UNIVERSITY OF RICHMOND

Policy Manual

Policy #:	HRM-1005	**Policy Title:**	HIPAA Privacy Policy and Procedures
Effective:	05/16/2022	**Responsible Office:**	Human Resources
Date Approved:	05/16/2022	**Approval:**	Vice President and General Counsel
Replaces Policy Dated:	N/A	**Responsible University Official:**	Director, Compensation and Benefits

PURPOSE:

The purpose of this policy is to ensure that the University of Richmond complies with the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations. The University will change this policy as necessary and appropriate to comply with changes to HIPAA or its implementing regulations.

This policy is intended to provide guidance to all Covered Employees (as defined below) regarding the management and protection of Protected Health Information (PHI) subject to HIPAA.

SCOPE:

This document and the policies herein apply to the sponsorship and administration of the University's Health Plan (as defined below) and to all Covered Employees (as defined below) with access or potential access to PHI generated or maintained in connection with the University's Health Plan.

This policy applies to the health care components of the University which are: (a) the University's Health Plan; and (b) the Benefits & Compensation Section of the University's Human Resources Department; and (c) all Covered Employees that supervise, assist, or advise the Benefits & Compensation Section of the University's Human Resources Department, but solely to the extent they perform functions covered by HIPAA and its implementing regulations.

This policy is not intended to apply to PHI or other medical or health records maintained by any office, section, or division of the University that is engaged in functions not covered by HIPAA, including, but not limited to the University's Student Health Center, Counseling and Psychological Services (CAPS), or its Athletic Deparment. The records of these offices shall be maintained confidentially to the extent required by Virginia law and applicable Virginia regulations.

INDEX:

HRM-1005.1 – Definitions

A. Breach. The acquisition, access, use, or disclosure of PHI which compromises the security or privacy of the PHI unless the University or a business associate demonstrates that there is a low probability that the PHI has been compromised.

A breach does not include:

1. Any unintentional acquisition, access, or use of protected health information by an employee or person acting under the authority of the Univeristy or a business associate, if it was made in good faith and within the scope of authority and does not result in further non permitted use or disclosure.

2. Any inadvertent disclosure by an individual authorized to access PHI to another individual authorized to acces PHI at the University if that information is not further used or disclosed in an impermissible manner.

3. A disclosure of PHI where the Univeristy or a business associate has a good faith belief that an unauthorized individual to whom the disclosure was made would not reasonably have been able to retain such information.

B. Business Associate. Any entity that:

1. Performs or assists in performing a University function or activity involving the use and disclosure of PHI (including claims processing or administration, data analysis, underwriting, etc.); or

2. Provides legal, accounting, actuarial, consulting, data aggregation, management, accredidation, or financial services, where the performance of such services involves giving the service provider access to PHI.

C. Covered Employees. All employees that have access to or are exposed to PHI.

D. Covered Entity. A health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form relating to any covered transaction.

E. Disclosure. The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

F. Employees. All full-time, part-time, or temporary employees, interns, independent contractors, trainees, and other persons engaged in the performance of work for the University, its offices, programs or facilities.

G. Health Plan. The group medical plans, dental plan, health flexible spending account plan, and employee assistance plan sponsored by the University.

H. Inappropriate Disclosure. The intentional or unintentional release, transfer, provision of,access to, or divulging of PHI in a manner inconsistent with HIPAA, its implementing regulations, or this policy.

I. Notice of Privacy Practices. A written statement that describes the University's use and disclosure of PHI and that is distributed to all individuals whose information will be collected by or on behalf of the University's Health Plan.

J. Personal Representative. A person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person who is authorized under law to make health care decisions on behalf of an un-emancipated minor.

K. Privacy Rules. The regulations adopted by the Commonwealth of Virginia and federal agencies to implement the requirements of HIPAA and those obligations that arise under the privacy and security standards adopted by the Health Insurance Marketplaces, pursuant to 45 C.F.R. §155.260.

L. Protected Health Information (PHI). Individually identifiable information, including genetic information, that (i) relates to either 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 health care provided to an individual; and (ii) is transmitted by or maintained in electronic media or any other form or medium. PHI does not include individually identified health information: (i) in education records covered by the Family Educational Rights and Privacy Act (FERPA); (ii) relating to a University student which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in their professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice; (iii) contained in employment records maintained by the University in its role as an employer; or (iv) regarding a person who has been deceased for more than 50 years.

M. Treatment, Payment and Health Care Operations (TPO).

1. Treatment means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.

2. Payment means activities undertaken to obtain premiums, obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collections activities, medical necessity determinations and utilization review.

3. Health Care Operations includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, evaluating practitioner and provider performance or health plan performance, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities including customer service, and the creation of de-identified health information as defined by the Health Insurance Portability and Accountability Act (HIPAA).

