OLD DOMINION UNIVERSITY
University Policy

Policy #1004
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 ("HIPAA") COMPLIANCE POLICY

Responsible Oversight Executive: Vice President for Administration and Finance
Date of Current Revision or Creation: August 1, 2019

A. PURPOSE

The purpose of this policy is to establish the University's framework for compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and implementing regulations to the extent applicable to Old Dominion University.

B. AUTHORITY

Code of Virginia Section 23.1-1301, as amended, grants authority to the Board of Visitors to make rules and policies concerning the institution. Section 6.01(a)(6) of the Board of Visitors Bylaws grants authority to the President to implement the policies and procedures of the Board relating to University operations.

Health Information Technology for Economic and Clinical Health Act of 2013 (HITECH)

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Family Educational Rights and Privacy Act (FERPA)

Government Data Collection and Dissemination Practices Act, Code of Virginia Section 2.2-3800 et seq., as amended

Code of Virginia Section 23.1-2000 et seq., as amended

Code of Virginia Section 32.1-127.1:03, as amended

Bylaws of the Old Dominion University Board of Visitors, Article VI, §6.01 (c) (7)

C. DEFINITIONS

Access - The ability to read, enter, copy, query, download, or update individually identifiable health information.

Business Associate - A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

Contact Person - The position designated to receive complaints under this policy and provide further information about matters covered by the University's Notice of Privacy Practices.

Covered Function - Any function the performance of which makes the entity a health care provider.

Covered Units - A department/unit is designated as a covered unit if it performs HIPAA covered functions, or engages in activities that would make it a business associate of another ODU covered unit or a business associate of an entity outside of ODU. The ODU HIPAA Compliance Committee is responsible for designating and identifying the ODU departments/units that are covered units and thus subject to HIPAA, based on performance of covered functions, and these shall be maintained by the HIPAA Privacy Official.

HIPAA Compliance Committee - The HIPAA Compliance Committee assists the HIPAA Privacy Official in the adoption and implementation of policies and procedures for University HIPAA compliance.

HIPAA Privacy Official - An individual responsible for adoption and implementation of the general policies and procedures for the University's HIPPA Compliance Program and posting notices on the University's website (45 CFR § 164.530).

Hybrid Entity - A covered entity that performs both covered and non-covered functions as part of its business functions. Hybrid entities are required to create adequate "firewalls" between the part of the entity that performs covered functions and non-covered functions.

Human Subjects Review Committee (HSRC) - An entity that reviews all proposed research involving human subjects to ensure that the subjects' rights and welfare are adequately protected and approves HIPAA waivers for research purposes.

Individually Identifiable Health Information - Information that is a subset of health information, including demographic information collected from an individual, and:

- is created or received by a health-care provider, health plan, employer, or health care clearinghouse; and
- relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and
  - identifies the individual; or
  - there is a reasonable basis to believe the information can be used to identify the individual. (45 CFR § 164.501).

Notice of Privacy Practices ("NPP") - Statutory requirement that assures an individual has a right to adequate notice of the uses and disclosures of PHI that may be made by the hybrid entity, and of the individual's rights and the hybrid entity's duties with respect to PHI. (45 CFR § 164.520).

Protected Health Information ("PHI") - Individually identifiable health information, but not including individually identifiable health information in education records covered by FERPA. (45 CFR § 164.501).

D. SCOPE

This policy applies to all employees, students, volunteers, employees of affiliated organizations who are paid through the University, and visitors to the institution that have access to individually identifiable health information. Employees include all staff, administrators, faculty, full- or part-time, and classified or non-classified persons who are paid by the University. Students include all persons admitted to the University who have not completed a program of study for which they were enrolled; student status continues whether or not the University's programs are in session. Affiliated organizations are separate entities that exist for the benefit of the University through an operating agreement and include the Foundations, the Community Development Corporation, and the Alumni Association. Visitors include vendors and their employees, parents of students, volunteers, guests, uninvited guests and all other persons located on property owned, leased, or otherwise controlled by the University.

