POLICIES ON PROTECTED HEALTH INFORMATION

1. **General** – It is the policy of the University of Delaware (the "University") to comply with the Health Insurance Portability and Accountability Act of 1996, as amended and its regulations (collectively, "HIPAA"), including the Standards of Privacy of Individually Identifiable Health Information (the "Privacy Standards") to the extent that HIPAA is applicable to the University. This policy provides general operating guidelines for HIPAA compliance.[1] For further specific information, please see the HIPAA statute and regulations, or contact one of the University's Privacy Officers (see Section 3 below).

1.1 **Status as a Hybrid Entity** – The University's activities include both functions that are covered by HIPAA ("Covered Functions") and functions that are not covered by HIPAA ("Non-Covered Functions"). Accordingly, the University has determined it is a hybrid entity for HIPAA purposes. Pursuant to HIPAA, the University has designed which of its components are covered by HIPAA ("Covered Components") and must comply with all policies contained herein.

1.2 **Health Care Provider Covered Components** – The following departments of the University are health care providers that have direct treatment relationships with individuals:

(a) Student Health Services;
(b) Sports Medicine Clinic;
(c) Physical Therapy Clinic;
(d) Nurse Managed Health Center (NMHC)

1.3 **Other Covered Components** – Certain departments of the University may have access to protected health information ("PHI") (as further defined in Section 4.1 below) due their services and activities in support of the University's health care provider Covered Components. The following departments of the University are presently included in the University's Covered Components only to the extent that they perform Covered Functions or activities that would make such component a business associate of a component that performs Covered Functions if the two components were separate legal entities:

(a) Department of Occupational Health and Safety;
(b) Office of Real Estate and Risk Management;
(c) Office of Billing and Collection;
(d) Information Technologies;
(e) University Executive Officers;
(f) Internal Audit Department;
(g) University Archives;
(h) University Procrument Services

1.4 **Modifications to Hybrid Entity Designation** – The University's designation of which departments are included as part of the University's Covered Components may be changed or modified at any time. All changes and modifications must be in writing and signed on behalf of the University.

2. **Policies and Procedures**

2.1 **General** – This HIPAA policy applies to all Covered Components and shall be distributed to all Covered Components.

2.2 **Specific Operating Policies** – Each Covered Component is responsible for complying with this HIPAA policy, as applicable, and for developing policies and procedures as needed to implement and comply with this policy.

3. **Privacy Officers**

3.1 **Designation of Privacy Officers** – The University has designated two (3) individuals as Privacy Officers for HIPAA compliance purposes. The Privacy Officer for matters concerning Student Health Services and the Sports Medicine Clinic is Timothy Dowling who can be contacted by calling 302-831-3699 or by writing: Timothy Dowling, University of Delaware, Student Health Services, Laurel Hall, Newark, DE 19716-8101. The Privacy Officer for matters concerning the Physical Therapy Clinic is Gina Hanley

[1] In addition to HIPAA, other laws regarding the privacy of information may apply to the University, including but not limited to state law and the Family Educational Rights and Privacy Act ("FERPA").

Pusey, who can be contacted by calling 302-831-8893 or by writing: Gina Hanley Pusey, Manager of Clinical Services University of Delaware – Physical Therapy Department, 053 McKinly Lab, Newark DE, 19716. The Privacy Officer for the NMHC is Allen Prettyman, Ph.D, and Assistant Professor University of Delaware – School of Nursing who may be contacted by calling 302 831 3195 or by writing: Allen Prettyman,NMHC 26 North College Avenue, McDowell Hall, Rm119, Newark DE, 19716. The designation of the Privacy Officers is subject to change.

3.2 **Responsibilities of Privacy Officers** – The University's Privacy Officers are responsible for the development and implementation of HIPAA policies and procedures. The Privacy Officers are also designated to receive complaints concerning the University's HIPAA related policies and procedures and to provide further information to individuals about matters covered by the University's Notices of Privacy Practices (described in Section 5 below). In addition, the Privacy Officers will take primary responsibility for responding to requests and demands from and investigations by the Office of Civil Rights (OCR) and the Department of Health and Human Services (HHS).

4. Uses and Disclosures of PHI

4.1 **Definition of PHI** – PHI is all health information that identifies an individual and PHI can be in any form – oral, written, or electronic. PHI does not include education records covered by the Family Educational Right and Privacy Act ("FERPA"); those student records described in FERPA that are maintained by a physician, psychiatrist, or other professional and which are made, maintained, or used in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment; and employment records held by a Covered Component in its role as employer.

4.2 **Disclosures to Non-Covered Components** – For the purposes of this policy, any disclosure to University departments which are not Covered Components ("Non-Covered Components") at the time of the disclosure are to be treated in the same manner as disclosures to separate and distinct outside entities. Any individual that performs duties for both a Covered Component and a Non-Covered Component must not use or disclose PHI created or received in the course of or incident to such individual's work for the Covered Component in a manner that violates this policy or the Privacy Standards.