N. Use. For purposes of this policy, the term "use" means the sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by the University's Health Plan or the University in its capacity as plan sponsor and/or administrator.

POLICY STATEMENT:

HRM-1005.2 – Policy Statement

The University's Health Plan will treat as confidential the PHI received or maintained by the University's Health Plan in a manner compliant with HIPAA, its implementing regulations, and the applicable laws and regulations of the Commonwealth of Virginia.

HRM-1005.3 – Confidentiality and Security of PHI

A. Confidentiality of PHI

1. PHI shall not be obtained, used, or disclosed except as permitted or required by law.
2. PHI may be used or disclosed as follows:
   a. To the individual.
   b. To carry out TPO activities as allowed under HIPAA and/or pursuant to and in compliance with a current and valid authorization, receipt, use and disclosure of PHI.
   c. In keeping with a Business Associate Agreement.
   d. As otherwise allowed or required under the HIPAA Rules or other federal and/or state laws concerning privacy of information that is used by the University in the course of its business operations.
3. Minimum Necessary: When obtaining, using, or disclosing PHI or when requesting PHI from another entity, reasonable efforts will be made to limit the PHI used or disclosed to the minimum necessary to accomplish the intended purpose.
4. Disclosures to Other Components of the University. Covered Employees shall not disclose PHI to and shall protect PHI from other departments, divisions, or sections of the University, or from the employees of such other departments, divisions, or sections, unless such disclosure of or access to PHI by a third party would be permissible under HIPAA, its implementing regulations, or this policy.
5. Accounting for Disclosures: An individual has a right to an accounting of disclosures of their PHI for up to a six-year period.

B. Security of PHI

1. Electronic Security. The University's Health Plan and the health care components of the University shall:

   a. Maintain reasonable and appropriate security measures to ensure the confidentiality and integrity of electronic PHI, protect against reasonable anticipated threats or hazards to the security or integrity of PHI, and protect against reasonably anticipated inappropriate disclosure or use of PHI;

   b. Periodically review and modify security measures as needed to maintain the reasonable and appropriate protection of electronic PHI;

   c. Document the security measures maintained pursuant to this Section 1111.3 (B)(1) and all modifications and updates to such security measures;

   d. Periodically conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI;

   e. Regularly review records of information system activity relating to servers or electronic transmission and storage platforms for PHI, such as audit logs, access reports, and security incident tracing reports;

   f. Maintain reasonable and appropriate procedures for managing and ensuring access to electronic PHI by Covered Employees and preventing access to electronic PHI by University Employees who are part of the health care component of the University or Covered Employees whose employment has terminated.

2. Techincal Safeguards. The University's Health Plan and the health care components of the University shall:

   a. Maintain access control procedures for information systems containing electronic PHI that limit access to those Covered Employees who have been granted access by the health care components of the University, including, but not limited to assigning unique login name or number to track user identify and establishing procedures for accessing electronic PHI in an emergency;

3. Physical Security. The University's Health Plan and the health care components of the University shall:

   a. Maintain reasonable and appropriate physical security measures to limit physical access to electronic information systems containing PHI and the facilities in which they are housed to Covered Employees and Business Associates authorized to access such systems and/or facilities;

   b. Maintain procedures for the appropriate use, surroundings, and security of workstations that have access to electronic PHI;

   c. Prohibit Employees from copying or storing electronic PHI to any personal or University-owned electronic device (e.g., laptop, smartphone, tablet) or to any personal or University-owned portable data storage device (e.g., thumbdrive, CD Rom, external hard drive);

d. Maintain reasonable and appropriate procedures for removing electronic PHI from servers, hardware, electronic devices or other electronic media for such items are made available to use for functions not covered by HIPAA.

e. Ensure thall all physical copies of PHI are stored in secure locations to which access is limited.

4. Disposal or Destruction of PHI. The University's Health Plan and the health care components of the University shall:

a. Maintain procedures that ensure the secure and confidential destruction or final disposition of electronic PHI (once the retention period for such PHI has expired) and/or any server, other hardware, or electronic media on which electronic PHI is stored.

b. Ensure that, once the retention period has expired, physical copies of PHI are shredded using secure process by an external vendor with which the University has an appropriate Business Associate Agreement.

HRM-1005.4 – Administrative Requirements for HIPAA Implementation

A. Personnel Designations.

1. Privacy Officer: The person responsible for the development and implementation of University-wide policies and procedures relating to the safeguarding of PHI subject to HIPAA. The Privacy Officer will be trained on all policies and procedures necessary to fulfill these responsibilities in ensuring the security and privacy of PHI.

