MONTCLAIR STATE UNIVERSITY

HIPAA PRIVACY POLICY

Approved by the Montclair State University Board of Trustees on April 3, 2014

Revised November 5, 2015

Table of Contents

I. PURPOSE

A. Montclair State University adopts this policy to establish requirements for the use and disclosure of individually identifiable protected health information in conformance with the Health Insurance Portability and Accountability Act of 1996, and the Health Information Technology for Economic and Clinical Health Act of 2009.

B. This policy does not apply to health information contained within education records covered under the Family Educational Rights and Privacy Act ("FERPA").

II. WHO IS SUBJECT TO THIS POLICY

A. Montclair State University is a Hybrid Entity because certain University employees provide Treatment in a University created clinic or faculty practice and submit medical bills to federal or state reimbursement programs or private health insurance carriers for Payment. The Health Care Components of the University are listed in Exhibit A and must comply with this Policy.

III. DEFINITIONS

The following definitions shall apply to the following terms throughout this Policy and without regard to whether they are capitalized. All undefined terms shall have the same meaning as defined by HIPAA.

Accounting of Disclosures – A written record of certain disclosures of PHI that may be required to be maintained and provided to a requesting individual under certain circumstances described in this policy.

Access – the ability or the means necessary to read, write, modify, or communicate data or information or otherwise use any system resource.

Authorization – A written document completed and signed by the individual that generally allows use and disclosure of PHI for purposes other than Treatment, payment or health care operations.

Breach - the acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA which compromises the security or privacy of the PHI. Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a Workforce member or person acting under the authority of a Healthcare Component or Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by HIPAA.

(ii) Any inadvertent disclosure by a person who is authorized to access PHI at a Healthcare Component or Business Associate to another person authorized to access PHI at the same Healthcare Component or Business Associate, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA.

(iii) A disclosure of PHI where a Healthcare Component or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Business Associate. An entity, other than in the capacity of a member of the Healthcare Component workforce, that creates, receives, maintains, or transmits PHI for on behalf of Healthcare Component or that provides services to or for Healthcare Component where the provision of services involves the disclosure of Healthcare Component's PHI. 45 C.F.R. § 160.103.

Covered Entity – the Health Care Components designated by MSU.

Covered Function – Those functions of a Healthcare Component the performance of which makes the Healthcare Component subject to HIPAA.

De-identified Information – Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. De-identified Information is not subject to the HIPAA Privacy Rule.

Designated Record Set – Medical or billing records about individuals maintained by or for a healthcare provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or records used in whole or in part by or for the provider to make decisions about individuals.

Discovery of a Breach. A Breach is considered to be discovered by Healthcare Component as of the first day on which the Breach is known to Healthcare Component or should have been known to Healthcare Component if it had exercised reasonable due diligence.

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

Health care – Care, services, or supplies related to the health of an individual. Health Care includes, but is not limited to, the following: Preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service assessment, or procedure with respect to the physical or mental condition, or functional status, or an individual or that affects the structure or function of the body; and Sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

Health Care Component – A component of the University in accordance with its designation as a hybrid entity as listed in Exhibit A.

Health Information – Any information, whether oral or recorded in any form or medium, that:

1. is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

2. relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

HIPAA – Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d *et seq.*

HIPAA Privacy Regulations – The HIPAA Standards for Privacy of Individually Identifiable Health Information, as set forth in 45 CFR Parts 160 and 164 and as otherwise amended.

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 health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

MSU – Montclair State University.

Privacy Officer shall mean the individual appointed by the Provost to assume the obligations of the Privacy Officer in this Policy.

Protected Health Information ("PHI") - Protected health information means individually identifiable health information that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual, and identifies or could reasonably be used to identify the individual.

PHI includes information that is transmitted by electronic media; maintained in electronic media or transmitted or maintained in any other form or medium.

PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 USC 1232g; records described at 20 USC 1232g(a)(4)(B)(iv); and employment records[1] held by a Healthcare Component in its role as employer.

Payment - activities undertaken by a Healthcare Component to obtain payment for the provision of healthcare; and relates to the individual to whom health care is provided.

