University of Puget Sound
Flexible Benefits Program
PRIVACY AND SECURITY POLICY AND PROCEDURES

PURPOSE: To establish a process for complying with the Standards for Privacy of Individually Identifiable Health Information in 45 CFR Part 160 and Part 164, subparts A, D and E and the Standards for Security of Electronic Protected Health Information at CFR Part 160 and Part 164, subparts A and C with respect to protected health information created, received, maintained or transmitted in the administration of the **University of Puget Sound Flexible Benefits Program** (the "Plan").

POLICY: The University of Puget Sound (the "University") sponsors the Plan. This Policy sets out the University's procedures on behalf of the Plan regarding "protected health information" ("PHI"), as that term is defined in federal regulations issued pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA). This Policy does not confer any rights on any third party, nor shall any such person or entity have any rights, directly or indirectly, to enforce this Policy as a third-party beneficiary or in any other capacity.

DEFINITIONS: All terms used, but not otherwise defined in the Policy and Procedures shall have the same meaning as those terms in 45 CFR §§ 160.103, 164.103, 164.304 and 164.402.

PROCEDURES: The following procedures shall be used to comply with the Standards for Privacy of Individually Identifiable Health Information in 45 CFR Part 160 and Part 164, subparts A, D and E and the Standards for Security of Electronic Protected Health Information at CFR Part 160 and Part 164, subparts A and C with respect to PHI created, received, maintained or transmitted in the administration of the Plan.

1. Privacy Officer; University Functions

1.1 The University shall designate a person to serve as the Plan's privacy officer (the "Privacy Officer"). **The Associate Vice President of Human Resources has been designated as the University's Privacy Officer.**

1.2 Any person serving as the Privacy Officer may resign that role with 15 days advance written notice to the University. The University may remove the Privacy Officer without having to show cause. The University shall appoint a new Privacy Officer as soon as reasonably practicable. Until a new appointment is made, the person serving in the role that carries with it direct authority to appoint the Privacy Officer, **the Vice President for Finance and Administration,** shall serve as the Privacy Officer.

1.3 The Privacy Officer shall design and implement the Plan's privacy practices and shall decide any questions about the privacy rights of participants and their beneficiaries. Any decision by the Privacy Officer within the Privacy Officer's authority shall be final and binding on all parties. The Privacy Officer shall have absolute discretion to carry out responsibilities under this Policy.

1.4 The Privacy Officer shall be the privacy official under HIPAA and applicable regulations and shall comply with HIPAA, the HITECH Act, applicable regulations and Plan provisions regarding privacy. The Privacy Officer shall keep records relating to the privacy rights of all persons under the Plan. Any person having a question or concern about privacy rights under the Plan may consult the Privacy Officer at any reasonable time. Notices to the Privacy Officer shall be sent to the University's address.

1.5 If the Vice President for Finance and Administration approves, the Privacy Officer may delegate all or part of the administrative duties of the Privacy Officer to one or more agents and may retain advisors for assistance. The Privacy Officer may consult with and rely upon the advice of counsel, who may be counsel for the University.

1.6 The Privacy Officer shall arrange for training of personnel with access to PHI as appropriate to permit them to perform their responsibilities relating to the Plan. Such training will be documented such that the materials used in the training and the names or positions of employees who were trained will be maintained by the University. The responsibility for arranging for training of personnel with access to PHI may be delegated to the Director of Compensation and Benefits and the Director of Employment and People Development. The responsibility for documenting such training will be delegated to the Director of Employment and People Development.

1.7 All University functions or responsibilities identified herein may be exercised by the Vice President for Finance and Administration, who may delegate all or any part of these functions.

2. Privacy Practices

2.1 The Privacy Officer shall develop and distribute the Plan's privacy notice as required by law.

2.2 The University shall establish technical and physical safeguards designed to prevent improper use or disclosure of PHI, following standard industry practices.

2.3 Subject to 1.5 above, the Privacy Officer shall be the Plan's contact person for receiving complaints regarding the Plan's privacy practices. Any Plan participant or beneficiary who is concerned that the Plan's privacy practices may have been breached may report those concerns to the Privacy Officer.