2. Persons with acess to PHI: Those individuals who will be listed by the title and documented in the University Risk Assessment

a. The Privacy Officer will update the list on a periodic basis

b. The previous listing will be maintained for a period of not less than six (6) years

B. Training Requirements.

1. All Covered Employees shall receive training on policies and procedures relating to PHI as necessary and appropriate for such persons to carry out their functions within the University.

2. Each new Covered Employee shall receive the training as described above within thirty (30) days after joining the University.

3. Each Covered Employee whose functions are impacted by a material change in the policies and procedures relating to PHI, or by a change in position or job description, shall receive the training as described above within a reasonable time after the change becomes effective.

4. The Privacy Officer shall receive training within thirty (30) days of employment with the University or appointment to the position.

5. Privacy training shall be appropriate to the tasks that each employee performs.

HRM-1005.5- Maintaining Appropriate Documentation Regarding Compliance with HIPAA

A. The University will maintain documentation, in written or electronic form, of policies, procedures, communications, and other administrative documents as required by 45 CFR § 164.530(i) and (j) for a period of at least six (6) years from the date of creation or the date when last in effect, whichever is later. This policy will be kept in the University Security Documentation Library. The Library is located in Box for internal access. Outdated and superseded materials from the Security Documentation Library will be kept in an archive (the Security Documentation Archive) for at least six (6) years after the date when they are first outdated or superseded.

B. The University will incorporate, document, and implement into its policies, procedures and other administrative documents any changes in law.

C. The following documentation will be maintained in an organized manner;

1. Policies and procedures related to the use or diclsoure of PHI;
2. Requests for the use or disclosure of PHI;
3. Agreements with Business Associates referring to the use or disclosure of PHI; and
4. Notice of Privacy Practices and any changes made thereto.

D. Documentation will be maintained in a manner that allows necessary availability, while also ensuring the security of information.

HRM-1005.6 - Minimum Necessary Provision

A. The University will make reasonable efforts to ensure that the minimum necessary amounts of PHI are disclosed, used, or requested to accomplish the intended purpose. Exceptions to the Minimum Necessary Requirement include disclosures:

1. To the individual who is the subject of the information;
2. Made pursuant to an authorization provided by the individual;
3. To the healthcare providers for treatment purposes;
4. Required for compliance with the standardized HIPAA transactions;
5. Made to the Secretary of HHS or their agent pursuant to a privacy investigation;
6. Otherwise required by the Privacy Rules or other law.

HRM-1005.7 – Notice of Privacy Practices

A. The University will provide a formal notice to individuals regarding the use or disclosure of PHI pursuant to 45 CFR §164.520. This will be provided in a separate document entitled Notice of Privacy Practices (NPP).

B. The NPP will be provided electronically to all benefit-eligible employees of the University:

1. In their new hire packets;
2. In their open enrollment guides;
3. On or after the effective date of a revision;

4. Upon request;
5. At least once every three (3) years, the University will inform all covered employees of the availability of the Notice and how to obtain it;
6. On the Univeristy Human Resources webpage.

C. The University reserves the right to change the terms of its NPP and to make new NPP provisions effective for all PHI that it maintains.
   1. In implementing a change in the NPP, the University will:
      a. Ensure that the policy or procedure, as revised to reflect a change in the University's privacy practice, complies with the standards, requirements, and implementation specifications of the Privacy regulations;
      b. Document the policy or procedure as revised;
      c. Revise the NPP to state the changes in practice and make the revised NPP available; and
      d. Not implement a change in policy or procedure prior to the effective date of the revised NPP.
   2. The University will provide each covered employee with any revisions of its NPP.

D. When providing the NPP to an individual by email, the University will:
   1. Provide a paper copy of the NPP to the individual upon request.

E. The University may change policies or procedures that do not affect the content of the NPP, provided that the policy or procedure complies with the privacy regulations and is documented as required in this policy.

HRM-1005.8 – Business Associates

A. The University may allow Business Associates to create or receive PHI on University's behalf. The University will document these assurances through a written agreement, and review of the Business Associates' HIPAA Compliance Plan.

B. The agreement between University and University Business Associates must meet the following requirements, as applicable:
   1. Establish permitted and required uses or disclosures of PHI that are consistent with those authorized for University, and provide reasonable assurance to University that the confidentiality of the PHI will be maintained.
   2. Provide that the Business Associate will:
      a. Not use or disclose the PHI except as authorized under the Agreement or required by law.
      b. Use safeguards to prevent unauthorized use or disclosure.
      c. Report unauthorized uses or disclosures to University.
      d. Pass on the same obligations relating to protection of PHI to any Business Associate Subcontractors they contract with.

e. Make information available for the provision of an accounting of uses and dislcosures in accordance with relevant law and policy.

f. Make its internal practices, books and records relating to its receipt or creation of PHI available to the Seretary of HHS for purposes of determining Business Associate's compliance with Privacy Rules.

g. Authorize termination of the Agreement by University upon a material breach by Business Associate, or for other reasons.