Personal Information ("PI") – an individual's first name or first initial and last name linked with one or more of the following data elements:

[1] Employment records that are not subject to this HIPAA Privacy Policy include medical information needed to carry out the University's obligations under the Family Medical Leave Act, the American's with Disabilities Act, and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance, and fitness-for-duty tests of employees.

1. Social Security number

2. Driver's license number or State identification card number

3. account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

Personally Identifiable Information ("PII") – Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Protected Health Information ("PHI") - Any oral, written, or electronic individually identifiable health information maintained or transmitted in any form or medium. Individually identifiable health information includes demographic information and any information that relates to 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 any individual.

Psychotherapy notes – Notes recorded (in any medium) by a health care provider who is a mental health professional that:

1. Document or analyze the contents of conversation during a private counseling session or a group, joint or family counseling session, and

2. Are separated from the rest of the individual's medical record.

3. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of Treatment furnished, results of clinical tests, and any summary diagnosis, functional status, Treatment plan, symptoms, prognosis, and progress to date.

Psychotherapy notes are used only by the therapist who wrote them, maintained separately from the medical record and not normally involved in the documentation necessary for health care Treatment, payment or health care operations.

Public health authority – An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Treatment – the provision, coordination, or management of health care and related services by one or more health care providers, including:

1. the coordination or management of health care by a health care provider with a third party

2. consultation between health care providers relating to a patient, or

3. the referral of a patient for health care from one health care provider to another.

"TPO" – To carry out treatment, payment or healthcare operations

University – Montclair State University

Unsecured PHI. Protected health information that is not encrypted and rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services (HHS).

Workforce – employees, volunteers, trainees, and other persons whose conduct, in the performance of work is under the direct control of the Healthcare Component, whether or not their services are paid by the entity.

IV. HYBRID ENTITY DESIGNATION

A. The University has designated itself a Hybrid Entity in accordance with HIPAA and adopts this Policy to ensure that its Health Care Components comply with the requirements of HIPAA.

1. The University's Health Care Components are listed in Exhibit A. Exhibit A shall be retained for at least six (6) years following any decision to terminate any division or department from the University's Health Care Components. Designations that remain a Health Care Component of the University should be retained permanently.

2. Firewalls must be implemented between Health Care Component's Covered Functions and all other functions. Specifically, MSU will ensure that:

   a. In circumstances that require a Health Care Component to disclose PHI to any department, division, school or college that is not a Health Care Component, the Health Care Component shall clearly mark the PHI as confidential;

   b. Each department, division, school or college within MSU that receives PHI shall not use or disclose PHI that it creates or receives from or on behalf of the Health Care Component in a way that is prohibited by HIPAA Privacy Regulations and Privacy Rule, and otherwise complies with HIPAA's Security Standards.

   c. Wherever possible, MSU Workforce performing Covered Functions shall be separated from Workforce that is performing other functions.

d. If a Workforce member performs duties for both a Health Care Component and other department, division, School or College that is not a Health Care Component, such Workforce member must not use or disclose PHI created or received in the course of or incident to the Workforce member's work for the Health Care Component in a way prohibited by this Policy.

V. USE AND DISCLOSURE OF PHI WITH AND WITHOUT CONSENT

A. Healthcare Component shall protect PHI from disclosure as required by this Policy.

B. Healthcare Component may not use or disclose PHI without a signed authorization by the individual from whom the PHI was created unless it is otherwise permitted under HIPAA, including under the following circumstances:

1. When requested by the Secretary of the United States Department of Health and Human Services ("DHHS") to investigate or determine compliance with privacy standards;

2. When the disclosure is to the individual to whom the PHI pertains, or a legal personal representative, including requests for accounting or access to inspect or copy;

3. To carry out treatment, payment or healthcare operations (hereinafter collectively referred to as "TPO");

4. Where an opportunity to agree or to object has been afforded to the individual and the individual does not object to the use and disclosure of PHI in the following circumstances:

a. To family and friends involved with the individual's care or payment related to the individual's healthcare, or

b. To disaster relief agencies to coordinate the notification of family and friends regarding the individual's location, condition, or death;

d. For information needed by coroners, medical examiners and funeral directors.

e. For information needed to facilitate an organ donation.

f. To alert a law enforcement agency of the death if the Healthcare Component has a suspicion that such death may have resulted from criminal conduct. If the agency is already investigating the death, other law enforcement powers to obtain PHI may apply.

