OREGON STATE UNIVERSITY EMPLOYEE ASSISTANCE PROGRAM PLAN
HIPAA PRIVACY AND SECURITY POLICY AND PROCEDURES
Effective April 14, 2026

I. Introduction.

Oregon State University (the "University") sponsors the Oregon State University Employee Assistance Program Plan (the "Plan").

The Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act, and their respective implementing regulations, are collectively referred to as "HIPAA" for purposes of this Policy (the "Policy"). HIPAA restricts the Plan's ability to use and disclose protected health information. Members of the University's workforce may have access to protected health information of Plan participants (1) on behalf of the Plan itself; or (2) on behalf of the University, for administrative functions of the Plan performed by the University and for other purposes permitted by HIPAA. This Policy sets forth the Plan's policies and procedures for HIPAA compliance by the Plan and by the University when it receives protected health information from the Plan.

Protected Health Information (PHI). Protected health information (PHI) means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. PHI includes information of persons living or deceased.

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, that is disclosed to the University solely for purposes of obtaining premium bids, or modifying, amending, or terminating the Plan;
2. PHI disclosed to the Plan or the University under a signed authorization that meets the requirements of the HIPAA privacy rules;
3. Health information related to a person who has been deceased for more than 50 years; and
4. Information disclosed to the University by an individual for functions that the University performs in its role as an employer and not as sponsor of the Plan or in providing administrative services to the Plan.

Participant. For purposes of this Policy, participant means any individual who is or has been enrolled in the Plan, including current and former employees and their dependents.

It is the University's policy that the Plan shall comply with HIPAA's requirements for the privacy of PHI. To that end, all members of the University's workforce who have access to PHI must comply with this Policy. The University's workforce includes individuals who are considered part of the workforce under HIPAA, such as employees, volunteers, contractors, trainees, and other persons whose work performance is under the direct control of the University, whether or not they are paid by the University. The term "workforce member" includes all of these types of workers.

No third-party rights in contract or otherwise (including but not limited to rights of participants or Business Associates) are intended to be created by these Policy. The University reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, this Policy shall be aspirational and shall not be binding upon the Plan or the University. 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 and security rules, the HIPAA privacy and security rules shall govern.

II. PRIVACY POLICY

1. Plan's Responsibilities as Covered Entity

A. Privacy Official and Contact Person

Michael Mandzuk, Interim Director Employee Benefits will be the Privacy Official for the Plan. The Privacy Official will be responsible for the development and implementation of policies and procedures relating to privacy of PHI, including but not limited to this Policy and the Plan's Privacy Use and Disclosure Procedures. The Privacy Official will coordinate the Plan's privacy activities with the Plan's Security Official.

Michael Mandzuk, Interim Director Employee Benefits, will be the Plan's Contact Person. Participants who have questions, concerns, or complaints about HIPAA may contact the Contact Person.

The Privacy Official is responsible for ensuring that the Plan complies with all provisions of the HIPAA privacy rules, including the requirement that the Plan have a HIPAA-compliant Business Associate Contract in place with each Business Associate. The Privacy Official shall also be responsible for monitoring compliance by all Business Associates with the terms of their Business Associate Contracts.

B. Workforce Training

It is the University's policy to train all members of its workforce who have access to PHI for familiarity and compliance with the Privacy Policy and Privacy Use and Disclosure Procedures. The Privacy Official is charged with developing training schedules and programs so that all workforce members receive the necessary and appropriate training to permit them to carry out their Plan functions in compliance with HIPAA. Workforce training will be updated as necessary to reflect any changes in policies or procedures and to ensure that workforce members are appropriately aware of their obligations.

C. Safeguards and Firewall

The University will establish on behalf of the Plan appropriate administrative, technical, and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Administrative safeguards include implementing procedures for use and disclosure of PHI, including identifying workforce members who need access to PHI to perform their jobs. Technical safeguards include tracking workforce members' access to PHI. Physical safeguards include locking filing cabinets and doors to rooms storing PHI.

Firewalls will be established to ensure that only authorized workforce members will have access to PHI and that other workforce members do not have access to PHI. Firewalls will also ensure that workforce members have access to only the minimum amount of PHI necessary for the Plan administrative functions

they perform, and that they will not disclose PHI to workforce members who are not authorized to access PHI.

D. Privacy Notice

The Privacy Official is responsible for developing and maintaining a notice of the Plan's privacy practices that complies with the HIPAA privacy rules and describes the following:

- The uses and disclosures of PHI that may be made by the Plan;
- The rights of individuals under HIPAA privacy rules;
- The Plan's legal duties with respect to the PHI; and
- Other information as required by the HIPAA privacy rules.

The privacy notice will inform participants that the University will have access to PHI in connection with the Plan administrative functions. The privacy notice will also provide a description of the Plan's complaint procedures, the name and telephone number of the Contact Person for further information, and the effective date of the notice. The effective date will not be earlier than the date the notice is published.

The notice of privacy practices shall be placed on the Plan's or the University's website. The notice also will be individually delivered:

- At the time of an individual's enrollment in the Plan; and
- To a person requesting the notice;

If Plan there is a material change to the notice, the Plan or the University will prominently post the change or the revised notice on the website by the effective date of the change. Plan

The Plan will also provide notice of availability of the privacy notice (or a copy of the privacy notice) at least once every three years in compliance with the HIPAA privacy regulations.

E. Complaints

The Contact Person will be the Plan's designated person to receive complaints regarding the Plan. The Privacy Official is responsible for creating a process for individuals to lodge complaints about the Plan's privacy procedures and for creating a system for handling such complaints. The complaint procedure is described below.

Individuals wishing to make a complaint are subject to the following procedure.

1) Complaints should be made to:

Oregon State University
Attn: Michael Mandzuk, Interim Director,
Employee Benefits 236 Kerr Administration
Building
Corvallis, OR 97331-2106
michael.mandzuk@oregonstate.edu

2) Complaints may be made by mail or email and do not need to be in any special form.

3) Complaints will be processed as follows:

   a. The existence of the complaint will be documented and retained in Plan records for six years from the date of the complaint.

   b. The Contact Person will notify the Privacy Officer of the existence of the complaint and will share with the Privacy Officer any background information in the Plan's possession that relates to the contents of the complaint.

   c. The Privacy Officer may resolve the complaint directly or delegate its resolution to another individual and may consult with counsel as desired.

   d. After investigating the matter and consulting with counsel as necessary, the Privacy Officer (or their delegee) will provide a written notice of the Plan's disposition of the matter, which the Contact Person shall share with the individual lodging the complaint.

F. Sanctions for Violations of Privacy Policy

Sanctions against workforce members for using or disclosing PHI in violation of HIPAA or this Policy will be imposed in accordance with applicable University policy and procedure, up to and including termination of employment.