3. Compliance Responsibilities: Business Associates must agree to report any use or disclosure of PHI not permitted by the Business Associate agreement and any successful security incident to University within a commercially reasonable period, but in no event later than within fifteen (15) business days, after it is discovered or should have reasonably been discovered.

4. Enforcement and Sanctioning of Business Associates: Any Business Associate found to have violated the Business Associate Agreement shall be subject to penalties, up to and including termination of the Agreement. In the case where inappropriate access or use of Protected Health information was or may have been involved, the Business Associate may additionally be reported ot the appropriate law enforcement agencies.

HRM-1005.9 – Enforcement and Sanctioning of Employees

A. Knowledge of a violation or potential violation of any of this Policy must be reported directly to the Privacy Officer. An employee found to have violated this reporting obligation shall be subject to disciplinary action.

B. Sanctions

The University will apply appropriate sanctions against its employees who fail to comply with University policies and procedures.

1. The type of sanction applied shall vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of health information, and similar factors.

2. Violations of a severe nature may result in notification to law enforcement officials as well as regulatory, accredidation, and/or licensure organizations.

3. All sanctions will be documented and retained for a period of at least six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

4. The University, to the extent practicable, shall mitigate any harmful effects of unauthorized uses or disclsoures of PHI by the University or any of its Business Associates.

HRM-1005.10 – Breach Incident by the Univeristy or Business Associate

A. Breach Incident by the Univeristy:

1. A breach shall be treated as discovered by University on the first day when such breach is known to the University or, by exercising reasonable diligence, would have been known to University. The University shall be deemed to have knowledge of a breach if the breach is knowns, or if by

exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of University.

2. If it is determined that a breach has occurred, the University will provide notification to applicable individuals and entities in accordance with University policy.

3. Employees shall immediately notify the University's Privacy Officer of any unauthorized access, use, or disclosure of PHI. The Privacy Officer will protect the identity and source of the information provided to the extent possible.

B. Breach Incident by a Business Associate:

1. A Breach shall be treated as discovered by the Business Associate on the first day when such Breach is known to Business Associate or, through the exercise of reasonable diligence, would have been known to the Business Associate. A business associate shall be deemed to have knowledge of the breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate. The Business Associate will mitigate, to the extent practicable, any harmful effect that is knowns to the Business Associate of a use or disclosure of PHI by the Business Associate in violation of the requirements of the Agreement between the Business Associate and the Covered Entity.

2. If it is determined that a Breach of Unsecured PHI has occurred, the Business Associate will provide notification to the Univeristy and other applicable individuals and entities in accordance with the University's Data Exposure Policy.

HRM-1005.11 – Employee Rights

A. Requesting a copy of Health Record

1. To the extent the University maintains individual PHI in a designated record set, an employee has a right to request a a copy of that PHI in electronic form within thirty (30) days of the request and to transmit the copy directly to another person designated by the individual, provided that such choice is clear, conspicuous, and specific.

B. Alternate Means of Receiving Confidential Communications for PHI

1. The University will accommodate reasonable requests by individuals to receive communications of PHI, to the extent the University maintains PHI, by alternative means or in alternative locations.

C. Individual Revocation of an Authorization to Disclose PHI

1. An employee may revoke a prior authorization provided to the University to disclose PHI.

D Complaints and Prohibition Against Retaliation

1. University employees have a right to submit a complaint regarding any aspect of the University practices regarding PHI to the Univeristy Privacy Officer and/or with HHS. Additionally, employees have a right to:

a. Testify, assist, or participate in an investigation, compliance review, proceeding, or hearing under Part C of Title XI;

b. Oppose any act made unlawful by the HIPAA Privacy Rule, provided the individual or person has a good faith belief the act opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA Privacy Rule;

c. Disclose PHI as a whistleblower when the disclosure is to a health oversight agency, public health authority, or an attorney retained by the individual for purposes of determining the individual's legal options with regard to the whistleblower activity.

2. Pursuant to the Univeristy's Policy Prohibiting Retaliation, neither the University nor any employee shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of their rights or participation in any process relating to HIPAA compliance, or against any person for filing a complaint with the Secretary of the U.S. Department of Health and Human Services, participating in an investigation, compliance review, proceeding or hearing, or engaging in reasonable opposition to any act that the person in good faith believes to be unlawful under the Privacy Rules as long as the action does not involve disclosure of PHI in violation of the regulations.

POLICY BACKGROUND:

Reviewed by President's Cabinet and approved by Vice President & General on May 16, 2022

Non-substantive changes made to revise gender-binary language on January 11, 2023

POLICY CONTACTS:

Vice President and General Counsel

Director of Compliance

Director of Compensation and Benefits