5. When the information listed in Exhibit B has been de-identified and there is no actual knowledge by the Healthcare Component that any of the remaining information could identify the individual.

6. As otherwise permitted under the HIPAA regulations.

C. In the event any state and federal law affords protection to privacy rights greater than this Policy, Healthcare Component shall comply with such greater obligations, (e.g. treatment for drug and alcohol use, HIV/AIDS, and mental health).

1. For psychotherapy notes, a valid authorization must be obtained for any use and disclosure unless otherwise permitted by HIPAA.

D. Uses and Disclosures for TPO

1. Healthcare Component may use and disclose PHI necessary to provide Treatment, obtain Payment, and conduct administrative and operational tasks as necessary to provide Health Care Services in accordance with Exhibit C.

2. Patients may request restrictions on the uses or disclosures of PHI for TPO. Healthcare Components must restrict disclosure of PHI if: a) the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and b) the PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the Healthcare Component in full.

3. The following types of activities require a written authorization from the individual who generates the PHI:

a. Marketing and fundraising activities require an authorization prior to the use and disclosure and PHI. The University will comply with HIPAA in the event it uses PHI for marketing purposes. All Workforce shall consult the Privacy Officer and University Counsel before using any PHI for marketing in order to ensure compliance with HIPAA.

b. Research activities require a written authorization unless there is written documentation that the University's IRB either waived or altered the requirement. See Exhibit C for requirements and specifications under which an authorization would not be required for Research.

E. Opportunity to Agree or Object

In the following three (3) circumstances, PHI may be disclosed without an authorization as long as the patient is given an opportunity to agree or object. Healthcare Component must establish a process to document that opportunity was afforded and if the individual objected.

1. To Persons involved in Treatment or Payment

a. PHI may be disclosed to a family member, a personal representative of the individual or another person when:

i. That information is relevant to such person's involvement with the individual's care or payment related to such care, or

ii. To notify (or assist in the notification of) such persons of the individual's location, general condition or death, and

iii. When sections below are complied with.

b. If the individual is present and has the capacity to make healthcare decisions, the Healthcare Component may use or disclose the PHI only if it:

i. Obtains the individual's agreement;

ii. Provides the individual the opportunity to object and the individual does not object; or

iii. Can be reasonably inferred from the circumstances, using its professional judgment, that the individual does not object to the disclosure.

c. If the individual is incapacitated or unable to consent due to emergency circumstance, the PHI may be disclosed only if:

i. The PHI is directly relevant to the person's Treatment, and it is in the individual's best interest:

ii. Healthcare Component may use professional judgment and experience with common practice to make reasonable inferences regarding the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-ray films, or other similar forms of PHI.

2. Disaster Relief Efforts

PHI may be used or disclosed to a public or private entity to assist in disaster relief efforts. The above rules for use and disclosure of PHI for involvement in an individual's Treatment and notification (depending upon whether the individual is present or not) apply as long as they do not interfere with the ability to respond to a disaster relief situation.

F. Authorizations

1. MSU shall maintain an authorization form that complies with HIPAA. A sample authorization is attached as Exhibit D.

G. Extent of the Information That May be Used and Disclosed.

1. The University may disclose only the information specified in a validly executed authorization.

2. In the absence of a validly executed authorization, the University must make reasonable effort to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose. The minimum necessary rule does not apply to the following circumstances:

    a. Disclosures to or requests by a health care provider for Treatment;

    b. Disclosures to the individual or personal legal representative who is the subject of the PHI;

    c. Uses or disclosures required for compliance with electronic transactions;

    d. Disclosures to the DHHS when disclosure of information is required under HIPAA or this Policy for enforcement purposes; and

    e. Uses and disclosures that are required by any other law.

