

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(f).

#### § 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(f), 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<br>contact<br>information: | Privacy Official Designee is Dottie Cainion, Benefits<br>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.