4.3 **Verification of Disclosures** – Prior to any disclosure of PHI permitted by this policy or the Privacy Standards, the Covered Component must:

(a) Except for disclosures pursuant to Section 4.5(e) below, verify the identity of the person requesting PHI and the authority of any such person to have access to PHI under the Privacy Standards if the identity or authority of such person is not known to the Covered Component; and

(b) Obtain any documentation, statements, or representations from the person requesting the PHI when such documentation, statement, or representation is required for the disclosure under this policy or the Privacy Standards.

4.4 **Uses and Disclosures of PHI Pursuant to a Valid Authorization** – PHI may be used and disclosed pursuant to a valid HIPAA written authorization which has been signed by the individual or his or her personal representative. An authorization must contain each of the elements required by HIPAA and any state law requirements that may apply to the use or disclosure. Each of the University's health care providers listed in Section 1.2 above have developed a form authorization for uses and disclosures under the Privacy Standards. Copies of the form authorizations may be obtained by contacting the appropriate Privacy Officer. All signed authorizations must be maintained in accordance with Section 10 (Documentation) below. Individuals have the right to revoke their authorizations at any time, except to the extent that the University's Covered Components or others have relied on the individual's prior authorization.

4.5 **Uses and Disclosures of PHI Without an Authorization** – PHI may be used and disclosed without an authorization in the following instances:

(a) **To the Individual** – Protected health care information may be disclosed to the individual who is the subject of the information without an authorization.

(b) **Treatment, Payment, and Health Care Operations**

(i) Covered Components may use or disclose PHI for the treatment, payment, or health care operations of the University's Covered Components.

(ii) Covered Components may disclose PHI for treatment activities of a health care provider.

(iii) Covered Components may disclose PHI to another health care provider or entity covered by the Privacy Standards for the payment activities of the entity that receives the information.

(iv) Covered Components may disclose PHI to another entity covered by the Privacy Standards for the health care operations of that entity if the University's Covered Components and that entity either has or had a relationship with the individual who is the subject of the PHI, provided that the PHI pertains to such relationship and the

disclosure is for certain permitted health care operations or for the purpose of health care fraud and abuse detection or compliance.

(c) **Business Associates** – A Covered Component may disclose PHI to its business associates who provide services on its behalf (i.e., lawyers, accountants, consultants, etc.) so long as the business associate has a business associate agreement with the Covered Component that has been approved by a University Privacy Officer. Business associate agreements must be signed and in writing, and must meet all of the requirements set forth in the Privacy Standards. Those with questions regarding who has a current business associate agreement with the Covered Component may contact a University Privacy Officer.

(d) **Incident to Uses or Disclosures** - PHI may be used or disclosed incident to a use or disclosure permitted by the Privacy Standards.

(e) **Permission or Opportunity to Object** - A Covered Component may use and disclose PHI in certain circumstances if the individual has been informed in advance of the use or disclosure and has been given the opportunity to object to the use or disclosure. These circumstances include:

(i) Providing certain directory information to the clergy and other persons who ask for the individual by name;

(ii) Providing relevant information to people involved with the patient's care or payment related to the patient's care;

(iii) Providing information regarding the patient's location, condition, or death to notify a person responsible for the care of the patient; and

(iv) Providing information to appropriate entities for disaster relief efforts.

Notice and permission may be obtained from individuals orally for these purposes. Notice and the opportunity to object is not required in emergency circumstances or when the individual is not present. In such instances, the Covered Component must make a determination whether the use or disclosure of PHI is in the patient's best interest, based on professional judgment and common practice. However, the use or disclosure must not be inconsistent with any known prior expressed preference of the individual. The Covered Component shall provide the individual the opportunity to object in such circumstances when it becomes practicable. The same process should be used in determining whether to allow another person to act on behalf of the individual to pick up prescriptions, medical supplies, X-rays, and other PHI.

(f) **Disclosures Required by Law and Other Similar Purposes** - A Covered Component may disclose PHI without an authorization and without providing an opportunity for the individual to agree or object if the use or disclosure is for one of the following purposes. All uses or disclosures for these purposes must conform to all requirements imposed by HIPAA and/or state law, as applicable. Covered Components who believe a desired use or disclosure may fit into one of these categories must consult with a Privacy Officer prior to making the disclosure.

(i) For public health activities or legal authorities charged with preventing or controlling disease, injury, or disability;

(ii) To report abuse, neglect, or domestic violence;

(iii) To health oversight agencies;

(iv) For judicial and administrative proceedings (in response to a subpoena or court order);

(v) For law enforcement purposes, for example to identify a suspect, to provide information about the victim of a crime, or to report criminal conduct;

(vi) To provide information regarding decedents, for example, to coroners, medical examiners, and funeral homes;

(vii) For cadaveric organ, eye, or tissue donation;

(viii) To avert a serious threat to health or safety;

(ix) For specialized government functions, for example, national security and intelligence activities, or to the military

(x) To comply with worker's compensation laws; or

(xi) As required or permitted by law.

