request Approved without a fee (see section A below)

☐ Request Approved with a fee (see section B below)

☐ Request Denied (see section C below)

Section A: Request Approved without a Fee

Your request for an accounting of non-routine disclosures of personal health plan information is approved.

Your requested accounting of disclosures is attached to this form. There is no charge for processing request.

Section B: Request Approved with a Fee

Your request for an accounting of non-routine disclosures of personal health plan information is approved.

You requested and received an accounting of non-routine disclosures of personal health plan information, free of charge on _____ [Insert date that last free of charge accounting was disclosed]. The charge for processing this request is $_____ [Insert fee], as a fee for the preparation of your request for an accounting. You have the right to withdraw or modify your request for an accounting. Unless you contact Human Resources – Benefits Department at the following address 3715 Oakes Avenue, Everett, WA 98201 within 10 days from _____ [Insert date] to withdraw or modify your request, Human Resources – Benefits Department will mail you your requested accounting and will send you a bill for $_____ which you agreed to pay by signing Part I of this form.

Section C: Request Denied

Your request for an accounting of non-routine disclosures of personal health plan information is denied because none of your PHI was disclosed for a non-routine purpose.

If you wish to make a complaint, please contact Human Resources – Benefits Department at (425) 388-4710.

Name of Plan Representative	Signature of Plan Representative	Date of Determination

f. Authorization for Use and/or Disclosure of Health Information

Directions for the Plan's Administrator for Using Model Authorization Form

Providing Form. If any person wishes to request an Authorization for the use or disclosure of PHI in the Everett School Employee Benefit Trust, Authorization Contact should provide the person with this Form.

Receiving a Completed Form. Upon receipt of this Form Authorization Contact should initial and date the top right corner and must verify that the Form has been properly completed.

If the person submitting the Form is not the subject of the PHI, Authorization Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.

This model Authorization Form is intended to allow a person to have health information sent from Everett School Employee Benefit Trust's health plan (including its Business Associates, Insurers and HMOs) to a third party for non-health plan purposes, including Everett School Employee Benefit Trust. Everett School Employee Benefit Trust may want to modify the specific options described in Sections A – D of this Form to reflect the most common types of requests that occur for its plans.

The "Your Rights" section includes optional language. The first option assumes Payment, enrollment, and eligibility decisions are not conditioned on the signing of an Authorization. The second option says the Plan may require Authorizations prior to a person's enrollment to make enrollment/eligibility determinations or underwriting or risk rating determinations. The appropriate option should be selected, to reflect Everett School Employee Benefit Trust's practices.

Everett School Employee Benefit Trust could also amend this Form to be used by Everett School Employee Benefit Trust or an individual in requesting PHI from another covered entity in cases when an Authorization is required (either by the HIPAA privacy rule or that Covered Entity). However, the other Covered Entity is likely to require the use of its own Authorization Form.

This model Authorization Form complies with the requirements of the Health Insurance Portability and Accountability Act (HIPAA). State laws may impose addition requirements. Everett School Employee Benefit Trust should review this form and state law issues with counsel.

Instructions for the Individual Completing this Authorization Form

- The Everett School Employee Benefit Trust (the "Plan") cannot use or disclose your health information (or the health information of your children or other people on whose behalf you can act) for certain purposes without your Authorization. This form is intended to meet the Authorization requirement.
- You must respond to each section, and sign and date this form, in order for the Authorization to be valid.
- If you wish to authorize the use and/or disclosure of any notes the Plan may have that were taken by a mental health professional at a counseling session, along with other health information, you must complete one (1) form for the counseling session notes and one (1) separate form for other health information.
- The sample responses given for each section below are not exhaustive and are meant for illustrations only. Under HIPAA, there are no limitations on the information that can be authorized for disclosure.

Section A: Health Information to be Used or Released. Describe in a specific and meaningful way the information to be used or released. Example descriptions include medical records relating to my appendectomy, my laboratory results and medical records from [date] to [date], or the results of the MRI performed on me in July 1998.

Section B: Person(s) Authorized to Use and/or Receive Information. Provide a name or specific identification of the person, class of persons, or organization(s) authorized to use or receive the health information described in Section A.

Section C: Purpose(s) for which Information will be Used or Released. Describe each purpose for which the information will be used or released. If you initiate the Authorization and do not wish to provide a statement of purpose, you may select "at my request."

Section D: Expiration. Specify when this Authorization will expire. For example, you may state a specific date, a specific period of time following the date you signed this Authorization Form, or the resolution of the dispute for which you've requested assistance.

Signature Line. If you are authorizing the release of somebody else's health information, then you must describe your authority to act for the Individual.

Authorization to Use and/or Disclose Personal Health Plan Information

Form Received By _____ Date _____

1. Employee Name:	**1a. Employee Health Plan ID Number:**
1b. Employee Date of Birth:	
2. Name of Person Whose Health Information is the Subject of this Authorization:	**2a. Relationship to Employee:** Employee ☐ Spouse ☐ Child ☐ Other ☐
3. Your Name:	**3a. Authority** **If you are not the person in Box 2, please describe your authority to act on his or her behalf:** _____ _____
4. Mailing Address for Records:	**4a. City, State, Zip Code:**

I hereby authorize Everett School Employee Benefit Trust ("Plan") to use and/or disclose the health information described in Sections A — E below.