2.4 The University shall take a range of corrective action with employees or other workforce members who violate this Policy, up to and including termination of employment, pursuant to the University's employment policies as provided in the University's campus-wide policies, the Staff Policies and Procedures, the Student Integrity Code, and the Faculty Code.

2.5 The University shall not coerce or discriminate or retaliate against any person for exercising his or her HIPAA privacy rights or rights under HITECH or for opposing any violation of such rights. The University shall not require any person to waive his or her HIPAA privacy rights or HITECH rights as a condition of eligibility, enrollment, treatment or payment under the Plan.

2.6 The Privacy Officer shall take reasonable steps to mitigate the harmful effects of an improper use or disclosure of PHI that becomes known to the Privacy Officer. In addition, the Privacy Officer shall comply with the breach notification requirements under HITECH, as described in Section 7 of this Policy.

2.7 The Privacy Officer shall retain documents relating to the Plan's privacy practices, including authorizations, requests for information, complaints and sanctions, for at least six years.

2.8 If the University receives PHI, the University shall amend the Plan document to describe permitted uses and disclosures of PHI and certify to the Privacy Officer that the Plan has been so amended and the University will comply with the amendment to the Plan.

3. Rules Regarding Use and Disclosure of PHI

3.1 Except as otherwise provided in this Policy, only the following employees or workforce members shall have access to PHI:

Vice President for Finance and Administration
Employees in Human Resources, Office of Finance, and Technology Services, and other areas who are required to have access as part of the execution of their duties.

Employees or other workforce members who are permitted access to PHI shall be referred to as "Authorized Employees."

3.2 Authorized Employees may use PHI for Plan administration in connection with payment or health care operations as described in 3.3 below and may disclose only the minimum necessary amount of PHI, pursuant to 3.4 below.

3.3 For purposes of this Policy, payment and health care operations shall have the following meanings:

(a) Payment means the Plan's own payments and the payment by another covered entity, as defined in HIPAA and applicable regulations, and includes, but is not limited to, the following activities:

(1) Obtaining contributions to the Plan.

(2) Determining or paying Plan benefits.

(3) Determining Plan eligibility and coverage, including coordination of benefits and subrogation of claims.

(4) Billing, claims management, collections, and data processing.

(b) Health care operations means the Plan's own operations and those of another covered entity with which the participant or beneficiary has or had a relationship and includes, but is not limited to, the following activities:

(1) Quality control.

(2) Detecting or preventing fraud or abuse.

(3) Medical, legal or auditing review.

(4) Business management and planning.

3.4 Authorized Employees may disclose PHI as follows:

(a) To the person who is the subject of the PHI upon a proper written request to the Privacy Officer.

(b) To the Department of Health and Human Services for purposes of enforcement of HIPAA.

(c) As permitted for legal or public-policy purposes, including, but not limited to, the following disclosures that are limited to the minimum necessary amount of PHI:

(1) About abuse, neglect or domestic violence.

(2) For judicial or administrative proceedings.

(3) For law enforcement purposes.

(4) For public-health or health-oversight activities or for certain limited research purposes or specialized government functions.

(5) In connection with the death of a participant or beneficiary.

(6) For organ or tissue donation purposes.

(7) To avert a serious threat to health or safety.

(8) That relate to workers' compensation programs.

(d) To another Authorized Employee or covered entity in connection with Plan administration, as long as the disclosure is limited to the minimum necessary amount of PHI.

(e) To a business associate, as defined in HIPAA and regulations, if the Privacy Officer confirms that an appropriate agreement with the business associate is in effect and the disclosure is limited to the minimum necessary amount of PHI.

(f) Pursuant to a valid authorization provided by or on behalf of the person who is the subject of the PHI.

4. Practices Regarding Requests by Participants and Beneficiaries

4.1 The Privacy Officer shall give Plan participants and beneficiaries access to their own PHI and the PHI of those whose PHI they are legally entitled to view, upon proper written request to the Privacy Officer, if the PHI is maintained by the University or the Plan and includes information about the enrollment, coverage, payment or claims adjudication record of the person under the Plan.