(g) **Certain Research** - A Covered Component may use or disclose PHI without an authorization for certain research purposes in the following circumstances:

(i) Upon obtaining documentation of Institutional Review Board (IRB) approval of a waiver or alteration of the authorization requirements;

(ii) For reviews preparatory to research if the researcher provides appropriate assurances;

(iii) For research on decedents if the researcher provides appropriate assurances; or

(iv) For disclosure of de-identified information or limited data sets (as described in Section 4.4(h)-(i) below).

(h) **De-Identified Information** - A Covered Component may use or disclose health information that has been de-identified. Health information is de-identified if the health information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. Once PHI has been properly de-identified, the information is no longer subject to the HIPAA Privacy Standards. PHI may be de-identified by removing the certain identifiers of the individual,[2] or of relative, employers, or household members of the individual; provided that the Covered Components do not have actual knowledge that the information could be used alone or in combination with other information to identify the individual who is the subject of the information. PHI may also be de-identified by a qualified statistician in accordance with the Privacy Standards. The Covered Component may choose to assign a code or other means of record identification to allow de-identified information to be re-identified by the Covered Component, however, the code or other means of record identification cannot be derived from or related to information about the individual and cannot be otherwise capable of being translated so as to identify the individual. The Covered Component may not use or disclose the code or other means of record identification for any other purpose, other than for re-identification by the Covered Component. The Covered Component may not disclose the mechanism for re-identification. The Covered Component may use a third party to de-identify information on its behalf if it has entered into a business associate agreement with such third party permitting the third party to de-identify the information. All business associate agreements must be approved by a Privacy Officer.

(i) **Limited Data Sets** – A Covered Component may use or disclose PHI for the purposes of research, public health, or health care operations that is part of a limited data set, provided that a data use agreement with the recipient is in effect. Certain indirect identifiers (e.g., cities, states, zip codes, and certain dates) may be included in a limited data set, however the data use agreement must provide that the recipient of the limited data set will only use and disclose the PHI for limited purposes. All data use agreements must be approved by a Privacy Officer.

(j) **Accounting of Certain Disclosures** - For disclosures permitted under the Privacy Standards that are not excluded (as described in Section 9.3(a) below), Covered Components must track and retain the information required for an accounting of disclosures as set forth in Section 9.3(d) below. Each of the University's health care providers listed in Section 1.2 above have developed a form for tracking disclosures. Copies of this form may be obtained by contacting the appropriate Privacy Officer.

5. Notice of Privacy Practices

5.1 **General** – Under HIPAA, each of the University's health care providers listed in Section 1.2 above must provide individuals with a Notice of Privacy Practices that meets the requirements of the Privacy Standards. Among other things, the Notice of Privacy Practices describes how the Covered Component may use and disclose PHI, individuals' rights with regards to PHI, and who to contact for further information regarding the Covered Component's privacy practices. Each of the University's health care providers listed in Section 1.2 above have developed a Notice of Privacy Practices which applies to all Covered Components of the University. Each Covered Component shall act in conformance with the its Notice of Privacy Practices and shall abide by its terms and conditions.

---

[2] The identifiers are: (1) Names; (2) All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes (however, the initial three digits of a zip code may be used if, according to the current publicly available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000); (3) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (4) Telephone numbers; (5) Fax numbers; (6) Electronic mail address; (7) Social security numbers; (8) Medical records numbers; (9) Health plan beneficiary numbers; (10) Account numbers; (11) Certificate/license numbers; (12) Vehicle identifiers and serial numbers, including license plate numbers; (13) Device identifiers and serial numbers; (14) Web Universal Resource Locators (URLs); (15) Internet Protocol (IP) address numbers; (16) Biometric identifiers, including finger and voice prints; (17) Full face photographic images and any comparable images; and (18) Any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes described below.

5.2 **Distribution of Notices of Privacy Practices** – Each of the University's health care providers listed in Section 1.2 above must provide a copy of its Notice of Privacy Practices to an individual no later than the date of the first service delivery unless it is not feasible due to an emergency situation. In an emergency treatment situation, the health care provider should provide the Notice of Privacy Practices as soon as reasonably practicable after the emergency treatment situation. The Notice of Privacy Practices must be prominently posted in the University's health care facilities and must be on the University's website. Copies of the Notice of Privacy Practices must also be available at each service delivery site and given to every individual who requests a copy.

5.3 **Acknowledgment of Receipt of Notice of Privacy Practices** – Health care providers must make a good faith effort to obtain written acknowledgment of each individual's receipt of a Notice of Privacy Practices. Each of the University's health care providers listed in Section 1.2 above has developed a form Acknowledgment of Receipt of Notice of Privacy Practices. If the health care provider is unable to obtain the acknowledgment, the health care provider must document his or her efforts to obtain the authorization and the reasons why it could not be obtained.

5.4 **Changes to the Notice of Privacy Practices** – Each Covered Component reserves the right to change its Notice of Privacy Practices. All changes to Notices of Privacy Practices must be approved by a Privacy Officer prior to use. Whenever the Notices of Privacy Practices are revised, the Covered Component(s) will post the new Notices and new Notices of Privacy Practices will be available upon request.