3. Healthcare Component will use reasonable efforts to limit the disclosure of PHI to the minimum necessary to accomplish the intended purpose. A disclosure shall be the minimum necessary for a stated purpose when:

    a. Healthcare Component is making disclosures to a public official where no authorization or consent is required, and the public official represents that the information requested is the minimum necessary;

    b. The information is requested by another health care provider, health plan or health care clearing house covered under HIPAA;

    c. The information is requested by a professional who is a member of MSU's Workforce or a Business Associate for the purpose of providing professional services to Healthcare Component, if the professional represents that the information requested is the minimum necessary for the stated purpose; or

    d. Documentation or representations are made that comply with the uses and disclosures involving research in accordance with HIPAA.

H. Verification Requirement

1. Each member of the Workforce will verify as applicable and in accordance with HIPAA the identity and authority of persons requesting PHI.

2. If the requesting person is a public official or someone acting on his or her behalf, the Healthcare Component may rely upon the following:

a. Agency identification badge, credentials or other proof of status;

b. Government letterhead, if request is made by letter;

c. A written statement of the legal authority (or, if impracticable, an oral statement) under which the information is requested.

d. If a request is made pursuant to a legal process, warrant, subpoena, order, or other legal process, it is presumed to constitute legal authority.

e. For persons acting on behalf of the official, a written statement on government letterhead or other evidence or documentation that establishes that the person is acting under the public official's authority (such as contract for services, memo of understanding).

f. In the event a request for disclosure is provided by a public official, the University's Workforce should forward all such requests to the Office of University Counsel for review and response.

3. Healthcare Component may rely on the exercise of professional judgment as to disclosures pursuant to persons involved in a patient's Treatment or Payment, and in relation to disaster relief as discussed in this Policy. As to disclosures regarding serious threats to health and safety, Healthcare Component shall exercise its judgment in accordance with Exhibit C.

VI. APPOINTMENT OF PRIVACY OFFICER

A. The Provost or his designee shall appoint a Privacy Officer.

B. The Privacy Officer is responsible for:

1. Maintaining the master copy of the Notice of privacy; and

2. In consultation with University Counsel, approving requested changes to the Notice by Healthcare Component.

3. Receiving questions and complaints regarding the Notice;

4. Coordinating the investigation of a Breach and any associated notice related to such Breach;

5. Reviewing and responding to requests for Limited Data Sets;

6. Evaluating Business Associate Agreements; and

7. Receiving notice of a Breach of a Business Associate Agreement, coordinating the investigation of such Breach, and coordinating any associated notice related to such Breach.

C. The Privacy Officer must document compliance with the Notice requirements of this policy by retaining copies of the original and any subsequent revisions of the Notice issued by the Healthcare Component for six years from the date of the creation of the Notice, or the date when it last was in effect, whichever is later.

VII. NOTICE OF PRIVACY

A. A form of Notice of Privacy Practices is attached as Exhibit E to this Policy and must be posted on the webpages for the Healthcare Components within the University's website.

B. Revisions to Notice of Privacy Practices:

1. Healthcare Component must , in accordance with HIPAA, revise and distribute its Notice in accordance with HIPAA whenever there is a material change to the uses or disclosures, the individual's rights, the Healthcare Component's legal duties, or other privacy practices stated in the Notice.

2. Except when required by law, a material change to any term of the Notice may not be implemented prior to the effective date of the Notice in which the change is reflected.

3. Whenever the Notice is revised, Healthcare Component shall make the revised Notice available to patients upon request on or after the effective date of the revision and must post the Notice on their webpage, if any, and in clear and prominent locations within each Healthcare Component.

C. Face-to-Face Provision of the Notice of Privacy Practices:

1. The Notice must be offered to all individuals whenever they enter a Healthcare Component seeking health care services or otherwise receive health care services from MSU.

2. Healthcare Component must provide the Notice to individuals at the first provision of services.

   a. In emergency situations, Healthcare Component must provide the Notice as soon as reasonably practicable after the emergency situation is resolved. At the time the Notice is provided, Workforce members may offer to answer questions regarding the Notice.