4.2 The Privacy Officer shall give Plan participants and beneficiaries an accounting of disclosures of the person's PHI made by the Plan or its business associates during the six years preceding the date of the request, subject to the following rules:

(a) The participant or beneficiary is not entitled an accounting of the following types of disclosures:

(1) To carry out treatment, payment or health care operations.

(2) To the participant or beneficiary.

(3) Pursuant to an authorization from or on behalf of the participant or beneficiary.

(4) Incident to an otherwise permitted use or disclosure.

(5) As part of a limited data set.

(6) For national-security or law-enforcement purposes.

(b) Any request must be made to the Privacy Officer in writing and specify the time period and types of disclosures for which the accounting is requested.

(c) The Privacy Officer shall respond to a request for an accounting of disclosures within 60 days, though the deadline shall be extended to 90 days if the Officer notifies the claimant within the original 60-day period explaining the reason for the delay and the date the accounting is expected to be provided.

(d) To the extent the Privacy Officer grants the request for an accounting, the Privacy Officer's response shall include the date and recipient of the disclosure, a brief

description of the information disclosed and a brief statement of the purpose of the disclosure, or a copy of the disclosure request.

(e) The first accounting provided regarding a set of PHI in any 12-month period shall be provided without charge. The Privacy Officer may impose a reasonable charge for additional accountings within any 12-month period.

4.3 The Privacy Officer shall honor a participant's or beneficiary's reasonable written request to receive communications regarding their PHI by alternative means or at an alternative location, if the requester provides information clearly establishing that a failure to honor the request could endanger the requester.

4.4 The Privacy Officer shall honor a participant's or beneficiary's reasonable written request to amend his or her PHI held by the Plan in a designated record set, if the Privacy Officer determines the PHI is not accurate and complete.

(a) The Privacy Officer shall respond to a request for an accounting of disclosures within 60 days, though the deadline shall be extended to 90 days if the Privacy Officer notifies the claimant within the original 60-day period explaining the reason for the delay and the date the accounting is expected to be provided.

(b) To the extent the amendment is denied, the Privacy Officer shall issue a denial notice containing the basis for the denial, information about the requester's right to submit a written statement disagreeing with the denial and the procedure for doing so, a statement that a requester who does not submit a written statement of disagreement may request that the request for amendment and its denial be included in future disclosures of the information and a statement of how the requester may submit a complaint concerning the denial.

(c) The Privacy Officer shall review and respond promptly to any written statement of disagreement.

5. Security Officer

5.1 The University shall designate a person to serve as the Plan's Security Officer (the "Security Officer"). **The Chief Information Officer/ Associate Vice President for Technology Services has been designated as the University's Security Officer.**

5.2 Any person serving as the Security Officer may resign any time with advance written notice to the University. The University may remove the Security Officer without having to show cause. The University shall appoint a new Security Officer as soon as reasonably practicable. Until a new appointment is made, the person with direct authority to appoint the Security Officer, the Vice President for Finance and Administration shall serve as the Security Officer. The Vice President of Finance and Administration has direct authority to appoint the Security Officer.

5.3 The Security Officer shall oversee the design and implementation of the Plan's security practices in accordance with industry standard practices. The Security Officer shall have absolute discretion to carry out its responsibilities under this Policy.

5.4 The Security Officer shall be the security official under HIPAA and applicable regulations and shall comply with HIPAA, applicable regulations and Plan provisions regarding security.

5.5 If the University approves, the Security Officer may delegate all or part of the Security Officer administrative duties to one or more agents and may retain advisors for assistance. The Security Officer may consult with and rely upon the advice of counsel, who may be counsel for the University.

6. Security Practices

6.1 The University shall implement administrative, technical and physical safeguards necessary to reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI created, received, maintained or transmitted on behalf of the Plan. See Attachment A.

6.2 The University shall ensure that any agent, including a subcontractor, to whom the Plan provides electronic PHI agrees to implement reasonable and appropriate security measures to protect the information.

6.3 The University shall train employees, as reasonable and appropriate, regarding the security safeguards so that they are aware of security measures and able to carry out their functions in compliance with the Security Rules**.**

6.4 If the University creates, receives, maintains, or transmits electronic PHI on behalf of the Plan, the University shall amend the Plan document to require the implementation of security safeguards and certify to that the Plan has been so amended and the University will comply with the amendment to the Plan.