G. Mitigation of Inadvertent Disclosures of PHI

The Plan shall mitigate, to the extent possible, any harmful effects that become known to it from a use or disclosure of an individual's PHI in violation of HIPAA or this Policy. As a result, if a workforce member or Business Associate becomes aware of an unauthorized use or disclosure of PHI, either by a workforce member or a Business Associate, the workforce member or Business Associate must contact the Privacy Official without unreasonable delay so that appropriate steps to mitigate harm to the participant 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 participants for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No participant shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment, or eligibility under the Plan.

I. Employer Policy

An employer policy shall include provisions to describe the permitted and required uses by, and disclosures to, the University of PHI for plan administrative or other permitted purposes. Specifically, an employer policy shall require the University to:

- Not use or further disclose PHI other than to the Plan as necessary to operate the Plan or as required by law;
- ensure that there is adequate separation (also known as a firewall) between the Plan and the University as sponsor of the Plan;

- Ensure that any agents to whom it provides PHI agree to the same restrictions and conditions that apply to the University;
- Not use or disclose PHI for employment-related actions or for any other benefit or employee benefit plan of the University;
- Report to the Privacy Official any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- Make PHI available to Plan participants, consider their requests for amendments, and, upon request, provide them with an accounting of PHI disclosures in accordance with the HIPAA privacy rules;
- Make the University's internal practices and records relating to the use and disclosure of PHI received from the Plan available to the Department of Health and Human Services (HHS) upon request; and
- If feasible, return or destroy all PHI received from the Plan that the University 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

The Plan's privacy policies and procedures shall be 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), as well as any changes in the Plan's operations or operating environment. Any changes to policies or procedures must be promptly documented and incorporated into workforce training.

The Plan shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights. The Plan shall also document the dates, content, and attendance of workforce members at training sessions.

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

2. Use and Disclosure of PHI

A. Use and Disclosure Defined

The 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 University workforce member with a job description including the processing of employee benefits, or by a Business Associate of the Plan.

Disclosure. The release, transfer, provision of access to, or divulging in any other manner of PHI to persons who are not University workforce members with access (see subsection C below) , or to a person or entity who is not a Business Associate of the Plan.

B. Workforce Must Comply with Plan's Policy and Procedures

All members of the University's workforce who have access to PHI must comply with this Policy, including the Detailed Procedures for Use and Disclosure set forth in section II.4 below.

C. Permitted Uses and Disclosures for Plan Administration Purposes

The Plan may disclose PHI to the following University workforce members to perform Plan administrative functions ("workforce members with access"):

1. University Human Resources team members who work in the following positions:
   - Benefits Specialists;
   - Work Life Coordinator;
   - Benefits Manager; and
   - Executive Director of University Human Resources

2. University Information and Technology team members who work in the following positions:
   - Data Product Manager
   - Lead Data Modeler
   - Analyst Programmer
   - Data and Integration Engineers

3. Attorneys within the Office of General Counsel for purposes of providing legal advice to the Plan.

Workforce members will be given access to the minimum necessary PHI to complete their job functions.

Workforce members with access may disclose PHI to other workforce members with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Workforce members with access may not disclose PHI to any other workforce members unless a valid, signed authorization is in place or the disclosure otherwise is in compliance with this Policy and the Plan. Workforce members with access must take all appropriate steps to ensure that the PHI is not disclosed, available, or used for employment purposes. For purposes of this Policy, "plan administrative functions" include the payment and health care operation activities described in section III.D of this Policy.

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

PHI may be disclosed for the Plan's own payment purposes, and PHI may be disclosed to another covered entity for the payment purposes of that covered entity.

Payment. Payment includes activities undertaken to obtain participants' contributions to the Plan, if any, or to determine or fulfill the Plan's responsibility to obtain or provide reimbursement for health care. Payment also includes the following:

- Eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;

- Risk-adjusting based on characteristics of the covered group of participants;
- 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 activity permitted by the HIPAA privacy regulations.

PHI may be disclosed for purposes of the Plan's own health care operations. 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 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 regulations.

E. No Disclosure of PHI for Non-Plan Purposes

PHI may not be used or disclosed for the payment or operations of the University's "non-Plan" benefits (e.g., disability, workers' compensation, life insurance), unless the participant has provided an authorization for such use or disclosure (as discussed in "Disclosures Pursuant to an Authorization") or such use or disclosure is required or allowed by applicable state law and all applicable requirements under HIPAA are met.

F. Mandatory Disclosures of PHI

A participant's PHI must be disclosed, in the following situations:

- The disclosure is to the individual who is the subject of the information (see Section II.4.G. below.;
- The disclosure is required by law; or
- The disclosure is made to HHS for purposes of enforcing HIPAA.

G. Other Permitted Disclosures of PHI

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. Section II.4 B. describes specific requirements that must be met before these types of disclosures may be made. The requirements include prior approval of the Privacy Official. Permitted are disclosures-

- About victims of abuse, neglect, or domestic violence;
- To a health care provider for treatment purposes;
- For judicial and administrative proceedings;

- For law-enforcement purposes;
- For public health activities;
- For health oversight activities;
- 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.

H. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

I. Complying With the "Minimum-Necessary" Standard

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

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.

Minimum Necessary When Disclosing PHI. The Plan, when disclosing PHI subject to the minimum-necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI that is necessary for the requestor is disclosed. More details on disclosure requirements are found in Section II.4. All disclosures not discussed in this Policy and subject to the minimum necessary standard must be reviewed on an individual basis with the Privacy Official to ensure that the amount of PHI disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. The Plan, when requesting PHI subject to the minimum-necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI necessary for the Plan is requested. More details on disclosure requirements are found in Section II. 4. All requests not discussed in this Policy 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.

J. Disclosures of PHI to Business Associates

A Business Associate is an entity that-

- Creates, receives, maintains, or transmits PHI on behalf of the Plan (including for claims processing or administration, data analysis, or underwriting); or

- Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services to or for the Plan, where the performance of such services involves giving the service provider access to PHI.
- Workforce members may disclose PHI to Business Associates and allow Business Associates to create, receive, maintain, or transmit PHI on the Plan's behalf. However, prior to doing so, the Plan must first obtain satisfactory assurances from the Business Associate, in the form of a business associate contract, that it will appropriately safeguard PHI. The Privacy Official shall maintain a log of all Business Associates and shall maintain all Business Associate Contracts in a readily accessible and retrievable form and format.

K. Disclosures of De-Identified Information

The Plan may use and disclose information that has been "de-identified" in accordance with the HIPAA privacy regulations. 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.

L. Breach Notification Requirements

The Plan will comply with the Reportable Breach Notification Policy set forth in Appendix A of this Policy.