5.5 **Documentation of Notice of Privacy Practices.**– The Covered Components must retain documentation of all Notices of Privacy Practices and all written acknowledgements of the receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment in accordance with Section 10 (Documentation) below.

6. **Minimum Necessary**

6.1 **Minimum Necessary Policy** – University employees, agents, and subcontractors shall only access, receive, and use PHI to the extent that the PHI is needed to provide the necessary or requested services. PHI should be accessed, used, and disclosed only by authorized personnel. When using or disclosing PHI or when requesting PHI from another entity covered by the Privacy Standard, a Covered Component must make reasonable efforts to limit its uses, disclosures, or requests of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. In addition, the following restrictions regarding the use and/or access to PHI for the following classes of employees/contractors of the Covered Components shall be in place:

(a) **Treatment Personnel** – All treatment personnel shall have full access to PHI to the extent necessary for such personnel to carry out their duties, and may include the entire medical record, if the entire medical record is required for such treatment personnel to perform his or her duties. All such use and/or access shall be in accordance with the specific policies and procedures that may from time to time be adopted by the specific Covered Component as set forth in Section 6.3 below.

(b) **Billing and Collection Personnel** – Billing and collection personnel shall have full access to PHI to the extent necessary for such personnel to carry out their duties, and may include the entire medical record, if the entire medical record is required for such billing personnel to perform his or her duties. All such use and/or access shall be in accordance with the specific policies and procedures that may from time to time be adopted by the specific Covered Component as set forth in Section 6.3 below.

(c) **University Archives Personnel and Medical Records Personnel** – University archives personnel and medical records personnel shall have access to PHI to the extent necessary for such personnel to carry out their duties, and may include the entire medical record, if the entire medical record is required for such personnel to perform his or her duties, which include, among other things, accessing records in order to facilitate treatment, payment, and health care operations of the University's Covered Components. All such use and/or access shall be in accordance with the specific policies and procedures that may from time to time be adopted by the specific Covered Component as set forth in Section 6.3 below.

(d) **University Executive Officers** – The executive officers of the University shall have full access to PHI to the extent necessary for such personnel to carry out their duties, and may include the entire medical record, to the extent that such access is necessary for the executive officers to carry out their respective duties of providing overall administration of the Covered Components. All such use and/or access shall be in accordance with the specific policies and procedures that may from time to time be adopted by the specific Covered Component as set forth in Section 6.3 below.

(e) **Health and Safety, Risk Management, and Audit Personnel** – Personnel dealing with health and safety, risk management, and University audits shall have access to PHI to the extent necessary for such personnel to carry out their duties, and may include the entire medical record, to the extent that such access is necessary for such individuals to carry out their respective duties of providing health and safety, risk management, and audit services to the Covered Components. All such use and/or access shall be in accordance with the specific policies and procedures that may from time to time be adopted by the specific Covered Component as set forth in Section 6.3 below.

(f) **Information Technologies Personnel** – Personnel dealing with information technologies shall have access to PHI to the extent necessary for such personnel to carry out their duties, which may include the entire medical record, to the extent that such access is necessary for such individuals to carry out their respective duties. All such use and/or access shall be in accordance with the specific policies and procedures that may from time to time be adopted by the specific Covered Component as set forth in Section 6.3 below.

(g) **Administrative Personnel** – Administrative personnel's access to PHI shall be limited to the extent necessary to carry out their duties, which should not, other than under very limited circumstances, include access to the entire medical record. For the purposes of this policy, administrative personnel shall include: secretaries, administrative assistants, and receptionists. All such use and/or access shall be in accordance with the specific policies and procedures that may from time to time be adopted by the specific Covered Component as set forth in Section 6.3 below.

6.2 **Exclusions from the Minimum Necessary Policy** – The minimum necessary policy does not apply to:

(a) Disclosures to or requests by a health care provider for treatment;

(b) Uses or disclosures made to the individual of his or her own PHI;

(c) Uses or disclosures made pursuant to an authorization;

(d) Disclosures made to the Secretary of the United States Department of Health and Human Services;

(e) Certain uses and disclosures that are required by law; and

(f) Uses and disclosures that are required for compliance with the Privacy Standards.

6.3 **Implementation of Minimum Necessary Policies** – Each Covered Component shall identify any other persons or class of persons who need access to PHI in order to carry out the functions of his or her job other than those listed in Section 6.1 above, identify the types of health information to which access is necessary; and develop appropriate conditions on such access. When requesting PHI from another entity covered by the Privacy Standard, a Covered Component shall limit its uses, disclosures, or requests of PHI to the minimum necessary to accomplish the intended purpose of the request. Typical requests of the University's Covered Components that are health care providers are for treatment purposes, which are exempt from the minimum necessary policy. All other requests for PHI will be the minimum necessary in order to accomplish the specific purpose of the request, unless the individual authorizes a broader type of disclosure. For any other type of disclosure that it makes on a routine and recurring basis, each Covered Component is responsible for developing and implementing procedures (which may be standard protocols) that limit uses, disclosures, and requests of PHI to the minimum amount necessary to accomplish the intended purpose. For all other uses, requests, disclosures, each Covered Component must develop criteria and policies designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought and review requests for disclosure on an individual basis in accordance with such criteria. Such policies shall be kept on file by the Covered Component and are subject to review by the University's Privacy Officers.