3. Except in an emergency situation, upon provision of the Notice, Workforce members must make a good faith attempt to obtain a written acknowledgement of receipt of the Notice signed by the patient and his/her personal representative. If the acknowledgement cannot be obtained, staff must document their efforts to obtain acknowledgement and the reason the acknowledgement was not obtained.

4. If the Notice cannot be provided and/or the acknowledgement is not signed due to an emergency situation, Workforce members must provide the Notice and attempt

to obtain the acknowledgement as soon as reasonably practical after the emergency treatment situation is resolved.

5. A copy of the Notice must be posted in prominent locations at each Healthcare Component.

D. Provision of Notice of Privacy Practices in Special Circumstances:

1. *By Telephone* – In the event the initial delivery of health care services occurs over the telephone, the Notice must be mailed to the patient no later than the next day or be emailed to the patient (see "*By E-Mail,*" below). The clinic must include an acknowledgement and request the patient to sign the acknowledgement and mail or otherwise return it to the Healthcare Component. The clinic must document that the patient was instructed to sign and return the acknowledgement to the clinic. Attached to this Policy as Exhibit F is a sample acknowledgement to be used when mailing the Notice to the patient.

2. *By E-Mail* – If the initial delivery of health care series occurs electronically, the Healthcare Component must automatically provide electronic Notice to the patient. Notice may be sent to the patient by e-mail if the patient agrees to receive the Notice electronically and such agreement has not been withdrawn. When the Notice is sent by e-mail, the Healthcare Component must include a standard message asking the recipient to return an e-mail acknowledgement that he or she has received the Notice.

a. If the Healthcare Component's staff knows that the e-mail transmission failed, a paper copy of the Notice must be given to the patient upon first delivery of service.

b. Any patient who is a recipient of an electronic Notice retains the right to obtain a paper copy of the Notice upon request.

E. Dissemination of Notice

1. Workforce members in the Healthcare Component are responsible for providing the Notice to patients, answering questions, and collecting the acknowledgement.

2. The Healthcare Component is responsible for maintaining copies of written acknowledgements of receipt of the Notice or documentation of good faith efforts to obtain such written acknowledgement for six years from the date of creation.

VIII. ACCESS BY INDIVIDUALS TO PHI

Healthcare Component must provide an individual with the right of access to inspect and obtain a copy of PHI pertaining to the individual in a designated record set as long as the record is maintained. Individuals shall make requests for such access in writing.

A. Requirements:

1. Healthcare Component shall provide individuals an opportunity inspect and copy their PHI, unless an exception applies, including but not limited to:

    a. psychotherapy notes; and

    b. information complied in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding

2. Healthcare Component may deny an individual access if the individual has given a right to have such denial reviewed by the Privacy Officer and the following circumstances are present:

    a. The access requested is reasonably likely to endanger the life or physical safety of the individual or another person.

    b. The PHI makes reference to another person and the access requested is reasonably likely to cause substantial harm to such other person.

    c. The request for access is made by the individual's personal representative and access is reasonably likely to cause substantial harm to the individual or another person.

B. Responsibilities:

1. If an individual has been denied access to records and has requested a review of a denial, the Healthcare Component in possession of the records shall, in accordance with HIPAA, designate, and refer the request to the Privacy Officer to review the decision to deny access. The Privacy Officer, within a reasonable period of time but not to exceed 90 days, must determine whether or not to deny access based on the standards put forth in this Policy. Privacy Officer shall, in accordance with HIPAA, provide written notice to the requesting individual of the determination and take other actions as required to carry out the determination.

2. Healthcare Component must act on requests to access PHI within thirty (30) days after receipt of a request. If the request is for PHI not maintained or accessible to the Healthcare Component, the Healthcare Component may take action by no later than sixty (60) days from the receipt of such a request. However, the Healthcare Component must provide a written statement of the reasons for the delay and the date by which it will complete its action on the request. No other time extensions will be granted in excess of sixty (60) days.