[Alternative for Everett School Employee Benefit Trust: modify this section to specify the organization that will release the information on behalf of the Plan, such as Insurer, HMO, Business Associate, or Everett School Employee Benefit Trust]

Section A: Health Information to be Used and/or Disclosed.

Specify the health information to be released and/or used, including (if applicable) the time period(s) to which the information relates. Select only one (1) of the following boxes:

☐ All of my past, present or future health claims and/or medical records.

☐ All of my health information relating to Claim Number _____.

☐ Other (please specify). _____ _____

Section B: Person(s) Authorized to Use and/or Receive Information.

Specify the persons or class of persons authorized to use and/or receive the health information described in Section A: _____.

Section C: Purposes for Which Information will be Used or Disclosed.

Specify each purpose for which the health information described in Section A may be used or disclosed. Select all of the applicable boxes below:

☐ To facilitate the resolution of a claim dispute.

☐ As part of my application for leave of under the Family and Medical Leave Act (FMLA) or state family leave laws.

☐ For a disability coverage determination.

☐ At my request.

☐ Other (please specify)._____

Section D: Expiration of Authorization

Specify when this Authorization expires. (Provide a date or triggering event related to the use or disclosure of the information.)

☐ On the following date: _____.

☐ Upon the passage of the following amount of time: _____.

☐ Upon my disenrollment from Everett School Employee Benefit Trust's health plan.

☐ Upon my return from FMLA leave.

☐ Other (please specify) _____

Your rights:

- You can revoke this Authorization at any time by submitting a written revocation to Human Resources – Benefits Department at the following address: 3715 Oakes Avenue, Everett, WA 98201.
- A revocation will not apply to information that has already been used or disclosed in reliance on the Authorization.
- Once the information is disclosed pursuant to this Authorization, it may be redisclosed by the recipient and the information by no longer be protected by HIPAA.
- **[Option 1: The Plan may not condition Treatment, Payment, enrollment or eligibility for benefits on whether I sign the Authorization.]**
- **[Option 2: This clause applies to individuals not yet enrolled in the Plan. If this Authorization was requested so the Plan can make an eligibility or enrollment determination or an underwriting or risk rating determination, then the person in Box 2 may be ineligible for enrollment or benefits if you fail to sign this form.]**
- You will be provided with a copy of this Authorization Form, after signing, if the Plan sought the Authorization.

_____

Signature of Participant & Date

10.09 List of Legally Required Uses, Public Health Activities, Other Situations Not Requiring Authorization

As described in Section 4, the Plan, its Insurers and Business Associates will, without obtaining a Participant's Authorization, use and disclose PHI if required by law, for certain public health purposes, and in other similar situations, described in the following chart:

Purpose for disclosure	Permissible disclosures of PHI
Workers' compensation	• Includes disclosures of PHI to workers' compensation or similar legal programs that provide benefits for work-related injuries or illness without regard to fault, as authorized by and necessary to comply with such laws.
Necessary to prevent or lessen serious threat to health or safety	• Includes disclosures of PHI to a person or persons if made under good faith belief that releasing PHI is necessary to prevent or lessen a serious and imminent threat to public or personal health or safety if made to someone reasonably able to prevent or lessen the threat (including disclosures to the target of the threat). • Includes disclosures of PHI to assist law enforcement officials in identifying or apprehending an individual because the individual has made a statement admitting participation in a violent crime that the Plan reasonably believes may have caused serious physical harm to a victim, or where it appears the individual has escaped from prison or from lawful custody.
Public health activities	• Includes disclosures of PHI authorized by law to persons who may be at risk of contracting or spreading a disease or condition. • Includes disclosures of PHI to public health authorities to prevent or control disease and to report child abuse or neglect. • Includes disclosures of PHI to the FDA to collect or report adverse events or product defects.
Victims of abuse, neglect, or domestic violence	• Includes disclosures of PHI to government authorities, including social services or protected services agencies authorized by law to receive reports of abuse, neglect, or domestic violence, as required by law or if the subject of the PHI agrees or the Plan believes disclosure is necessary to prevent serious harm to the individual or potential victims; the