3. Individual Rights

HIPAA gives participants the right to access and obtain copies of their PHI that the Plan (or its Business Associates) maintains in a designated record set. A participant's personal representative may request access to PHI on behalf of the participant. The Plan will provide access to PHI in accordance with HIPAA.

A Designated Record Set is a group of records maintained by or for the Plan that includes-

- The enrollment, payment, and claims adjudication record of a participant that is maintained by or for the Plan; or
- Other PHI used, in whole or in part, by or for the Plan to make coverage decisions about an individual.
- Participants will be instructed to send their requests for access to the Plan's Contact Person. The Plan will take reasonable efforts to verify the identity of the requesting participant following the procedures set forth in Section II.4. D. The Plan will attempt to provide participants with access to their PHI as soon as possible, and within 30 days, after receiving a written request. If the Plan is unable to provide access within 30 days, it may extend the response by up to 30 additional days so long as it communicates the reason for the extension to the participant and the estimated response date within the initial 30-day period.

The Plan will send requested information in a Designated Record Set to a third party identified by the participant, so long as the request is signed and in writing, and clearly identifies the third party and where to send the information.

Generally, the Plan will not deny participants access to their own PHI. However, if an exception to the right to access set forth in 45 CFR §164.524 exists, the Privacy Official will review the request for access and will respond within the timeframe and with the information required by the privacy rule.

If information in one or more Designated Record Sets is maintained electronically, and an individual requests an electronic copy of the information, the Plan will provide the individual with access to the requested information in the electronic form and format requested by the individual, if it is readily producible in that form and format. If the requested information is not readily producible in that form and format, the requested information will be produced in a readable electronic form and format as agreed by the Plan and the individual. If the Plan and the individual are unable to agree on an electronic form and format, the Plan will provide a paper copy of the information to the individual.

The Plan will send information to the participant by mail or email, as requested by the participant. However, if a participant asks to receive a copy of PHI by unencrypted email, the Plan will provide a brief warning to the participant that there is some level of risk that the participant's PHI could be read or otherwise accessed by a third party while in transit and confirm that the participant still wants to receive PHI by unencrypted email. If the participant says yes, the Plan will comply with the request. Because of the security risk, the Plan will not copy information onto participant-supplied storage media.
If a participant requests a copy of information in a Designated Record Set, the Plan may impose a reasonable, cost-based fee, provided that the fee includes only the cost of (1) labor for copying the information requested by the participant, whether in paper or electronic form; (2) supplies for creating the paper copy or electronic media if the participant requests that the electronic copy be provided on portable media; and (3) postage, when the participant has requested that the copy be mailed. If the participant agrees to receive an explanation or summary, the Plan may charge for preparing the explanation or summary, if the participant agrees in advance. The Plan may not charge a fee to participants who merely request access to (but not copies of) information.

If a participant believes that PHI about the participant in a Designated Record Set is incorrect or incomplete, the participant may ask the Plan to amend the PHI. The participant has the right to request an amendment for as long as the information is kept by or for the Plan. The request for amendment must be made in writing and submitted to the Plan's Contact Person. In addition, the participant must provide a reason that supports the request. The Plan may deny the request for an amendment if it is not in writing or does not include a reason to support the request.

The Plan will act on the request as soon as possible, and within 60 days, after receiving the request. If the Plan is unable to act on the request within 60 days, it may extend the period for up to 30 additional days, provided that the Plan notifies the participant of the reason for the delay and the date it will act on the request during the original 60-day period.

In addition, the Plan may deny the request if the request is to amend information that-

- Was not created by the Plan, unless the participant provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
- Is not part of a Designated Record Set;
- Is not subject to the right of access described above; or
- Is accurate and complete.

If the Plan denies the request, it will provide the participant with a written explanation of the basis for the denial, the participant's right to file a statement of disagreement with the Plan, and the Plan's complaint procedures. Any future disclosures of the disputed information will include that statement.

A participant has the right to obtain an accounting of certain disclosures of their own PHI. This right to an accounting extends to disclosures made in the most recent six years, other than disclosures:

- To carry out treatment, payment, or health care operations;
- To individuals about their own PHI;
- Incident to an otherwise permitted use or disclosure;
- Pursuant to an authorization;
- To persons involved in the individual's care or payment for the individual's care or for certain other notification purposes;
- To correctional institutions or law enforcement when the disclosure was permitted without authorization;
- As part of a limited data set;
- For specific national security or law-enforcement purposes; or
- Disclosures that occurred prior to the compliance date.

Participants shall be instructed to send their requests for an accounting to the Plan's Contact Person. The Plan shall respond to an accounting request within 60 days. If the Plan is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant 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 shall be provided free of charge. The Privacy Official may impose reasonable production and mailing costs for additional accountings.

Participants may ask to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may request that Plan information be sent only to their work address rather than a home address or may request that communications be made by phone. Participants will be instructed to send their requests to the Plan's Contact Person. The decision to honor a request shall be made by the Privacy Official.

A participant may request restrictions on the use and disclosure of the participant's PHI. Plan Participants will be instructed to send their requests to the Plan's Contact Person. The Plan may, but need not, honor such requests. However, the Plan will comply with a restriction request if (1) except as otherwise required by law, the disclosure is to a Plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (2) the PHI pertains solely to a health care item or service for which the health care provider involved has been paid in full by the individual or another person, other than the Plan. The decision to honor restriction requests shall be made by the Privacy Official.

4. Detailed Procedures for Use and Disclosure of PHI

Where a term has been defined within another part of this Policy, those definitions continue to apply here.

Many use and disclosure rules are articulated within this Policy. This Procedures for Use and Disclosure of PHI supplements and provides additional detail to the otherwise stated use and disclosure rules.

A. Permissive Disclosures of PHI: For Legal and Public Policy Purposes

- *Disclosures for Legal or Public Policy Purposes.* A workforce member who receives a request for disclosure of an individual's PHI that appears to fall within one of the categories described below under "Legal and Public Policy Disclosures Covered" must contact the Privacy Official. Disclosures may be made under the following procedures:
    - The disclosure must be approved by the Privacy Official.
    - Disclosures must comply with the "Minimum-Necessary Standard" unless otherwise required by law.
    - Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