E. POLICY STATEMENT

It is the policy of the University that the security of health-care-related information and the privacy of individuals be protected to the maximum extent possible, in accordance with the Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act of 2013 (HITECH), other applicable statutes, and with the overall responsibility of the University to support the privacy rights and concerns of its members.

The University has elected to be a "Hybrid Entity," as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and performs both covered and non-covered functions as part of its operation. University departments or units may have to comply with HIPAA based on the interaction they have with the covered units.

Other units of the University may from time to time have access to Protected Health Information ("PHI") to perform business or professional services requiring access to PHI on behalf of the Provider and Health Plan components. These service units will not use or disclose the PHI created or received from or on behalf of the covered units in an impermissible manner and will appropriately safeguard the information. Those in service units who access PHI will complete HIPAA training prior to accessing the PHI and will have access only to the information they need to perform the service. Service units will provide information about their use or disclosure of PHI to the covered units and the University's Privacy and Security Officer as necessary for covered units to comply with HIPAA.

The University will establish appropriate safeguards to ensure that covered units do not inappropriately disclose PHI to another unit of the University and that covered units' workforce members use and disclose PHI received from the covered units only as permitted or required by State and Federal law.

The University will cooperate with the Secretary of the U.S. Department of Health and Human Services ("Secretary") as required for complaint investigations and compliance reviews. The University will respond to questions and complaints regarding privacy and security of PHI at the University and will resolve the complaints as appropriate.

The University will not sanction and will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against persons who file complaints with the Secretary, persons who testify, assist or participate in an investigation, compliance review, proceeding or hearing, or a person opposing any act or practice that is unlawful provided that the person had a good faith belief that the practice complained about is unlawful and the manner of opposition is reasonable and does not involve an unlawful disclosure of PHI. Any individual who feels that he or she has been retaliated against as a result of such participation should refer to University Policy 3020, Whistleblower Retaliation Policy, for additional guidance.

The HIPAA Program is administered by the HIPAA Privacy Official. The HIPAA Privacy Official, designated by the Vice President for Administration and Finance, is responsible for adoption and implementation of the general policies and procedures for University HIPAA compliance and posting same on the University's website. The HIPAA Privacy Official may also designate additional departments within the University as covered units and subject to the requirements of this policy.

The HIPAA Privacy Official is assisted by a HIPAA Compliance Committee consisting of individuals who are primary stakeholders with regard to the use and protection of PHI. The HIPAA Compliance Committee will assist the HIPAA Privacy Official in the adoption and implementation of policies and procedures for University HIPAA compliance. Members of the HIPAA Compliance Committee will include the HIPAA Privacy Official and representatives from Information Technology Services, Information Security, designated covered units and the Office of University Counsel. Other members may be added at the discretion of the HIPAA Privacy Official.

The Associate University Counsel will serve as the Contact Person for purposes of this policy and is designated to receive complaints under this policy and provide further information about matters covered by the University's Notice of Privacy Practices.

F. PROCEDURES

1. Covered Units are responsible for:

    a. complying with this HIPAA policy and for developing operating procedures and forms as needed to implement and comply with such policies as are applicable, including appropriate administrative, technical and physical safeguards to protect the privacy of protected health information;

    b. providing the HIPAA Privacy Official with current copies of their procedures and any forms or other HIPAA-related documents. The HIPAA Privacy Official may require a covered unit to change its procedures, forms or related documents; and

    c. completing a Business Associate Agreement (BAA) with business associates that will use PHI for administrative, research, pricing, billing and/or quality-assurance purposes. A copy of the signed BAA will be provided to the Privacy Official.

2. Information Technology Services will provide technical support to covered units in order to meet the technical safeguards required to maintain HIPAA compliance.

3. All employees are required to report any potential breach of PHI immediately to the Privacy Official. Some examples of breaches include:

    a. Loss or theft of a laptop, external hard drive, thumb drive, or paper chart containing PHI

    b. Access to PHI outside of an individual's job responsibilities

    c. Improper disposal of PHI such as failure to shred paper documents or securely delete electronic records prior to device disposal or repurposing

    d. Misdirected mailings, emails, or faxes

    e. Malware infection on electronic protected health information containing devices

    The Privacy Official will follow the process detailed in Information Technology Standard 05.2.0, Data Breach Notification Standard, and will consult, as appropriate, with University officials on possible remedies.