3. If the Healthcare Component grants the request to access the PHI, in whole or in part, it shall inform the individual of the acceptance of the request and:

    a. Provide the access requested.

        Healthcare Component must allow inspection or provide a copy or both, of the PHI in designated record sets. If the same PHI that is the subject of a

request for access is maintained in more than one designated record set or at more than one location, Healthcare Component shall only produce the PHI once in response to a request for access.

b. Provide access in the form requested.

i. Healthcare Component shall provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format; or in a readable hard copy form or such other form or format as agreed to by Healthcare Component and the individual.

ii. Notwithstanding the preceding paragraph, if the PHI that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the Healthcare Component must provide the individual with access to the PHI in the electronic form and format requested by the individual if it is readily producible in such form and format; or, if not, in a readable electronic form and format, then as agreed to by the Healthcare Component and individual.

iii. Healthcare Component may provide the individual with a summary of the PHI requested, instead of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided, if: (x) The individual agrees in advance to such a summary or explanation; and (y) The individual agrees in advance to the fees imposed, if any, by the Healthcare Component for such summary or explanation.

c. Manner of Access

i. Healthcare Component must provide access, by arranging with the individual a convenient time and place, to inspect or obtain a copy of the PHI; or mail a copy of the PHI at the individual's request. Healthcare Component may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

ii. If an individual's request for access directs the Healthcare Component to transmit the copy of PHI directly to another person designated by the individual, the Healthcare Component must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual and clearly identify the designated person and where to send the copy of PHI.

iii. If the individual requests a copy of the PHI or agrees to a summary or explanation of information, Healthcare Component may impose a reasonable cost-based fee, provided that the fee includes only the cost of: (a) labor for copying the PHI requested whether in paper or electronic form; (b) supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media; (c) postage, when the individual has requested the copy or explanation be mailed; and (d) preparing an explanation or summary of the PHI, if agreed to by the individual as required by HIPAA.

d. If Healthcare Component denies the request to access the PHI, in whole or in part, it must provide the individual with a timely written denial. The denial must be in plain language and contain:

i. The basis for the denial.

ii. A statement of the individual's review rights, including a description of how the individual may exercise such review rights.

iii. A description of how the individual may complain to Privacy Officer or the Department of Health and Human Services (DHHS), pursuant to this Policy's procedures. The description must include the name, or title, and telephone number of the contact person or office.

e. If Healthcare Component does not maintain the PHI that is the subject of the individual's request for access, and Healthcare Component knows where the requested information is maintained, Healthcare Component must inform the individual where to direct the request for access.

f. Healthcare Component must document and retain the following information:

i. The designated record sets that are subject to access by individuals.

ii. The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

g. All requests made for access to PHI must be made to the individual designated by the Healthcare Component to receive such requests.

IX. REQUESTS FOR RESTRICTION OF USE AND DISCLOSURE OF PHI

A. Requirements:

1. Individuals shall be permitted to request that Healthcare Component restrict:

a. uses and disclosures of PHI to carry out TPO; and

b. disclosures related to involvement in Treatment.

2. Healthcare Component may, however, deny the request.

3. All requests for restrictions and termination of the agreement to restrict must be in writing.

4. All requests made for restrictions to PHI must be made to the individual designated by the Healthcare Component within the Health Care Component to receive such requests.

B. Responsibilities:

1. A Healthcare Component must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of PHI from the Healthcare Component by alternative means or at alternative locations. Healthcare Component must review all requests that are made by individuals to restrict use and disclosure of the individuals PHI; however, it shall not be required to agree to the restrictions requested if it determines that the restrictions would interfere with Treatment, Payment or Health Care Operations. If restricted PHI is disclosed to a health care provider for emergency treatment, the Healthcare Component must request that such health care provider not further use or disclose the information.

2. If Healthcare Component agrees to an individual's restriction request, the restriction must be appropriately documented and such documentation be retained by the Healthcare Component. Also, the restriction must be communicated in a manner as to assure that anyone accessing the information becomes aware of the restriction.