B. Legal and Public Policy Uses and Disclosures Covered

- *Victims of Abuse, Neglect, or Domestic Violence*, if the following conditions are met:
    - The individual agrees with the disclosure; or
    - The disclosure is expressly authorized by statute or regulation and the disclosure is necessary to prevent harm to the individual (or other potential victims) or the individual is incapacitated and unable to agree and the information will not be used against the individual and is necessary for an immediate enforcement activity. In this case, the individual must be promptly informed of the disclosure unless this would place the individual at risk of serious harm or if informing the individual would involve a personal representative who is believed to be responsible for the abuse, neglect, or violence and informing that person would not be in the best interest of the individual, as determined by the Privacy Official in the exercise of professional judgment.
- *Judicial and Administrative Proceedings*, in response to:
    - An order of a court or administrative tribunal (provided that disclosure must be limited to PHI expressly authorized by the order); and
    - A subpoena, discovery request or other lawful process, not accompanied by the order of a court or administrative tribunal, upon receipt of assurances that the individual has been given notice of the request, or that the party seeking the information has made reasonable efforts to obtain a qualified protective order.
- *Law-Enforcement Official for Law-Enforcement Purposes*, under the following conditions:
    - Pursuant to a legal process and as otherwise required by law, but only if the information sought is relevant and material to a legitimate law-enforcement inquiry, 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 de-identified information could not reasonably be used.
    - Information requested is limited information to identify or locate a suspect, fugitive, material witness, or missing person.
    - Information about an individual who is a victim or a suspected victim of a crime (1) if the individual agrees to disclosure; or (2) without agreement from the individual, if the information is not to be used against the victim, is needed to determine whether a violation of law occurred, the need for the information is urgent, and disclosure is in the best interest of the individual as determined by the Privacy Official in the exercise of professional judgment.
    - Information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct.

    - Information that constitutes evidence of criminal conduct that occurred on the University's premises.
- *Appropriate Public Health Authorities for Public Health Activities.*
- *Health Oversight Agency for Health Oversight Activities,* as authorized by law.
- *Coroner or Medical Examiner About Decedents,* for the purpose of identifying a deceased person, determining the cause of death, or other duties as authorized by law.
- *Cadaveric Organ, Eye or Tissue Donation Purposes,* to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes, or tissue for the purpose of facilitating transplantation.
- *Certain Limited-Research Purposes,* provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board.
- *Avert a Serious Threat to Health or Safety,* upon a good faith belief that the use or disclosure is necessary to prevent a serious and imminent threat to the health or safety of a person or the public, and the use or disclosure is to a person reasonably able to prevent or lessen the threat, including to the target of the threat.
- *Specialized Government Functions,* including disclosures of an inmate's PHI to correctional institutions and disclosures of an individual's PHI to authorized federal officials for the conduct of national security activities.
- *Workers' Compensation Programs,* to the extent necessary to comply with laws relating to workers' compensation or other similar programs providing benefits in case of occupational illness or injury.

C. Requests From Spouses, Family Members, and Friends for Disclosure of PHI

The Plan and the University will not disclose PHI to family and friends of an individual except as required or permitted by HIPAA. Generally, an authorization is required before another party, including spouse, family member, or friend, will be able to access PHI. However, minimum necessary PHI may be disclosed though an EOB sent in connection with services received under the Plan.

- If a workforce member receives a request for disclosure of an individual's PHI from a spouse, family member, or personal friend of an individual, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is a minor child; or (2) the personal representative of the individual, then follow the procedure for "Verification of Identity of Those Requesting Protected Health Information" in subsection D. below.
- Once the identity of a parent or personal representative is verified, then follow the procedure for "Request for Individual Access."
- All other requests from spouses, family members, and friends must be authorized by the individual whose PHI is involved. See the procedures for "Disclosures Pursuant to Individual Authorization." in subsection G. below.

D. Verification of Identity of Those Requesting Protected Health Information

Verifying Identity and Authority of Requesting Party. Workforce members with access must take steps to verify the identity of individuals who request access to PHI. They must also verify the authority of any person to have access to PHI, if the identity or authority of such person is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, a parent seeking access to the PHI of their minor child, a personal representative, or a public official seeking access.

- *Request Made by Individual.* When an individual requests access to their own PHI, the following steps should be followed:

- Request a form of identification from the individual. Workforce members may rely on a valid driver's license, passport, or other photo identification issued by a government agency.
- Verify that the identification matches the identity of the individual requesting access to the PHI. If there is any doubt as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, the workforce member should contact the Privacy Official.
- Make a copy of the identification provided by the individual and file it with the individual's designated record set.
- If the individual requests PHI over the telephone, the individual's Social Security Number will be requested to confirm identity.
- Disclosures must be documented in accordance with the procedure for "Documentation Requirements" in subsection E. below

- *Request Made by Parent Seeking PHI of Minor Child.* When a parent requests access to the PHI of the parent's minor child, the following steps should be followed:
  - Seek verification of the person's relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent.
  - Disclosures must be documented in accordance with the procedure "Documentation Requirements" in subsection E. below.
- *Request Made by Personal Representative.* When a personal representative requests access to an individual's PHI, the following steps should be followed:
  - Require a copy of a valid power of attorney or other documentation establishing the representative's right to make health care decisions on behalf of the individual-requirements may vary state-by-state. If there are any questions about the validity of this document, seek review by the Privacy Official.
  - Make a copy of the documentation provided and file it with the individual's designated record set.
  - Disclosures must be documented in accordance with the procedure for "Documentation Requirements" in subsection E. below.
- *Request Made by Public Official.* If a public official requests access to PHI, and if the request is for one of the purposes set forth above in "Mandatory Disclosures of PHI" (Section II.2.F.) or "Permissive Disclosures of PHI," (Section II.4.A) the following steps should be followed to verify the official's identity and authority:
  - If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status. Make a copy of the identification provided and file it with the individual's designated record set.
  - If the request is in writing, verify that the request is on the appropriate government letterhead;
  - If the request is by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or obtain other evidence or documentation of authority, 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.
  - Request 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. If the individual's 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, contact the Privacy Official.
  - Obtain approval for the disclosure from the Privacy Official.

- Disclosures must be documented in accordance with the procedure for "Documentation Requirements" in subsection E. below.

E. Documentation

Documentation. Workforce members shall maintain copies of all of the following items for a period of at least six years from the date the documents were created or were last in effect, whichever is later:

- "Notices of Privacy Practices" that are issued to participants;
- Copies of policies and procedures;
- Individual authorizations;
- When disclosure of "certain" PHI, as identified in the next bullet is made:
  - the date of the disclosure;
  - the name of the entity or person who received the PHI and, if known, the address of such entity or person;
  - a brief description of the PHI disclosed;
  - a brief statement of the purpose of the disclosure; and
  - any other documentation required under these Use and Disclosure Procedures.

- The following qualify as "certain" PHI as referenced in the preceding bullet point:

  - accidental disclosures or breaches of unsecured PHI (for example, providing PHI to a company that you mistakenly thought was a business associate);
  - disclosures required by law (for example, reports to state or federal agencies and disclosures made to the Secretary of HHS pursuant to the Secretary's authority to investigate the covered entity's compliance with the administrative simplification regulations);
  - disclosures listed in 45 CFR §164.512, such as disclosures that are necessary to comply with workers' compensation laws; and
  - disclosures to law enforcement and pursuant to a subpoena or court order.

