HIPAA COMPLIANCE POLICY

I. Policy Statement

Portland State University (“University”) is committed to protecting the security, confidentiality, integrity, and availability of its information resources, including protected health information. Protected health information is an asset and shall be managed to ensure its security, confidentiality, integrity, and availability for authorized purposes. All members of the University community share the responsibility for safeguarding protected health information to which they have access.

II. Reason for Policy/Purpose

In implementing its education, research, and community service missions, the University engages in certain activities that require the University to access, receive, maintain, transmit, or use protected health information (the “Business Associate Activities”) and which trigger compliance with the provisions applicable to business associates under the Health Insurance Portability and Accountability Act (“HIPAA”). This policy and the HIPAA Policies adopted hereunder are intended to support the mission of the University and to facilitate Business Associate Activities that are important to the University by:

- Ensuring compliance with legal requirements imposed by HIPAA and the University’s contractual obligations;
- Providing for the establishment of HIPAA Policies that set forth, among other things, the required technical, physical, and administrative safeguards to maintain the security, confidentiality, integrity, and availability of electronic protected health information; and
- Setting forth the roles and responsibilities necessary for the University to meet its obligations with respect to Business Associate Activities and protected health information.

III. Applicability

This policy applies to all employees, students, volunteers, visiting researchers, schools, colleges, and administrative units of the University, contracted nonpermanent individuals and vendors while doing business with the University, and other members of the University community that

1 – HIPAA Compliance Policy
have access to protected health information in connection with the University’s Business Associate Activities.

IV. Definitions

**Business Associate Activities:** Activities performed by the University for or on behalf of a covered entity or an organized health care arrangement through which the University creates, receives, maintains, or transmits protected health information for a function or activity regulated by HIPAA, including, without limitation, health care operations, data analysis, processing or administration, utilization review, quality assurance, benefit management, and practice management. Consulting and other services to or for a covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service or services involves the disclosure of protected health information from such covered entity or health care arrangement, or from another business associate of such covered entity or health care arrangement, to the University.

**HIPAA:** The Administrative Simplification Section of the Health Insurance Portability and Accountability Act of 1996, as codified at 42 U.S.C. § 1320d through d-9, and the requirements of any applicable regulations promulgated thereunder, and Title XIII of the American Recovery & Reinvestment Act of 2009 (the “HITECH Act”), as well as all pertinent current and future regulations issued by the Department of Health and Human Services thereunder.

**HIPAA Policies:** The policies, rules, and/or guidelines adopted by Research & Strategic Partnerships pursuant to this policy.


**Protected Health Information or PHI:** Any individually identifiable health information created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, which is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. Individually identifiable health information is health information, including demographic information collected from an individual, that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. Protected health information excludes education records covered by the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. 1232g), as amended, student treatment records described under FERPA at 20 U.S.C. 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer.
V. Policy

1. Roles and Responsibilities

1.1 Research & Strategic Partnerships (“RSP”) shall, in cooperation with relevant stakeholders, develop and adopt necessary and appropriate HIPAA Policies, which will include, among other things, the technical, physical, and administrative safeguards required to ensure the confidentiality, integrity, and availability of electronic PHI and protect electronic PHI against reasonably anticipated threats or hazards and unauthorized uses or disclosures. All relevant University stakeholders shall cooperate with RSP in the development and implementation of the HIPAA Policies. The HIPAA Policies are not required to be made through the process outlined in the Policy on Policies.

The Vice President for RSP shall designate a HIPAA Security Officer.

1.2 The HIPAA Security Officer shall have the responsibilities set forth in the HIPAA Policies. The HIPAA Security Officer may, in consultation with relevant stakeholders, add, revise, or modify the HIPAA Policies as necessary to incorporate changes to HIPAA or the HIPAA Security Rule or to improve compliance. In addition, the HIPAA Security Officer is responsible for reviewing and approving or disapproving proposed projects or activities that may require the University to access, receive, maintain, transmit, or use PHI. The HIPAA Security Officer, in consultation with the project sponsor and other relevant stakeholders, is responsible for determining whether a proposed project includes Business Associate Activities and, where necessary, implementing a business associate agreement and monitoring compliance with its terms. The HIPAA Security Officer shall, in cooperation with relevant stakeholders, develop procedures for implementing the review and approval of projects, which procedures shall be deemed a HIPAA Policy.

1.3 All members of the University community are responsible for understanding the HIPAA Policies and complying with their respective obligations thereunder.

2. Enforcement. Any employee found to have violated this policy or the HIPAA Policies may be subject to disciplinary action in accordance with applicable PSU policies and procedures and collective bargaining agreements, up to and including termination of employment. Any student found to have violated this policy or the HIPAA Policies may be subject to disciplinary action in accordance with applicable PSU policies and procedures, up to and including expulsion from the University. Student employees may be disciplined as an employee and as a student, resulting in both professional and educational consequences. Any vendor, contractor, or affiliate found to have violated this policy or the HIPAA Policies may be subject to disciplinary action, up to and including termination of contract or affiliation. Additional civil and/or criminal punishments may be applicable.
VI. Links To Related Forms

None.

VII. Links To Related Policies, Procedures or Information

None.

VIII. Contacts

If you have any questions regarding this policy, please contact Research & Strategic Partnerships at (503) 725-2213 or research@pdx.edu.

IX. History/Revision Dates

Adoption Date: June 12, 2015
Next Review Date: June 15, 2020

X. Policy Adoption/Reaffirmation/Revision Approvals

Approved: PORTLAND STATE UNIVERSITY PRESIDENT
Date: 6/16/15

Approved: PORTLAND STATE UNIVERSITY GENERAL COUNSEL
Date: 6/16/15