6.4 **Reliance on Others** – Covered Components may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when: (i) making disclosures to public officials that are required by law, if the public official represents that the information is the minimum necessary for the stated purposes; (ii) the information is requested by another entity covered by the Privacy Standards; (iii) the information is requested by a professional who is a member of the Covered Components' workforce or is a business associate of the Covered Components for the purpose of providing professional services to the Covered Components, if the professional represents that the information requested is the minimum necessary for the stated purpose; or (iv) documentation or representations that comply with the Privacy Standards has been provided by the person requesting the PHI for research purposes.

6.5 **Disclosure of Entire Medical Record** – Covered Components shall not use, disclose, or request an entire medical record, except in cases in which the entire medical record is specifically justified as the amount reasonably necessary to accomplish the purpose of the use, disclosure, or request.

7. **Safeguarding and Storage of PHI**

7.1 **General** – All PHI is to be treated as confidential and in a manner to protect it from being intentionally or unintentionally heard, seen, or received by an individual or entity without a need or right to the PHI. All PHI in hard copy shall be stored in a secure manner (e.g., in a locked cabinet or secure area). All University employees in each Covered Component, and their agents and subcontractors must use appropriate safeguards to prevent the unauthorized use or disclosure of PHI, and shall follow all University policies and procedures with respect to such safeguards and storage as may be from time-to-time enacted. Each Covered Component shall also establish and implement HIPAA policies and procedures regarding safeguarding PHI as applicable, including mechanisms to control the flow of PHI from Covered Components to Non-Covered Components; physical, administrative, and procedural safeguards to ensure PHI is not improperly used, disclosed, or obtained; and policies and procedures to ensure adequate separation when staff is shared between Covered Components and Non-Covered Components.

7.2 **Electronic PHI**– Before leaving computers unattended, all operators shall first close out of any program that contains PHI or shall secure his or her computer with a password protected screen saver. All computers containing PHI shall be shut down at the end of the day. Passwords shall not be shared with any other University employee, agent, subcontractor, or any other third party.

8. **Training**

8.1 **General** – The University shall provide training on the University's HIPAA policies and procedures for all members of its workforce that are included in the University's Covered Components, as necessary and appropriate for such members of its workforce to carry out their functions within the University.

8.2 **New Members of Workforce** – The University shall provide training on the University's HIPAA policies and procedures for all new members of its workforce that are included in the University's Covered Components within a reasonable period of time after such persons join the University's workforce.

8.3 **Training on New HIPAA Policies and Procedures** – Following initial training, in the event of any material change in the University's HIPAA policies and procedures, the University shall train the members of its workforce whose functions are affected by the material change within a reasonable time after the material change becomes effective.

8.4 **Documentation of Training** – The University shall document that HIPAA training as set forth in this Section 8 has been provided in accordance with Section 10 (Documentation) below.

9. **Individuals' Rights Regarding PHI** – HIPAA provides certain rights to individuals regarding their PHI, as set forth below.

9.1 **Right to Access**

(a) **Requests for Access** – Individuals generally have the right to access, inspect, and obtain a copy of PHI maintained in his or her medical record. Individuals must make a written request to the Covered Component to access their PHI. Individuals may be charged a reasonable cost-based fee for the costs of copying, mailing, or other supplies associated with their request. Each of the University's health care providers listed in Section 1.2 above have developed a form for individuals to request access to PHI. Copies of this form may be obtained by contacting the appropriate Privacy Officer.

(b) **Denial of Access** – Individuals may be denied access to psychotherapy notes and to other information in certain circumstances under the Privacy Standards. Such other information includes PHI compiled for use in legal or administrative actions; certain PHI involving the Clinical Laboratory Improvement Amendments of 1988 (CLIA); PHI requested by inmates that may jeopardize health, safety, or security; PHI that is temporarily suspended during research; PHI subject to the federal Privacy Act; PHI obtained from someone other than a health care provider under a promise of confidentiality; or PHI a professional has determined is reasonably likely endanger life or physical safety or cause substantial harm. The Privacy Standards require that for some denials, the individual is given the right to request a review of the denial by a health care professional not involved in the initial decision. Covered Components, must, to the extent possible, provide any other PHI requested to the individual after excluding the PHI properly denied. Covered Components must have approval from a Privacy Officer before denying an individual's request for access. If the Covered Component denies a request for access (with the approval of a Privacy Officer), it must inform the individual of its decision in writing within the time limits set forth in Section 9.1(d) below. The written denial must be in plain language and contain (i) the basis of the denial; (ii) a statement of the individual's rights regarding review of the decision and how the individual may exercise his/her review rights; and (iii) a description of how the individual may complain to the University's Privacy Officer or the Secretary of Health and Human Services. Each of the University's health care providers listed in Section 1.2 above have developed a form for responding to requests for access of PHI. Copies of this form may be obtained by contacting the appropriate Privacy Officer.