4. Research

    PHI may be utilized in research only after obtaining approval through a human subjects review by the Human Subjects Review Committee (HRSC). The HSRC will inform the HIPAA Privacy Official upon approval of a waiver.

5. Training

    All covered units as well as departments whose employees have direct or indirect access to PHI will train employees (faculty, staff, students and volunteers) on policies and procedures with respect to PHI as required by HIPAA. Such training will be as necessary and appropriate for the members of the staff to carry out their functions. The HIPAA Privacy Official is responsible for providing training guidance and assistance.

    Training shall be provided to all members and each new member shall be trained within a reasonable time after joining the workforce. Additional training will be provided to each member of a covered unit's workforce whose functions are materially affected by any changes in HIPAA-related policies or procedures. Such training will be provided within a reasonable time after the material change becomes effective.

    All covered units will maintain copies of the training materials and document that the required training has been provided. All training documents, including attendance rosters, will be forwarded to the HIPAA Privacy Official. The documentation will be retained in accordance with the General Schedules published by the Library of Virginia (LVA.)

6. Complaints

    Complaints concerning HIPAA policies and procedures and/or compliance with those policies and procedures will be made in writing to the Contact Person. The Contact Person will investigate all complaints in a timely manner and provide a written determination to the parties involved (e.g., the complainant and the subject covered units) and to the HIPAA Privacy Official. The HIPAA Privacy Official will, after conferring with the Office of Human Resources, Provost and Vice President for Academic Affairs and Director, Student Conduct

and Academic Integrity, recommend sanctions, as appropriate, and propose amendments to policies and procedures, as needed.

7. Waiver of Rights

   Individuals will not be required to waive any of their rights, or the right to file a complaint under the HIPAA privacy regulations as a condition of treatment, payment, enrollment in a health plan, or eligibility for benefits.

8. Mitigation

   The University will mitigate, to the extent practicable, any known harmful effect of the use or disclosure, by the University or its business associates, of PHI in violation of its policies and procedures or the HIPAA privacy regulations.

9. Sanctions

   Violation of this policy by University employees, students and employees of affiliated organizations may result in appropriate disciplinary action.

G. RECORDS RETENTION

Applicable records must be retained and then destroyed in accordance with the Commonwealth's Records Retention Schedules. Specifically, GS-111/200238 for Institutional Review Board (IRB): Human Subjects Records (retained for six years following project completion) and GS-120/200349 for Health Insurance Portability and Accountability Act Records (retained for six years after the close of the calendar year).

H. RESPONSIBLE OFFICER

HIPAA Privacy Official

I. RELATED INFORMATION

U.S Department of Health & Human Services, Joint Guidance on the Application of the *Family Educational Rights and Privacy Act* (*FERPA*) And the *Health Insurance Portability and Accountability Act of 1996* (*HIPAA*) to Student Health Records
Board of Visitors Policy 1450 - Faculty Sanctions
Board of Visitors Policy 1530 - Code of Student Conduct
University Policy 3505 - Information Technology Security Policy
University Policy 3700 - Records Management Policy
University Policy 4100 - Student Record Policy
University Policy 6600 - Standards of Conduct for Classified Employees

POLICY HISTORY

****

Policy Formulation Committee (PFC) & Responsible Officer Approval to Proceed:

/s/ Doug Streit — July 25, 2019
Responsible Officer — Date

Policy Review Committee (PRC) Approval to Proceed:

/s/ Donna W. Meeks — May 28, 2019
Chair, Policy Review Committee (PRC) — Date

Executive Policy Review Committee (EPRC) Approval to Proceed:

/s/ Gregory DuBois — July 25, 2019
Responsible Oversight Executive — Date

University Counsel Approval to Proceed:

/s/ R. Earl Nance — July 31, 2019
University Counsel — Date

Presidential Approval:

/s/ John R. Broderick — August 1, 2019
President — Date

Policy Revision Dates: March 24, 2014; August 1, 2019

Scheduled Review Date: July 31, 2024