F. Mitigation of Inadvertent Disclosures of PHI

Mitigation: Reporting Required. HIPAA requires that a covered entity mitigate, to the extent possible, any harmful effects that become known to the Plan of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this manual. As a result, anyone who becomes aware of a disclosure of PHI, whether by a workforce member, a Business Associate, or other outside consultant/contractor, that is not in compliance with the policies and procedures set forth in this manual, should contact the Privacy Official without unreasonable delay so that the appropriate steps to mitigate the harm to the individual can be taken.

G. Procedures for Complying with Individual Rights

"Designated Record Set" Defined

Designated Record Set is a group of records maintained by or for the University that includes:

- the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or
- other protected health information used, in whole or in part, by or for the Plan to make coverage

decisions about an individual.

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or from a minor's parent or an individual's personal representative) for disclosure of an individual's PHI to the individual or to a third party, the workforce member must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- Review the disclosure request to determine whether the PHI requested is held in one or more designated record sets. See the Privacy Official if it appears that the requested information is not held in any designated record set. *No request for access may be denied without approval from the Privacy Official.*
- Review the disclosure request to determine whether an exception to the disclosure requirement might exist; for example, disclosure may be denied for requests to access psychotherapy notes, documents compiled for a legal proceeding, certain requests by inmates, information compiled for research purposes if the individual has agreed to denial of access, information obtained under a promise of confidentiality, and other disclosures that are determined by a health care professional to be likely to cause harm. See the Privacy Official if there is any question about whether one of these exceptions applies. *No request for access may be denied without approval from the Privacy Official.*
- Respond to the request by providing the information or denying the request within 30 days. If the requested PHI cannot be accessed within the 30-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 30-day period, explaining the reasons for the extension and the date by which the University will respond.
- A Denial Notice must contain (1) the basis for the denial; (2) a statement of the individual's right to request a review of the denial, if applicable; and (3) a statement of how the individual may file a complaint concerning the denial. All notices of denial must be prepared or approved by the Privacy Official.
- Provide the information requested in a readable hard copy form. Individuals (except for inmates) have the right to receive a copy by mail or by email or can come in and pick up a copy. Individuals (including inmates) also have the right to come in and inspect the information.
- If the PHI requested is maintained electronically in one or more designated record sets, and the individual requests an electronic copy of such information, the Plan will provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; if the PHI is not readily producible in such form and format, the PHI will be produced in a readable electronic form and format as agreed by the Plan and the individual. If the Plan and the individual cannot agree on an acceptable electronic form and format, the Plan will provide a paper copy of the information.
- If the individual has requested a summary and explanation of the requested information in lieu of, or in addition to, the full information, prepare such summary and explanation of the information requested and make it available to the individual in the form or format requested by the individual.
- Disclosures must be documented in accordance with the procedure "Documentation Requirements."

H. Processing Requests for an Accounting of Disclosures of Protected Health Information

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request

from an individual (or a minor's parent or an individual's personal representative) for an accounting of disclosures, the workforce member must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- If the individual requesting the accounting has already received one accounting within the 12-month period immediately preceding the date of receipt of the current request, prepare a notice to the individual informing him or her that a fee for processing will be charged and providing the individual with a chance to withdraw or revise the request.
- Respond to the request within 60 days by providing the accounting (as described in more detail below) or informing the individual that there have been no disclosures that must be included in an accounting (see the list of exceptions to the accounting requirement below). If the accounting cannot be provided within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the University will respond.
- The accounting must include disclosures (but not uses) of the requesting individual's PHI made by the Plan and any of its business associates during the period requested by the individual up to six years prior to the request. The accounting does not have to include disclosures made:
    - to carry out treatment, payment, and health care operations;
    - to the individual about his or her own PHI;
    - incident to an otherwise permitted use or disclosure;
    - pursuant to an individual authorization;
    - to persons involved in the individual's care or payment for the individual's care or for certain other notification purposes;
    - for specific national security or intelligence purposes;
    - to correctional institutions or law enforcement when the disclosure was permitted without an authorization; and
    - as part of a limited data set.
- Business Associates of the Plan are also required to comply with HIPAA in disclosing PHI.

I. Processing Requests for Confidential Communications

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) to receive communications of PHI by alternative means or at alternative locations, the workforce member must take the following steps

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- Determine whether the request contains a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.
- The workforce member should take steps to honor requests if the individual states that disclosure could endanger the individual.
- If a request will not be accommodated, the workforce member must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.
- All confidential communication requests that are approved will be documented.

J. Processing Requests for Restrictions on Uses and Disclosures of Protected Health Information

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for a restriction on the use and/or disclosure of the individual's PHI, the workforce member must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- The Plan will comply with a restriction request if (1) except as otherwise required by law, the disclosure is to a Plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment), and (2) the PHI pertains solely to a health care item or service for which the health care provider has been paid in full by the individual or another person, other than the Plan.
- If a request will not be accommodated, the workforce member must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.

III. SECURITY POLICY & PROCEDURES

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act), and their implementing regulations and guidance require the Plan to implement various security measures with respect to electronic protected health information (electronic PHI).

Electronic PHI is PHI that is transmitted by or maintained in electronic media.

Electronic Media means:

(1) Electronic storage material on which data is or may be recorded electronically, including 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, extranet, intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, voice via telephone, and facsimile, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

No third-party rights (including but not limited to rights of Plan participants, beneficiaries, or covered dependents) are created by this Policy. The 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 Plan. This Policy does not address requirements under state law or federal laws other than HIPAA.

A. Security Official

David McMorries, Assistant Vice Provost & Chief Information Security Office, is the Security Official for the Group Plan.

B. Risk Analysis

The Plan will rely on the risk analysis performed by the Plan Sponsor (University) to identify threats, vulnerabilities, and risks to electronic PHI.

C. Risk Management

The Plan relies on the Plan Sponsor to identify and manage risks to electronic PHI by limiting vulnerabilities to a reasonable and appropriate level, taking into account the following:

- The Plan Sponsor's and the Plan's size, complexity, and capabilities;
- The Plan Sponsor's and the Plan's technical infrastructure, hardware, software, and security capabilities;
- The costs of security measures; and
- The criticality of the electronic PHI potentially affected and the probability of the various risks.

D. Administrative, Physical, and Technical Safeguards

HIPAA's security rule requires the Plan Sponsor to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the Plan Sponsor creates, receives, maintains, or transmits on behalf of the Plan. The Plan adopts the following safeguards implemented by the Plan Sponsor:

Standard	**Implementation Specification**	**Documentation**	**Description**
Administrative Safeguards			
Security Management Process	Sanction Policy (Required)	Acceptable Use of Computing Resources Policy; Conditions of Service Policy; Corrective Discipline and Termination for Cause of Professional Faculty Appointment Policy; and applicable collective bargaining agreements.	Apply appropriate sanctions against workforce members who fail to comply with the Plan's security policies and procedures.
	Information System Activity Review (Required)	Security Operations Center Standard Operating Procedure.	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
Assigned Security Responsibility	No implementation specifications	Security official appointed in this Policy.	Appoint a security official.