Purpose for disclosure	Permissible disclosures of PHI
	Plan will notify the individual that is the subject of the disclosure if it won't put the individual at further risk.
Judicial and administrative proceedings	• Includes disclosures of PHI in response to a court or administrative order; and disclosures in response to a subpoena, discovery request or other lawful process (the Plan is required to notify the individual that is the subject of the request for PHI of the request, or to receive satisfactory assurance from the party seeking the PHI that efforts were made to notify the individual that is the subject of the request for PHI or to obtain a qualified protective order concerning the PHI).
Law enforcement purposes	• Includes disclosures of PHI to law enforcement officials as required by law or pursuant to legal process, or to identify a suspect, fugitive, witness or missing person. • Includes disclosures of PHI about a crime victim if the individual that is the subject of the PHI agrees or if disclosure is necessary for immediate law enforcement activity. • Includes disclosures of PHI regarding a death that may have resulted from criminal conduct and disclosures to provide evidence of criminal conduct on the Plan's premises.
Decedents	• Includes disclosures of PHI to a coroner or medical examiner to identify the deceased or to determine the cause of death, and to funeral directors to carry out their duties.
Organ, eye, or tissue donation	• Includes disclosures of PHI to organ procurement organizations or other entities to facilitate cadaveric organ, eye, or tissue donation and transplantation.
Research purposes	• Includes disclosures of PHI subject to approval by institutional or privacy boards, and subject to certain assurances and representations by researchers regarding necessity of using PHI and treatment of PHI during a research project.
Health oversight activities	• Includes disclosures of PHI to health agencies for activities authorized by law (audits, inspections, investigations, or licensing actions) for oversight of the health care system, government benefits programs for which health information is relevant to beneficiary eligibility, compliance with regulatory programs, or civil rights laws.
Specialized government functions	• Includes disclosures of PHI of individuals who are Armed Forces personnel or foreign military personnel under appropriate military command authority.

Purpose for disclosure	Permissible disclosures of PHI
	• Includes disclosures to authorized federal officials for national security or intelligence activities. • Includes disclosures to correctional facilities or custodial law enforcement officials about inmates.
Department of Health and Human Services (HHS) Investigations	• Includes disclosures of PHI to HHS to investigate or determine the Plan's compliance with the HIPAA Privacy Rule.

COMPLIANCE AND RISK MANAGEMENT

Health Insurance Portability and Accountability Act of 1996 (HIPAA) – Privacy, Security, and Reportable Breach Notification Policies

The Trustees intend these policies to provide guidelines to protect the privacy of participants and beneficiaries participating in the Everett School Employee Benefit Trust ("Trust"), and to ensure that all information related to participants and beneficiaries is maintained in the strictest confidence and in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing privacy regulations (the "Privacy Rule") and security regulations (the "Security Rule"). Under the Privacy Rule, the Trust's policy restricts the Group Health Plan's use and disclosure of protected health information, or "PHI." Under the Security Rule, this policy ensures the confidentiality, integrity and availability of electronic PHI, or "ePHI," and protects against any reasonably anticipated threats or hazards to the security or integrity of ePHI. The Trustees also intend to comply with the rules for reporting certain breaches of confidentiality to plan participants under HIPAA and Washington state law.

Details of the policies and implementing procedures may be found in the Trust's HIPAA Privacy Policy and HIPAA Security Policy.

Cross References:

HIPAA Privacy Policy	
HIPAA Security Policy	
District Policy 3245	Technology
District Procedure 3245P	Technology
District Policy 5225	Technology
District Procedure 5225P	Technology

Approved: August 29, 2005
Revised: January 24, 2011
Revised: April 30, 2012
Revised: March 17, 2016

Everett School Employee Benefit Trust

HIPAA Security Policy

I. Introduction

Everett School Employee Benefit Trust ("Trust") provides one or more group health plans subject to HIPAA's security regulations (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"). Members of the District's workforce may create, receive, maintain, or transmit certain limited amounts of electronic protected health information (as defined below) on behalf of the Plan Sponsor, for plan administration functions.

The Group Health Plan is subject to the security rules of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing administrative simplification security regulations ("Security Rules").

Most of the Group Health Plan is provided pursuant to insurance policies issued by insurance companies ("Health Insurance Issuers"). Almost all of the electronic protected health information of the Group Health Plan resides with these Health Insurance Issuers, which are also subject to HIPAA and the Security Rules. This policy is complementary and supplementary to the HIPAA security policies of the Health Insurance Issuers. To the extent that PHI (defined below) is under the control of a Health Insurance Issuer, and has not been disclosed or released to any member of the District's workforce, the Health Insurance Issuer has primary responsibility for compliance with the Security Rules.

The purpose of this document is to set a policy for the Group Health Plan to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") security regulations concerning electronic protected health information, which are found at 45 C.F.R. Parts 160 and 164. HIPAA and its implementing regulations require the Group Health Plan to implement various security measures with respect to electronic protected health information ("ePHI").

It is the Group Health Plan's policy to comply fully with the requirements of HIPAA's security regulations. No third-party rights (including, but not limited to, rights of Group Health Plan participants, beneficiaries, or covered dependents) are intended to be created by this Policy. The Group Health Plan reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent that this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Group Health Plan. This Policy does not address requirements under state law or federal laws other than HIPAA.

II. Definitions

A. *Electronic Protected Health Information or ePHI* is protected health information that is transmitted by or maintained in electronic media.

B. *Protected Health Information or PHI* is the information that is subject to and defined in the Group Health Plan's privacy policies and procedures. For purposes of this Policy, PHI does not include the following, referred to in this Policy as "Exempt Information":

1. summary health information, as defined by HIPAA's privacy rules, for purposes of (a) obtaining premium bids or (b) modifying, amending, or terminating the Group Health Plan;

2. enrollment and disenrollment information concerning the Group Health Plan which does not include any substantial clinical information;

3. health information which has been de-identified in accordance with HIPAA's privacy rules; or

4. PHI disclosed to the Group Health Plan and/or District under signed authorization that meets the requirements of the HIPAA privacy rules.