3. If the Healthcare Component agrees to an individual's restriction request, it is not permitted to use or disclose the specified PHI in any manner that would not violate that restriction, except in the event that the individual is in need for emergency Treatment and the restricted PHI is needed to provide such Treatment. In this case, Healthcare Component may use the restricted PHI or disclose the PHI to a Healthcare Provider to provide such Treatment to the individual. In this event, Healthcare Component must request that such provider not further use or disclose the information.

4. Healthcare Component may terminate a restriction if:

a. the individual agrees to or requested the termination in writing;

b. the individual orally agrees to the termination and the oral agreement is documented; or

c. Healthcare Component informs the individual that it is terminating its agreement to restriction.

5. In the event that Healthcare Component, for any of the above mentioned reasons, terminates the agreement for restriction, the termination is only effective with respect to PHI created or received after it has so informed the individual.

X. REQUESTS FOR AMENDMENT OF PHI

A. Healthcare Component shall maintain a process to enable its patients to request an amendment of their Individual Health Information held by the Healthcare Component by designating a person within the Healthcare Component to receive such requests. Such requests must be made in writing and include a reason supporting the amendment.

1. An individual may request the Healthcare Component amend his or her Individual Health Information. Individuals shall make such requests in writing and provide a reason to support the amendment. The Health Healthcare Component shall provide all individuals Notice of the University's Privacy Practices prior to Treatment.

2. The Healthcare Component may deny the request to amend if the Individual Health Information that is the subject of the request meets the following conditions:

a. It was not created by the Healthcare Component, unless the originator is no longer available to act on the request.

b. It is not part of the individual's Designated Health Record.

c. It would not be accessible to the individual pursuant to this Policy's section entitled Access of Individual's Protected Health Information.

d. It is accurate and complete.

3. Healthcare Component must act on the individual's request for amendment no later than sixty (60) days after receipt of the request for an amendment. Healthcare Component may extend the time to respond no more than thirty (30) days provided the Healthcare Component gives the individual a written statement of the reason for the delay, and the date by which the amendment will be processed.

4. If the request is granted, Healthcare Component shall:

a. Insert the amendment or provide a link to the amendment at the site of the information that is the subject of the request for amendment.

b. Inform the individual that the amendment is accepted.

Healthcare Component

c. Within a reasonable time frame, make reasonable efforts to provide the amendment to persons identified by the individual, and persons, including business associates, that the Healthcare Component knows have the PHI that is the subject of the amendment and that may have relied on or could foreseeably rely on the information to the detriment of the individual.

5. If the Healthcare Component denies the request for amendment, it must provide the individual with a timely, written denial in plain language that states:

   a. The basis for the denial.

   b. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement.

   c. A statement that if the individual does not submit a statement of disagreement, the individual may request the Healthcare Component to provide the individual's request for amendment and the denial with any future disclosures of PHI.

   d. A description of how the individual may complain to the Privacy Officer designated by the Healthcare Component or to the Secretary of DHHS.

6. The individual requesting the amendment shall submit to the Healthcare Component a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The University may reasonably limit the length of a statement of disagreement.

7. Healthcare Component may submit a rebuttal to the individual's statement of disagreement, and provide a copy to the individual who submitted the statement of disagreement.

8. Healthcare Component shall, as appropriate, identify the record of PHI that is the subject of the disputed amendment, append the individual's request for an amendment, the denial of the request, the individual's statement of disagreement, if any, and the rebuttal, if any.

9. If the individual has not submitted a written statement of disagreement, Healthcare Component must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of PHI only if the individual has requested such action.

10. When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included, Healthcare Component may separately transmit the material required.

11. Healthcare Component that is informed by another Healthcare Component of an amendment to an individual's PHI must amend the PHI in written or electronic form.

12. Healthcare Component shall document the titles of the positions responsible to receive and process requests for amendments.