Workforce Security	Authorization and/or Supervision	Access to PHI only granted to those who have a business need, as designated in the position description for the relevant position; Identity Access Management Standard Operating Procedure; and University Information and Technology Unit Rule on Passwords.	Implement procedures for the authorization and supervision of workforce members who work with electronic PHI or who work in locations where it might be accessed.
	Workforce Clearance Procedure	Access to PHI only granted to those who have a business need, as designated in the position description for the relevant position; Identity Access Management Standard Operating Procedure; and University Information and Technology Unit Rule on Passwords.	Implement procedures to determine that a workforce member's access to electronic PHI is appropriate.
	Termination Procedures	Identity Access Management Standard Operating Procedure.	Implement procedures to terminate access to electronic PHI when the employment of a workforce member ends, or when it is determined that it is not appropriate for a certain workforce member to have access to electronic PHI.
Information Access Management	Access Authorization	Identity Access Management Standard Operating Procedure.	Implement procedures to grant access to electronic PHI, for example, through access to a workstation, transaction, program, process, or other mechanism.

	Access Establishment and Modification	Identity Access Management Standard Operating Procedure.	Implement procedures that, based on the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
Security Awareness and Training	Security Reminders	OSU Critical Training Program; and HIPAA specific training for employees with access to PHI.	Implement procedures to distribute periodic security updates.
	Protection From Malicious Software	Security Operations Center Standard Operating Procedure.	Implement procedures to guard against, detect, and report malicious software.
	Login Monitoring	Identity Access Management Standard Operating Procedure.	Implement procedures to monitor login attempts and to report discrepancies.
Administrative Safeguards			
	Password Management	Identity Access Management Standard Operating Procedure; and University Information and Technology Unit Rule on Passwords.	Implement procedures to create, change, and safeguard passwords.
Security Incident Procedures	Response and Reporting (Required)	Security Operations Center Standard Operating Procedure; and University Data Management, Classification, and Incident Response Policy.	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the entity; and document security incidents and their outcomes.
Contingency Plan	Data Backup Plan (Required)	Technical Services Architecture Standard Operating Procedure.	Establish and implement procedures to create and maintain retrievable, exact copies of electronic PHI.

	Disaster Recovery Plan (Required)	Technical Services Architecture Standard Operating Procedure	Establish (and implement as needed) procedures to restore any loss of data.
	Emergency Mode Operation Plan (Required)	Technical Services Architecture Standard Operating Procedure; and Security Operations Center Standard Operating Procedure.	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.
	Testing and Revision Procedures (Addressable)	Technical Services Architecture Standard Operating Procedure; and Banner Business Recovery Plan.	Implement procedures for periodic testing and revision of contingency plan.
	Applications and Data Criticality Analysis (Addressable)	Technical Services Architecture Standard Operating Procedure	Assess the relative criticality of specific applications and data in support of other contingency plan components.
Evaluation	No implementation specifications	Annual external audit; Governance, Risk and Compliance Standard Operating Procedure.	Perform periodic technical and nontechnical evaluations of safeguards.
Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement (Required)	Business Associate Agreements are in place as required.	Document the business associate's satisfactory assurances through a written contract or other arrangement that meets the requirements of the security rule.
Physical Safeguards			
Facility Access Controls	Contingency Operations (Addressable)	Governance, Risk, and Compliance Standard Operating Procedure	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operation plan.

	Facility Security Plan (Addressable)	Governance, Risk and Compliance Standard Operating Procedure; Standard access measures	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
Physical Safeguards			
	Access Control and Validation Procedures (Addressable)	Identity Access Management Standard Operating Procedure.	Implement procedures based on a person's role or function to control and validate his or her access to facilities, including visitor control and control of access to software programs for testing and revision.
	Maintenance Records (Addressable)		Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).
Workstation Use	No implementation specifications	Identity Access Management Standard Operating Procedure; and Endpoint Standard Operating Procedure.	Implement policies and procedures that specify the proper functions, performance, and physical attributes of workstations that can access electronic PHI.
Workstation Security	No implementation specifications	Identity Access Management Standard Operating Procedure; and Endpoint Standard Operating Procedure.	Implement safeguards that permit only authorized users to gain physical access to workstations that can access electronic PHI.
Device and Media Controls	Disposal (Required)	Endpoint Standard Operating Procedure.	Implement policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored.

	Media Reuse (Required)	Endpoint Standard Operating Procedure.	Implement procedures for removal of electronic PHI from electronic media before the media are made available for reuse.
	Accountability (Addressable)		Maintain a record of the movements of hardware and electronic media and any person responsible therefor.
	Data Backup and Storage (Addressable)	Security Operations Center Standard Operating Procedure.	Create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment.
Technical Safeguards			
Access Control	Unique User Identification (Required)	Identity Access Management Standard Operating Procedure.	Assign a unique user name and/or number for identifying and tracking user identity.
	Emergency Access (Required)	Identity Access Management Standard Operating Procedure.	Establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency.

Technical Safeguards			
	Automatic Logoff (Addressable)	Endpoint Standard Operating Procedure.	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
	Encryption and Decryption (Addressable)	Endpoint Standard Operating Procedure.	Implement a mechanism to encrypt and decrypt electronic PHI (at rest).
Audit Controls	No implementation specifications	Security Operations Center Standard Operating Procedure.	Implement hardware, software, and/or procedures to record and examine activity in systems that store or use electronic PHI.

Integrity	Mechanism to Authenticate Electronic PHI (Addressable)	Security Operations Center Standard Operating Procedure.	Implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.
Person or Entity Authentication	No implementation specifications	Requirements are set forth in this Policy.	Implement procedures to verify the identity of a person or entity seeking access to electronic PHI.
Transmission Security	Integrity Controls (Addressable)	Endpoint Standard Operating Procedure.	Implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection.
	Encryption (Addressable)	Endpoint Standard Operating Procedure.	Implement a mechanism to encrypt electronic PHI (in transit) whenever it is deemed appropriate.
Organizational Requirements			
Business Associate Contracts or Other Arrangements	Business Associate Contracts or Other Arrangements (Required)	Business Associate Agreements are in place as required.	The Plan may not permit a business associate to create, receive, maintain, or transmit electronic PHI on the Plan's behalf without a business associate contract (or, in limited cases, another arrangement).
Organizational Relationships	Administrative, Physical, and Technical Safeguards; Agents and Subcontractors; Adequate Separation; Report (Required)	Since OSU is not subject to ERISA, there is no plan document; to meet this requirement, we have adopted the Oregon State University Policy on Protected Health Information.	Plan may not disclose electronic PHI to the Plan Sponsor unless the plan document has been amended to require that the Plan Sponsor implement certain safeguards and take certain other steps.