C. *Electronic Media* means:

1. Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, and voice via telephone are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

III. Security Official

Molly Ringo is the Security Official for the Group Health Plan. The Security Official is responsible for the development and implementation of the Group Health Plan's policies and procedures relating to security, including but not limited to this Policy. The Security Official also shall hear all complaints regarding alleged violations of this Policy and shall ensure that the complaint and its disposition are appropriately handled and documented.

IV. Risk Analysis

The Group Health Plan, in connection with the District's Human Resources Department, has undertaken a risk analysis to assess the potential vulnerabilities and risks to the confidentiality, integrity and availability of ePHI, with the following results:

The Group Health Plan has no employees. The Trustees of the Trust are not involved in the appeals of claim denials or in any other capacity concerning the processing of claims. All of the Group Health Plan's functions, including creation and maintenance of its records, are carried out by the Health Insurance Issuers, business associates of the Group Health Plan, and to a small extent, employees of the District's Human Resources Department. The Group Health Plan does not own or control any of the equipment or media used to create, maintain, receive, and transmit ePHI relating to the Group Health Plan, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the Health Insurance Issuers, other business associates, and to a limited extent, the District. Accordingly, Health Insurance Issuers, the business associates of the Group Health Plan or the District: (1) create and maintain all of the ePHI relating to the Group Health Plan; (2) own or control all of the equipment, media, and facilities used to create, maintain, receive, or transmit ePHI relating to the Group Health Plan, and (3) control their employees, agents, and subcontractors who have access to ePHI relating to the Group Health Plan. The Group Health Plan has no or limited ability to assess or in any way modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI being held by the Health Insurance Issuers and business associates.

Because the Group Health Plan has no access to or control over the employees, equipment, media, facilities, policies, procedures, or documentation of the Health Insurance Issuers and business associates affecting the security of the Group Health Plan ePHI, the Health Insurance Issuers and business associates have undertaken certain obligations relating to the security of ePHI that they handle in relation to the performance of administration functions for the Group Health Plan, the Group Health Plan's policies and procedures, including this Policy, do not separately address the following standards (including the implementation specifications associated with them) established under HIPAA and are set out in Subpart C of 45 CFR Part 164, except in conjunction with the District's Human Resources Department, as described in Section VIII of this Policy:

- security management process;
- workforce security;
- information access management;
- security awareness and training;
- security incident procedures;
- contingency plan;
- evaluation;
- facility access controls;
- workstation use;
- workstation security;
- device and media controls;
- access control;
- audit controls;
- integrity;
- person or entity authentication; and
- transmission security.

The HIPAA security policies and procedures of the Health Insurance Issuers and business associates for ePHI of the Group Health Plan for the standards listed above, as well as the policy under these procedures as set forth in Section VIII of this Policy, are adopted by the Group Health Plan.

V. Group Health Plan Document: Plan Sponsor's Safeguards

The Group Health Plan documents include provisions requiring the Plan Sponsor to:

- implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that the Plan Sponsor creates, receives, maintains, or transmits on behalf of the Group Health Plan ("Plan's ePHI");
- ensure that reasonable and appropriate security measures support the Group Health Plan document provisions providing for adequate separation between the Group Health Plan and the Plan Sponsor;
- ensure that any agents or subcontractors to whom the Plan Sponsor provides the Plan's ePHI agree to implement reasonable and appropriate security measures to protect the Plan's ePHI; and
- report to the Security Official any security incident of which the Plan Sponsor becomes aware.

VI. Risk Management

The Group Health Plan manages risks to its ePHI by limiting vulnerabilities, based on its risk analyses, to a reasonable and appropriate level, taking into account the following:

- The size, complexity, and capabilities of the Group Health Plan;
- The Group Health Plan's technical infrastructure, hardware, software, and security capabilities;
- The costs of security measures; and,
- The criticality of the ePHI potentially affected.

Based on risk analysis discussed in section IV of this Policy, the Group Health Plan has made a reasoned, well-informed, and good-faith determination on the implementation of the HIPAA security regulations that the Group Health Plan need not take any additional security measures, other than the measures set forth herein and the measures adopted to reduce risks to the confidentiality, integrity and availability of ePHI: (a) in conjunction with the Human Resources Department of the District as described in Section VIII; and (b) by the Health Insurance Issuers and business associates of the Group Health Plan.

VII. Disclosures of ePHI to Business Associates

A business associate is an entity (other than the Plan Sponsor), or a Health Insurance Issuer, that:

- performs or assists in performing a Group Health Plan function or activity involving the use and disclosure of PHI (including data analysis, underwriting, etc.); 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.