7. Data Breach Notification

7.1 **General Notification Requirements.** In the event the Plan discovers a Breach of Unsecured PHI, the Plan will notify each participant or beneficiary whose Unsecured PHI has been, or is reasonably believed by the Plan to have been, accessed, acquired, or disclosed as a result of such Breach, and will provide such other notifications as required by the HITECH Act. This notification requirement applies to any Unsecured PHI accessed, maintained, retained, modified, recorded, stored, destroyed, or otherwise held, used, or disclosed by the Plan.

7.2 **Reporting of Breaches.** Authorized Employees shall report suspected or actual Breaches of Unsecured PHI, immediately, to the Privacy Officer and Security Officer. University employees or workforce members who are not Authorized Employees shall comply with the University's general policies on confidentiality, privacy information and data breach incident response plan.

7.3 **Response to Actual or Suspected Breaches.** The Privacy Officer and the Security Officer shall ensure that an investigation of the actual or suspected Breach is promptly performed, without unreasonable delay. Based on the information obtained during the investigation, a determination shall be made as to whether notification is required.

7.4 **Timing of Notification.** Unless otherwise specified below, the Plan shall provide notifications of a Breach of Unsecured PHI without unreasonable delay and, with respect to individuals whose PHI was the subject of the breach, in no case later than 60 calendar days after the discovery of a Breach. For purposes of this Policy, a breach will be treated as discovered by the Plan as of the first day on which the breach is known to the Plan or, by exercising reasonable diligence, would have been known to any person, other than the individual committing the breach, who is: (a) an Authorized Employee; (b) a workforce member of the Plan; or (c) an agent of the Plan.

7.5 **Delay of Notification.** If a law enforcement official states to the Plan that a notification, notice, or posting required under this section would impede a criminal investigation or cause damage to national security, then the Plan shall:

7.5.1 **Written Statement.** If the statement is in writing and specifies the time for which the delay is required, delay such notification, notice, or posting for the time period specified by the official.

7.5.2 **Oral Statement.** If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily, but no longer than 30 days from the date of the oral statement, unless a written statement, as described above, is submitted during that time.

7.6 **Methods of Notification.** Notification of a Breach of Unsecured PHI shall be provided as follows:

7.6.1 **Notification to Participants and/or Beneficiaries.** Notice of a Breach provided to a participant or beneficiary must meet the requirements described below:

(a) The notice must be written and delivered to the participant or beneficiary by first-class mail addressed to the participant or beneficiary (or the next of kin or personal representative of the participant or beneficiary if the participant or beneficiary is deceased) at the participant's or beneficiary's (or next of kin's or personal representative's) last known address.

(b) In the alternative, if the participant or beneficiary (or next of kin or personal representative) has agreed to electronic notice and such agreement has not been withdrawn, then the notification may be delivered by electronic mail.

(c) In the case in which there is insufficient or out-of-date contact information that precludes direct written (or, if specified by the participant or beneficiary, electronic) notification as required above, a substitute form of notice reasonably calculated to reach the participant or beneficiary shall be provided. In the case where there is insufficient or out-of-date contact information for fewer than ten participants or beneficiaries, substitute notice may be provided by an alternate form of written notice, telephone, or other means. In the case that there are ten or more participants and/or beneficiaries for which there is insufficient or out-of-date contact information, substitute notice shall: (i) be in the form of either a conspicuous posting for a period of 90 days on the home page of the website of the Plan or conspicuous notice in major print or broadcast media in geographic areas where the participants and beneficiaries affected by the Breach likely reside, and (ii) include a toll-free telephone number where a participant or beneficiary can learn whether or not the participant's or beneficiary's Unsecured PHI may be included in the Breach. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notice to the next-of-kin or personal representative of the participant or beneficiary.

(d) If the Plan determines that urgency is required because of possible imminent misuse of Unsecured PHI, then the Plan may provide information to participants and beneficiaries by telephone or other means, as appropriate, in addition to the written notification required. This alternative notice does not obviate the need for written notice.

(e) The notification may be provided in one or more mailings as information becomes available.