(c) **Granting Access** – If the Covered Component grants a request for access, it must inform the individual of its decision and provide the access requested in the time limits set forth in Section 9.1(d) below. Access to the PHI must be in the form or format requested by the individual if it is readily producible in such form or format. If access is not readily producible in such form or format, the PHI should be provided in readable hard copy form or such other form or format agreed to by the

Covered Component and the individual. Access must be provided in a timely manner and at a convenient time and place. Each of the University's health care providers listed in Section 1.2 above have developed a form for responding to requests for access of PHI. Copies of this form may be obtained by contacting the appropriate Privacy Officer.

(d) **Timing of Response to Request for Access** – Covered Components must act on a request for access (whether access is granted or denied) no later than thirty (30) days after receipt of the request. However, if the PHI is not maintained or accessible on-site, the Covered Component must act no later than sixty (60) days from the receipt of the request. In exceptional situations, when the Covered Component is unable to take action within these time periods, the Covered Component may extend the time for action by no more than thirty (30) days, provided that within the first thirty (30) or sixty (60) days (as the case may be), the Covered Component provides the individual with a written statement of the reasons for delay and the date by which the Covered Component will take action on the request. A Covered Component may only have one extension of time per request.

(e) **Requests to the Wrong Entity** – If the Covered Component does not maintain the PHI involved in the individual's request, and the Covered Component knows where the requested PHI is maintained, the Covered Component must inform the individual where to direct the request for access.

(f) **Access Documentation** – Covered Components must document the designated record sets that are subject to access by individuals, the titles of the persons or offices responsible for receiving and processing requests for access, and all written communication regarding the access in accordance with Section 10 (Documentation) below.

9.2 **Right to Amend**

(a) **Request to Amend** - Individuals generally have the right, with limited exceptions, to request a Covered Component amend their medical record. Individuals must make a request to amend in writing and must explain why the information should be amended. Each of the University's health care providers listed in Section 1.2 above have developed a form for individuals to request to amend their PHI. Copies of this form may be obtained by contacting the appropriate Privacy Officer.

(b) **Timing of Response to Requests to Amend** – Covered Components must act on a request to amend PHI (whether amendment is granted or denied) no later than sixty (60) days after receipt of the request. In exceptional situations, when the Covered Component is unable to take action within sixty (60) days, the Covered Component may extend the time for action by no more than thirty (30) days, provided that within the first sixty (60) days, the Covered Component provides the individual with a written statement of the reasons for delay and the date by which the Covered Component will take action on the request. A Covered Component may only have one extension of time per request.

(c) **Denial of Request to Amend** – Covered Components may deny an individual's right to amend his or her medical record if: the request is not in writing; the request does not provide a reason for the amendment; the individual's health information was not created by the University's Covered Components (unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment); the PHI is not part of the information maintained by the University's Covered Components; the amendment pertains to information the individual is not permitted to copy and inspect under law; or the information in the individual's medical record is complete and accurate. All requests to amend shall be forwarded to a Privacy Officer and Covered Components must have approval from a Privacy Officer before denying an individual's request for amendment. If the Covered Component denies a request for amendment (with the approval of a Privacy Officer), it must inform the individual of its decision in writing within the time limits set forth in Section 9.2(b) above. The written denial must be in plain language and contain: (i) the basis of the denial; (ii) the individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement; (iii) a statement that if the individual does not submit a statement of disagreement, the individual may request that the Covered Component provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and (iv) a description of how the individual may complain to the University's Privacy Officer or the Secretary of Health and Human Services. Each of the University's health care providers listed in Section 1.2 above have developed a form for responding to requests to amend PHI. Copies of this form may be obtained by contacting the appropriate Privacy Officer.

(d) **Responses to Denials to Amend** – Covered Components must permit individuals to submit a written statement which disagrees with the denial of all or part of the requested amendment and states the basis of such disagreement. Each of the University's health care providers listed in Section 1.2 above have developed a form for statements of disagreement and requests to include an amendment request and denial with future disclosures. Copies of these forms may be obtained by contacting the appropriate Privacy Officer. Covered Components may prepare a written rebuttal to an individual's statement of disagreement. When a Covered Component prepares a written rebuttal, the Covered Component must provide a copy to the individual. As appropriate, the Covered Components must identify the records that are the subject of the disputed amendment and then append or otherwise provide a link to the individual's request for an amendment and the Covered Component's denial of the request (if

requested by the individual), and the individual's statement of disagreement, and the covered entity's rebuttal (if such documents exist).