The Group Health Plan permits business associates to create, receive, maintain, or transmit ePHI on its behalf. The Group Health Plan has obtained or will obtain satisfactory assurances from all business associates that they will appropriately safeguard the information. Such satisfactory assurances shall be documented through a written contract containing all of the requirements of the HIPAA privacy and security regulations and specifically providing that the business associate will:

- implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of all of the Plan's ePHI that the business associate creates, receives, maintains, or transmits on behalf of the Group Health Plan;
- ensure that any agents or subcontractors to whom the business associate provides the Plan's ePHI agree to implement reasonable and appropriate security measures to protect the Plan's ePHI;
- take required steps with respect to notification requirements concerning breaches of unsecure PHI;
- report to the Group Health Plan any security incident of which the business associate becomes aware; and
- authorize termination of the contract by the Group Health Plan, if the Group Health Plan determines that the business associate has violated a material term of the contract.

In addition to these requirements being contractual obligations of the business associate under the written contract, a business associate of the Group Health Plan is required under federal law and independent of such written contract to comply with the HIPAA security regulations to protect the security of the ePHI the business associate creates, receives, maintains, and transmits on behalf of the Group Health Plan. Thus, the Group Health Plan can reasonably rely that its business associates will comply with the HIPAA security requirements pursuant to applicable federal law.

VIII. HIPAA Security Compliance Measures for Group Health Plan in Conjunction with District's Human Resources Department

Certain employees of the District may have limited access to ePHI of the Group Health Plan for plan administration and other permissible purposes, via access to secure servers of the Health Insurance Issuers or other secure means. If available, access to these secured servers is password-protected, and only certain members of the Human Resources Department have passwords to access these servers. To an even more limited extent, it is possible that ePHI may be communicated via the District's email system, and such ePHI is stored and used on District computers and other electronic media. The Group Health Plan, in conjunction with the District's Human Resources Department, has undertaken necessary and appropriate steps, as described in this Section VII, to protect the security of the Plan's ePHI which is created, received, maintained, or transmitted by the Human Resources Department ("HR Department") employees.

A. Administrative Safeguards.

1. Security Management Process. The following policies and procedures regarding security management of ePHI are adopted:

   a. *Risk Analysis.* The following is a description of the risk analysis undertaken to assess the potential vulnerabilities and risks to the confidentiality, integrity and availability of the Plan's ePHI being used or held by certain District employees. The Health Insurance Issuers for the Group Health Plan create, receive, maintain and transmit the vast majority of Plan ePHI. A small amount of ePHI may be created, received, maintained or transmitted by the District is email in Microsoft Outlook ("Outlook") on the computers of employees of the HR Department and the District's wellness coordinator ("HR Employees"). The risks and vulnerabilities to this email in Outlook are very minimal. For confidentiality issues, there is a very low risk that unauthorized persons can access the material because unique passwords are required to access the email of these employees in Outlook, firewalls are in place to prevent hacking into the District's computer system and because of the physical security at the District's worksite. Software runs continuously on the District systems to scan emails to protect against viruses, worms and similar issues. Concerning integrity and availability, the ePHI in Outlook is not generally not critical or essential to the day-to-day workings of the Group Health Plan, which is operated and maintained by off-site Health Insurance Issuers and other business associates. If a computer holding ePHI at the District crashed, the ePHI in Outlook can generally be recreated or obtained from the Health Insurance Issuer or other source. In addition, a complete failure or crash of a District computer which would result in the destruction of the ePHI in Outlook would be extremely rare. For the same reason, there is little concern to the Group Health Plan if there was a fire or natural disaster at the District which destroyed the ePHI because the ePHI is also in the hands of the Group Health Plan's Health Insurance Issuers. The District has in place reasonable and appropriate measures to control passwords and to protect against viruses and worms.

   b. *Risk Management.* The following security measures are in place to reduce risks and vulnerabilities to the ePHI in Microsoft Outlook.

      i. The District's Human Resources' department is not open to the general public. Visitors or non-Department employees must be escorted by HR Employees.

      ii. HR Employees with access to ePHI are required to protect their passwords from other employees and from visitors by storing their passwords in secure locations.

      iii. Computers for the HR Employees have in place a mechanism by which the computer will lock-down after a period of 10 minutes of non-use.

      iv. Temporary employees will not be hired to fill HR Employee positions unless the temporary employees are fully trained regarding this policy and the HIPAA privacy policies relating to the Group Health Plan. Temporary employees will be screened to determine whether access to ePHI should be granted to them.

      v. In addition, the HR Department and the Group Health Plan will continue to implement other security measures already in place and described in the previous section, Risk Analysis, to protect the ePHI of the Group Health Plan.

c. *Sanction Policy.* District employees who violate this policy are subject to disciplinary action, including, but not limited to, reprimands and termination.

d. *Information System Activity Review.* On a periodic basis, the HR Department or a representative of the Group Health Plan will review records of information system activity, especially activity in Outlook, such as audit logs or access reports, to determine if security violations relating to the ePHI have occurred. The results of these reviews will be documented and kept in a secure file with the Security Official.