E. Disclosures of Electronic PHI to Third-Party Administrator and Other Business Associates

The Plan permits any third-party administrator and business associates to create, receive, maintain, or transmit electronic PHI on its behalf. The Plan has obtained or will obtain satisfactory assurances from

all business associates that they will appropriately safeguard the electronic PHI. Such satisfactory assurances shall be documented through a written contract requiring compliance with all of the requirements of the HIPAA security regulations.

F. Breach Notification Requirements

The Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of its business associates discovers a breach of unsecured PHI.

G. Documentation

The Plan's security policies and procedures shall be documented, reviewed periodically, and updated as necessary to respond to environmental or operational changes affecting the security of Plan electronic PHI, and any necessary changes to policies or procedures will be documented and implemented promptly. Policies, procedures, and other documentation controlled by the Plan may be maintained in either written or electronic form. The 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 Plan will make its policies, procedures, and other documentation available to the Security Official and the Plan Sponsor, the third-party administrator, and other business associates or other persons to the extent they are responsible for implementing the procedures to which the documentation pertains. The Plan may limit disclosures of policies and procedures if it determines that providing access to the policies and procedure would pose a security risk.

APPENDIX A: REPORTABLE BREACH NOTIFICATION POLICY

I. Introduction

This Reportable Breach Notification Policy is adopted by the Plan as part of its Privacy Policy and is intended to comply with the final HITECH regulations for breaches occurring on or after September 23, 2013 ("Breach Regulations"). Under the Breach Regulations, if a Reportable Breach of unsecured PHI has occurred, the Plan must comply with certain notice requirements with respect to the affected individuals, HHS, and, in certain instances, the media.

II. Identifying a Reportable Breach

The first step is to determine whether a Reportable Breach has occurred. If a Reportable Breach has not occurred, the notice requirements do not apply.

The Privacy Official is responsible for reviewing the circumstances of possible breaches brought to their attention and determining whether a Reportable Breach has occurred in accordance with this Reportable Breach Notification Policy and the Breach Regulations. All Business Associates, and all workforce members who have access to PHI, are required to report to the Privacy Official any incidents involving possible breaches.

Acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted under the privacy rules is presumed to be a Reportable Breach, unless the Privacy Official determines that there is a low probability that the privacy or security of the PHI has been or will be compromised.

The Privacy Official's determination of whether a Reportable Breach has occurred must include the following considerations:

Was there a 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 Plan or a Business Associate of the Plan. If not, then the notice requirements do not apply.

Was PHI involved? If not, then the notice requirements do not apply.

Was the PHI secured? For electronic PHI to be "secured," it must have been encrypted to NIST standards or destroyed. For paper PHI to be "secured," it must have been destroyed. If yes, then the notice requirements do not apply.

Was there unauthorized access, use, acquisition, or disclosure of PHI? The violation of HIPAA Privacy Rules must have involved one of these. If it did not, then the notice requirements do not apply.

Does an exception apply? The regulations contain three narrow exceptions to breach notification (described below).

Is there a low probability that privacy or security was compromised? If the Privacy Official determines that there is only a low probability of compromise, then the notice requirements do not apply.

If one of the following three exceptions applies, then a Reportable Breach has **not** occurred, and the notice requirements are not applicable.

Exception 1: A Reportable Breach does not occur if the breach involved an unintentional access, use, or acquisition of PHI by a workforce member or Business Associate, if the unauthorized access, use, acquisition, or disclosure (a) was in good faith; (b) was within the scope of authority of the workforce member or Business Associate; and (c) does not involve further use or disclosure in violation of the HIPAA privacy rules. For example, the exception might apply if an employee providing administrative services to the Plan were to mistakenly access the claim file of a participant whose name is similar to the name of the intended participant. However, the exception would not apply if an employee intentionally looked up a coworker's claim file out of curiosity.

Exception 2: A Reportable Breach has not occurred if the breach involved an inadvertent disclosure from one person authorized by the Plan to have access to PHI to another person at the same covered entity or Business Associate also authorized to have access to the PHI, provided that there is no further use or disclosure in violation of the HIPAA privacy rules. For example, the exception might apply if an employee providing administrative services to the Plan inadvertently emailed PHI to the wrong coworker. However, if the same employee emailed the information to an unrelated third party, the exception likely does not apply.

Exception 3: A Reportable Breach has not occurred if the breach involved a disclosure where the Plan has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI. For example, the exception may apply to an EOB mailed to the wrong person and returned to the Plan unopened, or if a report containing PHI is handed to the wrong person but is immediately retrieved before the person can read it. However, the exception does not apply if an EOB was mailed to the wrong person and the unintended recipient opened the envelope before realizing the mistake.

To determine whether there is only a low probability that the privacy or security of the PHI was compromised, the Privacy Official must perform a risk assessment that considers at least the following factors:

The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. For example, did the disclosure involve financial information, such as credit card numbers, Social Security numbers, or other information that increases the risk of identity theft or financial fraud? Did the disclosure involve clinical information such as a treatment plan, diagnosis, medication, medical history, or test results that could be used in a manner adverse to the individual? Did the use or disclosure otherwise further the unauthorized recipient's own interests?

The unauthorized person who used the PHI or to whom the disclosure was made. For example, does the unauthorized recipient of the PHI have obligations to protect the privacy and security of the PHI, such as another entity subject to the HIPAA privacy and security rules or an entity required to comply with the Privacy Act of 1974? Would those obligations lower the probability that the recipient would use or further disclose the PHI inappropriately? Also, was the PHI impermissibly used within a covered entity or business associate, or was it disclosed outside a covered entity or business associate?

Whether the PHI was actually acquired or viewed. If there was only an opportunity to view the information, but the Privacy Official determines that the information was not, in fact, viewed, there may be a lower (or no) probability of compromise. For example, if a laptop computer was lost or stolen and subsequently recovered, and the Privacy Official is able to determine (based on a forensic examination of

the computer) that none of the information was actually viewed, there may be no probability of compromise.

The extent to which the risk to the PHI has been mitigated. For example, if the Plan can obtain satisfactory assurances (in the form of a confidentiality agreement or similar documentation) from the unauthorized recipient that the information will not be further used or disclosed or will be destroyed, the probability that the privacy or security of the information has been compromised may be lowered. The identity of the recipient (e.g., another covered entity) may be relevant in determining what assurances are satisfactory.

If the Privacy Official determines that there is only a low probability that the privacy or security of the information was compromised, then the Plan will document the determination in writing, keep the documentation on file, and not provide notifications. On the other hand, if the Privacy Official is not able to determine that there is only a low probability that the privacy or security of the information was compromised, the Plan will provide notifications.