(e) **Granting Amendment** – All requests for amendments shall be forwarded to a Privacy Officer and Covered Components must have approval from a Privacy Officer before granting an individual's request for amendment. If the Covered Component grants a request for amendment (with the approval of a Privacy Officer), it must inform the individual of its decision and obtain the individual's agreement to have the Covered Component notify the relevant person with whom the amendment needs to be shared within the time limits set forth in Section 9.2(b) above. Each of the University's health care providers listed in Section 1.2 above have developed a form for responding to requests to amend PHI. Copies of this form may be obtained by contacting the appropriate Privacy Officer. Once the Covered Component grants a request for an amendment, the Covered Components must make the appropriate amendment to the PHI by identifying the records that are affected by the amendment and then appending or otherwise providing a link to the location of the amendment. Information should not be deleted from an individual's medical record. The Covered Components must make reasonable efforts to provide the amendment within a reasonable time to: (i) persons identified by the individual as having received PHI about the individual and needing the amendment; and (ii) persons, including business associates that the Covered Component knows have the PHI and that may have relied or could foreseeably rely on such information to the detriment of the individual. Each of the University's health care providers listed in Section 1.2 above have developed a form for notifying entities and individuals of an amendment to a individual's PHI. Copies of this form may be obtained by contacting the appropriate Privacy Officer. The Covered Component must include the amendment in any future disclosures of the individual's medical record.

(f) **Amendment Documentation** – Covered Components must document the titles of the persons or offices responsible for receiving and processing requests for amendment and all written communication regarding the amendment in accordance with Section 10 (Documentation) below.

9.3 **Right to an Accounting**

(a) **Requests for an Accounting** – Individuals have the right to receive a list of instances in which the University's Covered Components have disclosed his or her PHI in the six (6) years prior to the date the accounting is requested, except for those disclosures set forth by law. The disclosures excepted by law include disclosures:

(i) To carry out treatment, payment, and health care operations as described in Section 4.5(b) above.

(ii) To individuals of PHI about them as described in Section 4.5(a) above;

(iii) Incident to a use or disclosure otherwise permitted by the Privacy Standards;

(iv) Pursuant to an authorization as described in Section 4.4 above;

(v) For the Covered Component's directory or to person involved in the individual's care or for other notification purposes as described in 4.5(e) above;

(vi) For national security, intelligence purposes, or to correctional institutions or law enforcement officials as permitted by the Privacy Standards;

(vii) As part of a limited data set; or

(viii) That occurred prior to April 14, 2003.

Each of the University's health care providers listed in Section 1.2 above have developed a form for individuals to request an accounting of disclosures. Copies of this form may be obtained by contacting the appropriate Privacy Officer. All requests for an accounting must be forwarded to a Privacy Officer for review and approval.

(b) **Temporary Suspension of Right to Accounting** – Covered Components may temporarily suspend an individual's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official if the agency or official informs the Covered Component orally or in writing that an accounting to such an individual would be reasonably likely to impede the agency's activities. A written statement must specify the time period for the suspension. If the statement is made orally, the Covered Component must document the oral statement, including the identity of the agency or official making the statement; temporarily suspend the individual's right to an accounting; and limit the temporary suspension to no longer than thirty (30) days of the date of the oral statement, unless the agency provides a written statement during that time.

(c) **Timing of Response to Request for an Accounting and Fees** – Covered Components must act on a request to amend PHI (whether amendment is granted or denied) no later than sixty (60) days after receipt of the request. In exceptional situations, when the Covered Component is unable to take action within sixty (60) days, the Covered Component may extend the time for action by no more than thirty (30) days, provided that within the first sixty (60) days, the Covered Component provides the individual with a written statement of the reasons for delay and the date by which the Covered Component will take action on the request. A Covered Component may only have one extension of time per request. Covered Components must provide the first accounting to an individual in any twelve (12) month period without charge. Thereafter, for any additional accounting

requested in the same twelve (12) month period, the Covered Component may charge a reasonable, cost-based fee, provided that the Covered Component informs the individual in advance of the fee and provides the individual an opportunity to withdraw or modify his or her request.

(d) **Accounting Information** – Covered Components must provide the individual with a written accounting within the time limits set forth in Section 9.3(c) above. The accounting must include all disclosures (not excepted under Section 9.3(a) above) that occurred up to six (6) years prior to the date of the request (or a shorter time period requested by the individual), including:

(i) The date of the disclosure;

(ii) The name of the entity or person who received the PHI, and if known, the address of such person or entity;

(iii) A brief description of the PHI disclosed; and

(iv) A brief description 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 the disclosure).

More limited accountings may be provided in accordance with the Privacy Standards for multiple disclosures of PHI to the same person or entity for a single purpose or disclosures for certain research. Covered Components should contact a Privacy Officer in recording accounting information or in assembling responses to requests for accountings.

(e) **Accounting Documentation** – Covered Components must document the titles of the persons or offices responsible for receiving and processing requests for an accounting, the information required to be included in an accounting, and the written accounting provided to the individual in accordance with Section 10 (Documentation) below. All written communication regarding the accounting should also be documented in accordance with Section 10 (Documentation) below.