2. Workforce Security. The following policies and procedures regarding workforce security are adopted:

a. *Authorization and/or Supervision.* Outside visitors and employees of other departments of the District are not authorized to be in the HR Department workplace unless they are supervised by HR Employees, who are trained not to allow unauthorized access to ePHI. HR Employees are required to monitor their workstations so that unauthorized employees or guests do not inadvertently view or have access to ePHI of the Group Health Plan. Computers of HR Employees are protected by unique user identification and passwords. HR Employees are required to log off of their computers or turn their computers off at night when cleaning crews are in the area.

b. *Workforce Clearance Procedures*. Only HR Employees work on a daily basis with ePHI of the Group Health Plan. There is a screening process, which includes a background check in the hiring process, to determine that access to ePHI is appropriate for these employees. HR Employees only have access to ePHI for purposes of administration of the Group Health Plan.

c. *Termination Procedures*. Access to ePHI will be terminated as soon as practicable when an HR Employee's employment at the District terminates. When an HR Employee leaves the employment of the District, the employee is required to turn in all keys, badges and passcards for access to the building and to their previous workplaces. The entire accounts for such terminated employees, including passwords and unique user identifications, are immediately disabled on the District's computer systems. Health Insurance Issuers and business associates are informed about terminated employees and are instructed to disable passwords of the terminated employees to their secure servers.

3. Information Access Management. The following policies and procedures regarding information access management are adopted.

a. *Isolating Healthcare Clearinghouse Functions*. This standard does not apply to the Group Health Plan.

b. *Access Authorization*. Only HR Employees have access to ePHI on a regular basis. Other personnel, such as those responsible for the District's computers, are only granted access to ePHI on a very limited and "as needed" basis for issues dealing with the computer of an HR Employee. Any access to ePHI granted to non-HR Employee District personnel is also only the minimum necessary to accomplish the particular necessary task or function.

c. *Access Establishment and Modification*. Only HR Employees have access to ePHI on a regular basis. If an HR Employee is transferred outside of the HR Department, the Plan's Security Official and/or supervisory employees in the HR Department will take appropriate steps to block further access to ePHI of the Group Health Plan, including removing these files from Outlook Exchange for the employee and terminating their passwords to secure servers of the Health Insurance Issuers or business associates.

4. Security Awareness Training. The following policies and procedures regarding security awareness training are adopted.

   a. *Security Reminders*. HR Employees receive initial and continuing training in HIPAA security rules and this policy, as directed by the Security Official. The Security Official will periodically send emails or other communications reminding them of the rules and this policy, and will ensure that new HR Employees receive training as needed.

   b. *Protections from Malicious Software.* The District's computers and computer networks and systems, including those used by the HR Employees, have protections against viruses and worms and similar malicious software programs. These protections are updated on a periodic basis. HR Employees may not install unauthorized software on their computers at work.

   c. *Log-in Monitoring*. After three attempts, District computers will not grant access to an individual user if the user attempts to enter the system and does not enter the correct password. In this instance, the employee in question must obtain a new password in order to operate the computer at his or her desk. Issues and discrepancies relating to log-in monitoring success and failures are reported to the Security Official.

   d. *Password Management.* Passwords to the computers of the HR Employees have certain characteristics that make them difficult to duplicate. All passwords are required to be changed every 90 days. HR Employees may not share their passwords with other employees and may not have passwords easily accessible at their workstations.

5. Security Incident Procedures. The following policies and procedures regarding security incidents are adopted.

   a. *Response and Reporting*. All HR Employees are required to report any security incidents to the Security Official for appropriate investigation and action. For purposes of this Policy, a security incident is any attempted or successful unauthorized access, use, disclosure, modification of destruction of information or interference with system operations in the District computers which would involve ePHI. The Security Official will respond to security incidents and will document the security incidents and outcomes. To the extent practicable, the Security Official will take steps to mitigate the harmful effects of the security incidents which are reported to the Security Official.

6. Contingency Plan. The following contingency plans and policies are adopted.

   a. *Data Backup Plan*. The District has a data backup plan which applies to the ePHI held on the HR Department computers. In addition, since the Group Health Plan is run by Health Insurance Issuers, most of the ePHI of the Group Health Plan could be retrieved from the Health Insurance Issuers or from the person or entity that sent the email to or received the email from the HR Department. The ePHI at the Health Insurance Issuers' offices is subject to the data backup plans of the Health Insurance Issuers.

   b. *Disaster Recovery Plan.* A disaster at HR Department offices would not effect in any large measure the day-to-day operations of the Group Health Plan. In the event of a disaster at the offices, essential ePHI would be obtained from data backup sources, from providers, from the Health Insurance Issuers and from other sources. The Group Health Plan is also relying on, and would utilize, the disaster recovery plans of the Health Insurance Issuers for the Group Health Plans.

c. *Emergency Mode Operation Plan.* In an emergency, the Group Health Plan would be operated, as it is now, through off-site Health Insurance Issuers and business associates. The HR Department offices, and the computers within the offices, would be protected by security for the site. The Group Health Plan is also relying on the emergency mode operation plans of its Health Insurance Issuers for the Group Health Plan.

d. *Testing and Revision Procedures.* The District conducts fire drills and similar types of testing at the HR Offices.

e. *Periodic Review.* The Group Health Plan will conduct periodic reviews of its contingency plans to determine whether revisions are necessary or desirable.

f. *Applications and Data Criticality Analysis*. The most critical applications for ePHI are Outlook and the firewall software (i.e., the virus and worm protection software) utilized by the District.