7.6.2 **Notification to Media.** For a Breach of Unsecured PHI of more than 500 participants and/or beneficiaries who are residents of an applicable state or jurisdiction, the Plan shall notify prominent media outlets serving the applicable state or jurisdiction.

7.6.3 **Notification to Secretary of the Department of Health and Human Services.** Following the discovery of a Breach of Unsecured PHI, the Plan shall notify the Secretary of the Department of Health and Human Services:

(a) If a distinct Breach involved 500 or more participants and/or beneficiaries, then notification to the Secretary of the Department of Health and Human Services must be provided contemporaneously with the other notifications required above.

(b) If a distinct Breach involved fewer than 500 participants and/or beneficiaries, then the Plan may maintain a log or other documentation of any such Breaches occurring and not later than 60 days after the end of each calendar year and submit the notification concerning the Breaches occurring during the preceding calendar year to the Secretary of the Department of Health and Human Services in the manner specified on its website at http://www.hhs.gov/ocr/privacy.

7.7 **Content of Notification.** Regardless of the method by which notice is provided to participants and beneficiaries as set forth above, notice of a Breach shall include, to the extent possible, the following:

7.7.1 **What Happened.** A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.

7.7.2 **Types of Unsecured PHI.** A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, or disability code, or other types of information where involved).

7.7.3 **Protective Measures.** Any steps participants and beneficiaries should take to protect themselves from potential harm resulting from the Breach.

7.7.4 **Actions by the Plan.** A brief description of what the Plan is doing (a) to investigate the Breach, (b) to mitigate harm to participants and beneficiaries, and (c) to protect against any further Breaches.

7.7.5 **Contact Information.** Contact procedures for participants and beneficiaries to ask questions or learn additional information, which shall include a telephone number, an e-mail address, website, or postal address.

8. Amendment

The University may amend this Policy by a written document signed on behalf of the University that specifically states its intention to amend this Policy.

Attachment A: University of Puget Sound Technology Security Statement

The University of Puget Sound (Puget Sound) recognizes the critical need for privacy as it comes to Protected Health Information (PHI) and complies with Health Insurance Portability and Accountability Act (HIPAA). Drawing on industry best practices and the requirements of federal law, the university has implemented a series of multi-layered security controls to protect the integrity, reliability, and confidentiality of data.

A sample of key security controls in place:

- The university conducts an period risk assessment of information technology assets, defining risk level, potential impact, and probability.
- The university network is protected by firewalls and intrusion detection services. Rules on these devices and services are set to deny all traffic by default, and "allows" are written as exceptions. These devices are updated as appropriate through a change management process and evaluated to ensure the appropriate level of protection based on the sensitivity of the data.
- Servers are housed within a secured network operating center (NOC). The NOC has environmental controls (fire, water, temperature) and is accessible only by authorized personnel. In the event of a power outage, the NOC draws power from an uninterruptable power supply (UPS) and a backup generator.
- Servers are configured based on industry best practices. Only authorized, trained system administrators have administrative privileges. System administrators monitor security mailing lists and sites and update systems as appropriate. Servers are evaluated periodically, and any identified vulnerabilities are assessed and managed. PHI written to any server is scanned by host-based anti-virus software.
- Administrative privileges of information technology personnel are revoked upon termination from the university.
- Most university PHI is stored outside the institution either with the various insurance providers or health care delivery services. Should the university maintain PHI data, information is stored on the university's Enterprise Resource Planning (ERP) system, a separate server infrastructure with limited access and additional security controls.
- To the extent that university PHI is transmitted electronically to insurance providers or business associates, data is stored in a compressed, encrypted file with a secure password before being sent. Daily backups are stored in a tiered structure for disaster recovery purposes and include local and off-site storage. Off-site data is encrypted to prevent compromise and can only be retrieved by authorized personnel.
- No access to data is granted without prior authorization from the appropriate representative in the department responsible for that data.
- Desktops are configured based on industry best practices. Machines have current anti-virus software with updated virus signatures. Desktop authentication and access to network services are centrally managed.
- Security policies are drafted by Technology Services staff and reviewed with various technology committees before being approved by the Chief Technology Officer / Associate Vice President for Technology Services and the President's Cabinet.