9.4 **Right to Request Restrictions** – An individual has the right to request that the Covered Components place additional restrictions on their use and disclosure of the individual's PHI for treatment, payment, or healthcare operation, or to people involved in the individual's health care. Individuals must make their request for additional restrictions in writing. Covered Components are not required to agree to the requested restrictions, but if one Covered Component agrees to a restriction, all of the Covered Components must abide by the agreement (except in an emergency).

(a) **Procedures for Restrictions Requests** - All requests for restrictions must be approved by a University Privacy Officer. All agreements for additional restrictions must be in writing and signed by a person authorized to make such an agreement on behalf of the University. Agreements for additional restrictions must be documented in accordance with Section 10 (Documentation) below. Each of the University's health care providers listed in Section 1.2 above have developed a form for individuals to request restrictions, a form to respond to a request for additional restrictions, and a form for termination of a restriction. Copies of these forms may be obtained by contacting the appropriate Privacy Officer.

(b) **Termination of Restrictions** - A Covered Component may terminate its agreement to a restriction if:

(i) The individual agrees to or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented; or

(iii) The Covered Component informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after the Covered Component has informed the individual.

9.5 **Right to Confidential Communications** – An individual has the right to request that the University's Covered Components communicate with him or her about PHI by alternative means (e.g., email instead of postal mail) or to alternative locations (e.g., work rather than home). Individuals must make their request for confidential communications in writing and specify where or how they wish to be contacted. University employees or agents may not require an explanation from the individual as to the basis for the request (i.e., why the individual desires confidential communications). Covered Components must accommodate all reasonable requests. All requests for confidential communications must be approved by a University Privacy Officer. Each of the University's health care providers listed in Section 1.2 above have developed a form for individuals to request restrictions on the manner/method of confidential communications. Copies of this form may be obtained by contacting the appropriate Privacy Officer.

10. **Documentation** – All policies, procedures, communications, actions, activities, or designations that require documentation under HIPAA shall be maintained by the University's Covered Components in written or electronic form and shall be retained for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

11. **Unauthorized Uses and Disclosures of PHI**

11.1 **Reporting Unauthorized Uses and Disclosures** – If any University employee, agent, or subcontractor becomes aware of any use or disclosure of PHI that is not in accordance with this policy, such individual shall immediately notify the appropriate Privacy Officer.

11.2 **Procedures in the Event of a Report of an Unauthorized Use or Disclosure** – The University will promptly investigate any and all reports that PHI has been used or disclosed in violation of this policy, and shall make all appropriate notifications of the unauthorized use or disclosure. The University shall also make appropriate efforts to mitigate, to the extent practicable, any known harmful effect of a use or disclosure in made violation of the University's HIPAA policies or procedures by the University or a business associate of the University.

12. **Penalties for Unauthorized Use or Disclosure of PHI** – The University shall impose appropriate sanctions on any employee, agent, or subcontractor who is determined to violate this policy, up to and including suspension or termination. The University shall document any sanctions that are applied in accordance with Section 10 (Documentation) above.

13. **Complaints Process for Making Complaints** – Any individual may make complaints regarding the University's HIPAA policies and procedures or compliance therewith. All complaints must be in writing and should be sent to the appropriate Privacy Officer. Each of the University's health care providers listed in Section 1.2 above have developed a form for individuals to make a complaint. Copies of complaint forms may be obtained by contacting the appropriate Privacy Officer.

13.2 **No Penalty for Complaints** – No individual will be penalized in any way for making a complaint regarding the University's HIPAA policies and procedures or compliance therewith.

13.3 **Investigation of Complaints** – The Privacy Officer will investigate all complaints in a timely manner and shall appropriately document the investigation. The Privacy Officer shall make a written record of the disposition of the complaint and shall notify all parties involved of the disposition of the allegation (e.g., the individual(s) who made the complaint and all University departments involved).

13.4 **Documentation of Complaints** – The Privacy Officers shall keep appropriate documentation of all complaints and their dispositions in accordance with Section 10 (Documentation) above.

13.5 **No Waiver of Rights to File a Complaint** – No individual shall be required to waive their right to file a complaint under HIPAA as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

14. **No Intimidation or Retaliatory Acts** – The University, University employees, or any individual acting on behalf of the University may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against: (a) any individual for exercising any rights under, or for participating in any process established by HIPAA, including filing a complaint under the Privacy Standards; (b) any person for filing a compliant with the Secretary of the United States Department of Health and Human Services under the Privacy Standards; (c) any person testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI of the Social Security Act; or (d) any person opposing any act or practice made unlawful by HIPAA, provided the person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of the Privacy Standards.

15. **Compliance with Laws** – The University shall cooperate with all investigations and compliance checks conducted by the United States Department of Health and Human Services ("HHS") to determine whether the University is in compliance with HIPAA.

16. **Changes to this Policy** – The University may change this policy at any time and for any reason. The University shall change this policy and its procedures as necessary and appropriate to comply with the standards of HIPAA.