7. Evaluation. The following policies and procedures regarding evaluation of its security safeguards are adopted.

a. *Periodic Technical and Non-Technical Evaluation*. The Trustees of the Trust and the HR Department will conduct periodic evaluations (technical and non-technical) of its security safeguards to determine the continued protection of the ePHI of the Group Health Plan and to determine if new risks may be present. Such evaluations are appropriate when new technology, new risks or other changes to the security environment occur.

B. Physical Safeguards.

1. Facility Access Controls. The following policies and procedures regarding facility access controls are adopted.

a. *Contingency Operations.* In an emergency, the Group Health Plan would be operated, as it is now, through the Health Insurance Issuers. The District offices, and the computers within the offices, would be protected by security. In emergency situations, the HR Employees and the Security Official first will be granted access to the ePHI and will determine the extent to which access for other personnel is appropriate. Any critical data which is lost would be recovered from the Health Insurance Issuers and/or from other persons who sent the email to or received the email from the HR Employees.

b. *Facility Security Plan*. The District offices have a facility security plan. Most doors to the building have controlled entrances which require keys for entrance. Visitors to the building must check in and be escorted by District employees. Any unauthorized entries are immediately reported to security personnel or as necessary to the Everett police department and other law enforcement officials.

c. *Access Control and Validation Procedures*. Visitors to the District offices are escorted by District employees. Employees of other departments are not authorized to be in the Human Resources workplace unless they are supervised by HR Employees. Computers housing ePHI are protected by passwords. Computers are logged off or turned off at night when cleaning crews or other maintenance personnel are in the Human Resources department.

d. *Maintenance Records.* The Security Official will document repairs and modifications to the physical components of the security systems which relate to ePHI of the Group Health Plan.

2. Workstations Use and Workstations Security. The following policies and procedures regarding workstations use and security are adopted.

a. *Proper Functioning and Physical Attributes of Workstations, Physical Safeguards for Workstations.* District employees who are not employees of the HR Department are not authorized to be in the HR Department or to view the computers of HR Employees, unless such non-HR Department employees are adequately and properly supervised. Access to HR Employee workstations is controlled by unique user identification codes and passwords. HR Employees are required to log off of their computers at the end of the work day and when they are going to be away from their workstations for extended periods of time during the work day. See also the policies for Facility Security Plan. HR Employees are not authorized to access email with ePHI when they are off-site.

3. Device and Media Controls. The following policies and procedures regarding device and media controls are adopted.

a. *Proper Disposal of PHI and Hardware/Software Storing PHI.* Before disposal of a computer in the HR Department, the Security Official or her designee shall insure that all ePHI in the computer is completely removed from the computer. Before such removal of the ePHI, any essential ePHI on the computer will be retrieved and stored elsewhere if it is not otherwise available.

b. *Media Re-Use*. Before re-use of a HR Department computer by another District department, all ePHI on the computer is completely removed from the computer in a manner which makes its re-creation by a new user impossible. If ePHI is stored on CD, floppy discs or other similar electronic media, the ePHI will be completely removed prior to re-use of the electronic media, or the electronic media will be destroyed and not re-used. If ePHI is stored on CD, floppy discs or other similar electronic media, the media will be store in locked file cabinets.

c. *Accountability.* The District maintains a record of all District computers by serial number and a log of the location of these computers.

d. *Data Backup and Storage*. Appropriate steps will be undertaken to create a copy of essential ePHI on the computers of HR Employees if the computers are moved and such movement creates a risk of losing data or a risk to the integrity of the data.

C. Technical Safeguards.

1. Access Controls. The following policies and procedures regarding access controls are adopted.

a. *Unique User Identification*. There is an assigned unique user name for identifying and tracking the identity of users of the HR Department computers, along with passwords. All passwords are required to be changed every 90 days. It is violation of this policy for HR Employees to allow another person access to or to use the HR Employee's unique user identifications and/or passwords. All HR Employees must ensure that their passwords are not documented, written, or otherwise exposed in an insecure manner. If an HR Employee has a reason to believe that his or her user identification or password has in any way been compromised, he or she must report that security incident to the Security Official.

b. *Emergency Access Procedure*. In the event of an emergency, ePHI of the Group Health Plan will be obtained through the Health Insurance Issuers of the Group Health Plan. If the emergency extends to the Health Insurance Issuers' offices or facilities, the Group Health Plan will follow the emergency access procedures adopted by the Health Insurance Issuers.

c. *Automatic Logoff*. The computers of HR Employees have an automatic logoff feature.

d. *Encryption.* Because of the small amount of ePHI transmitted to or from or held at the HR Department, it is not reasonable and practical to encrypt ePHI (such as emails to other service providers or plan participants). If any such other PHI is of an extremely sensitive nature, it will be communicated via non-electronic means (such as dedicated fax lines).

2. Audit Controls. The following policies and procedures regarding audit controls of the ePHI are adopted.

a. *Record Internal Uses of PHI by User.* The District has in place computer programs which allow the District to record and examine activity by users.