III. If a Reportable Breach Has Occurred: Notice Timing and Responsibilities

If the Privacy Official determines that a Reportable Breach has occurred, the Privacy Official will determine (in accordance with the Breach Regulations) the date the breach was discovered in order to determine the time periods for giving notice of the Reportable Breach. The Plan has reasonable systems and procedures in place to discover the existence of possible breaches, and workforce members are trained to notify the Privacy Official or other responsible person immediately so the Plan can act within the applicable time periods.

The Privacy Official is responsible for the content of notices and for the timely delivery of notices in accordance with the Breach Regulations. However, the Privacy Official may, on behalf of the Plan, engage a third party (including a Business Associate) to assist with preparation and delivery of any required notices.

The Breach Regulations may require a breach to be treated as discovered on a date that is earlier than the date the Plan had actual knowledge of the breach. The Privacy Official will determine the date of discovery as the earlier of (1) the date that a workforce member (other than a workforce member who committed the breach) knows of the events giving rise to the breach; and (2) the date that a workforce member or agent of the Plan, such as a Business Associate (other than the person who committed the breach) would have known of the events giving rise to the breach by exercising reasonable diligence.

Except as otherwise specified in the notice sections that follow, notices must be given "without unreasonable delay" and in no event later than 60 calendar days after the discovery date of the breach. It is important to recognize that 60 days is an outside limit; in most cases, notification should be given much sooner. Accordingly, the investigation of a possible breach, to determine whether it is a Reportable Breach and the individuals who are affected, must be undertaken in a timely manner that does not compromise the notice deadline.

There is an exception to the timing requirements if a law-enforcement official asks the Plan to delay giving notices.

IV. Business Associates

If a Business Associate commits or identifies a possible Reportable Breach relating to Plan participants, the Business Associate must give notice to the Plan's Privacy Official. The Plan is responsible for providing any required notices of a Reportable Breach to individuals, HHS, and (if necessary) the media. The Plan may delegate responsibility for the notice requirement to a Business Associate, but only through a business associate contract.

Unless otherwise required under the Breach Regulations, the discovery date for purposes of the Plan's notice obligations is the date that the Plan receives notice from the Business Associate.

In its Business Associate contracts, the Plan will require Business Associates to-

- Report incidents involving breaches or possible breaches to the Privacy Official in a timely manner;
- Provide to the Plan the information required to be included in notices (as described below); and
- Establish and maintain procedures and policies to comply with the Breach Regulations, including workforce training.

V. Notice to Individuals

Notice to the affected individual(s) is always required in the event of a Reportable Breach. Notice will be given without unreasonable delay and in no event later than 60 calendar days after the date of discovery (as determined above).

a. Content of Notice to Individuals

Notices to individuals will be written in plain language and contain all of the following, in accordance with the Breach Regulations:

- A brief description of the incident.
- If known, the date of the Reportable Breach and the Discovery Date.
- A **description** of the types of unsecured PHI involved in the Reportable Breach (for example, full name, Social Security numbers, 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 and credit monitoring services).
- A description of what the Plan is doing to investigate the Reportable Breach, such as filing a police report or reviewing security logs or tapes.
- A description of what the Plan is doing to mitigate harm to individuals.
- A description of what measures the Plan is taking to protect against further breaches (such as sanctions imposed on workforce members involved in the Reportable Breach, encryption, installation of new firewalls).
- Contact information for individuals to learn more about the Reportable Breach or ask other questions, which must include at least one of the following: Toll-free phone number, email address, website, or postal address.

b. Types of Notice to Individuals

The Plan will deliver individual notices using the following methods, depending on the circumstances of the breach and the Plan's contact information for affected individuals.

Actual Notice will be given in all cases, unless the Plan has insufficient or out-of-date addresses for the affected individuals. Actual written notice-

- Will be sent via first-class mail to last known address of the individual(s);
- May be sent via email instead, if the individual has agreed to receive electronic notices;
- Will be sent to the parent on behalf of a minor child; and
- Will be sent to the next-of-kin or personal representative of a deceased person, if the Plan knows the individual is deceased and has the address of the next-of-kin or personal representative.

Substitute Notice will be given if the Plan has insufficient or out-of-date addresses for the affected individuals.

If addresses of fewer than ten living affected individuals are insufficient or out-of-date, substitute notice may be given by telephone, an alternate written notice, or other means.

If addresses of ten or more living affected individuals are insufficient or out-of-date, substitute notice must be given via either website or media.

- *Substitute notice via website.* Conspicuous posting on home page of the website of the Plan or Company for 90 days, including a toll-free number that remains active for at least 90 days where individuals can learn whether the individual's unsecured information may have been included in the breach. Contents of the notice can be provided directly on the website or via hyperlink.
- *Substitute notice via media.* Conspicuous notice in major print or broadcast media in the geographic areas where the affected individuals likely reside, including a toll-free number that remains active for at least 90 days where individuals can learn whether the individual's unsecured information may have been included in the breach. It may be necessary to give the substitute notice in both local media outlet(s) and statewide media outlet(s) and in more than one state.

Substitute Notice is not required if the individual is deceased and the Plan has insufficient or out-of-date information that precludes written notice to the next-of-kin or personal representative of the individual.

Urgent Notice will be given, in addition to other required notice, in circumstances where imminent misuse of unsecured PHI may occur. Urgent notice must be given by telephone or other appropriate means.

c. Notice to HHS

Notice of all Reportable Breaches will be given to HHS. The time and manner of the notice depends on the number of individuals affected. The Privacy Official is responsible for both types of notice to HHS.

Immediate Notice to HHS. If the Reportable Breach involves 500 or more affected individuals, regardless of where the individuals reside, notice will be given to HHS without unreasonable delay, and in no event later than 60 calendar days after the date of discovery (as determined above). Notice will be given in the manner directed on the HHS website.

Annual Report to HHS. The Privacy Official will maintain a log of Reportable Breaches that involve fewer than 500 affected individuals and will report to HHS the Reportable Breaches that were discovered in the preceding calendar year. The reports are due within 60 days after the end of the calendar year. The reports will be submitted as directed on the HHS website.

d. Notice to Media (Press Release)

Notice to media (generally in the form of a press release) will be given if a Reportable Breach affects more than 500 residents of any one state or jurisdiction. The Plan is not required to incur any costs to publish a media notice-the publication decision rests with the media outlet.

Unlike notice to HHS, the residence of affected individuals is relevant for notice to the media.

If notice to media is required, notice will be given to prominent media outlets serving the state or jurisdiction.

If notice to media is required, it will be given without unreasonable delay, and in no event more than 60 calendar days after the date of discovery (as determined above). The content requirements for a notice to media are the same as the requirements for a notice to individuals. The Privacy Official is responsible for giving notice to media.