3. Integrity. The following policies and procedures regarding integrity of ePHI are adopted.

a. *Mechanism to Authenticate ePHI.* The official records of the Group Health Plan are held in the possession of the Health Insurance Issuers, so the Group Health Plan relies on them to implement electronic mechanisms to corroborate that the Plan's ePHI has not been altered or destroyed in an unauthorized manner. The likelihood of tampering with emails in Outlook at the HR Department is minimal and in any instances where tampering might have occurred, the HR Employees will authenticate the ePHI with the Health Insurance Issuer or the provider of the medical services.

4. Person or Entity Authentication. The following policies and procedures regarding person or entity authentication are adopted.

a. *Person/Entity Seeking Access is the One Claimed.* The HR Department utilizes unique user ID and passwords to verify that persons seeking access to ePHI are the employees authorized to gain such access.

5. Transmission Security. The following policies and procedures regarding the security of transmissions of ePHI are adopted.

a. *Integrity Controls*. Most of the ePHI obtained by HR Employees is located on secured servers from Health Insurance Issuers for the Group Health Plans. Communication with them is password or otherwise protected.

b. *Encryption.* Most of the ePHI obtained by HR Employees is ePHI transmitted to and from the Health Insurance Issuers. Communication with them is conducted via a secure server or via other secure means. Because of the small amount of other ePHI transmitted to or from or held at HR Employees, it is not reasonable and practical to encrypt the other ePHI (such as emails to other service providers or plan participants). If any such other PHI is of an extremely sensitive nature, it will be communicated via non-electronic means (such as dedicated fax lines). For this small amount of other ePHI, the Group Health Plan has determined that this is a reasonable and practical alternative to encryption, given the technical and financial burdens associated with encryption.

D. Breaches of Unsecured PHI.

The Group Health Plan will comply with the requirements of HIPAA and implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Group Health Plan, a Health Insurance Issuer or a business associate discovers a breach of unsecured PHI.

IX. Documentation

The Group Health Plan's security policies and procedures shall be documented, reviewed periodically, and updated as necessary in response to environmental or operational changes affecting the security of Group Health Plan ePHI, and any changes to policies or procedures will be documented promptly.

Except to the extent that they are carried out by the HR Employees or business associates, the Group Health Plan shall document certain actions, activities, and assessments with respect to ePHI required by HIPAA to be documented (including amendment of the Group Health Plan document in accordance with this policy, for example).

Policies, procedures, and other documentation controlled by the Group Health Plan may be maintained in either written or electronic form. The Group Health Plan will maintain such documentation for at least six years from the date of creation or the date last in effect, whichever is later.

The Group Health Plan will make its policies, procedures, and other documentation available to the Security Official and the Plan Sponsor, Health Insurance Issuers, and business associates or other persons responsible for implementing the procedures to which the documentation pertains.

Everett School Employee Benefit Trust

Reportable Breach Notification Policy
HIPAA HITECH Rules and Washington State Law

Introduction

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

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

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

General Procedures

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

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

I. HIPAA HITECH Rules

Effective Date

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

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

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

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

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

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

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

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

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

(1) PHI = Individually identifiable health information

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

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

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

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

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

a. Unauthorized access of PHI

b. Unauthorized use of PHI

c. Unauthorized acquisition of PHI

d. Unauthorized disclosure of PHI

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) Examples:

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

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

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

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

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

(1) Examples:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Deadlines for Notices

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

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

(2) Examples:

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

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

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

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

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

1. Notices to Individual (See Section D)

a. Actual Notice

b. Substitute Notice

c. Urgent Notice

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

3. Notice to HHS (See Section F)

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

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

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

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

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

a. A brief description of incident.

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

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

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

(1) Contact credit card company

(2) Contact credit bureaus

(3) Obtain credit monitoring services

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

(1) Filing police report

(2) Reviewing security logs or tapes

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

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

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

(2) Encryption

(3) Installing new firewalls

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

(1) Toll-free phone number

(2) Email address

(3) Website

(4) Postal address

2. Forms of Notices to Individuals

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

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

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

(3) Sent to the parent of minor child

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

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

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

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

(a) Telephone notice

(b) Notice in person

(c) Email notice

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

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

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

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

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

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

3. Urgent Notice

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

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

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

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

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

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

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

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

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

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

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

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

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

F. **Notification to HHS Secretary**

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

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

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

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

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

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

G. **Training**

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

II. WASHINGTON STATE BREACH NOTIFICATION RULES

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

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

   a. SSN

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

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

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

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

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

APPENDIX

Deidentified Information

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

C. Names;

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

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

F. Telephone numbers;

G. Fax numbers;

H. Electronic mail addresses;

I. Social security numbers;

J. Medical record numbers;

K. Health plan beneficiary numbers;

L. Account numbers;

M. Certificate/license numbers;

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

O. Device identifiers and serial numbers;

P. Web Universal Resource Locators (URLs);

Q. Internet Protocol (IP) address numbers;

R. Biometric identifiers, including finger and voice prints;

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

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