XI. BREACH NOTIFICATION

A. **General**. Healthcare Component will presume that any acquisition, access, use, or disclosure of Unsecured PHI in a manner not permitted under the HIPAA Privacy Rule is a Breach that requires notification to affected individuals or to their personal representatives, unless an exception applies or Healthcare Component demonstrates that there is a low probability that the Unsecured PHI has been compromised, based on a risk assessment (described below). Upon Discovery of a Breach, Healthcare Component may, at its discretion, either (1) automatically notify affected individuals or their personal representatives of the Breach without conducting a risk assessment, or (2) first conduct a risk assessment to determine if such notification is necessary. All Business Associates of Healthcare Component are required to report any Breach to Healthcare Component without unreasonable delay upon discovery and in no case later than 60 calendar days after discovery.

1. If Healthcare Component discovers a potential Breach of Unsecured PHI and chooses to provide automatic notification or conducts a risk assessment and determines there is more than a low probability that the Unsecured PHI has been compromised, Healthcare Component must notify affected individuals or their personal representatives of the Breach without unreasonable delay and in no case later than 60 days of Discovery of a Breach. A Breach is considered discovered as of the first day on which the Breach is known by any workforce member or agent of Healthcare Component, or, in the exercise of reasonable diligence, would have been known to any person, other than the person committing the Breach, who is a workforce member or agent of Healthcare Component.

B. **Internal Reporting**. Any member of the Healthcare Component workforce must promptly notify his or her supervisor(s) and/or the Healthcare Component of any unauthorized access, use, or disclosure of Unsecured PHI, provide relevant facts regarding the unauthorized incident, and cooperate with any subsequent investigation.

1. **Incident Response**. The Privacy Officer will work with the appropriate Healthcare Component officials and University Counsel, as necessary, to determine an appropriate and timely response to the incident.

2. **Workforce Training**. All appropriate members of the Healthcare Component workforce will be trained how to identify and report potential Breaches and will be trained on any other applicable policies and procedures

related to PHI that are appropriate with respect to the member's job function. Appropriate sanctions, up to and including termination, will be applied against members of the workforce who fail to comply with this policy.

C. **Investigation**. The Privacy Officer will work with the appropriate workforce members, Healthcare Component officials, and University Counsel, as necessary, to uncover the facts and circumstances related to the incident. The investigative actions may include, but will not be limited to, conducting employee interviews, system audits, and site observation. Upon completion of the investigation, if Healthcare Component determines that the incident is an impermissible acquisition, access, use, or disclosure of Unsecured PHI, Healthcare Component will presume the incident is a Breach and will:

1. **Notify/Assess**. Automatically provide notification as set forth below upon conferring with Healthcare Component officials and University Counsel, as necessary, to determine the financial and reputational costs to Healthcare Component; **or** conduct a risk assessment, as set forth below, to determine if there is a low probability that the Unsecured PHI has been compromised. Healthcare Component is not required to provide notification if it demonstrates a low probability of compromise upon completion of the risk assessment.

2. **Mitigate Harm**. Mitigate, to the extent practicable, any harmful effects of the Breach that are known.

3. **Delay if Required by Law Enforcement**. Healthcare Component will delay notification if a law enforcement official states that such notification would impede a criminal investigation or would cause damage to national security. Healthcare Component will delay the notification as specified in a written statement from law enforcement or, if no written statement is provided, for not more than 30 days from the date Healthcare Component is in receipt of oral notification from law enforcement. Healthcare Component will document any such oral communication in writing.

D. **Risk Assessment**. If Healthcare Component chooses not to provide automatic notification upon Discovery of a Breach, then it must conduct a risk assessment of any acquisition, access, use, or disclosure of Unsecured PHI in a manner not permitted by the HIPAA Privacy Rule to determine whether there is a low probability that the impermissible acquisition, access, use, or disclosure compromised the security or privacy of the Unsecured PHI. The risk assessment will take into account the factors listed below to determine whether there is a low probability that Unsecured PHI has been compromised. The factors indicated below do not necessarily constitute an exhaustive list of items that Healthcare Component will consider to determine if there exists a low probability of compromise of Unsecured PHI. Circumstances involving a Breach will be analyzed on a case-by-

case basis and may require consideration of factors in addition to those included in the following:

1. **Nature of the Data Elements Breached**. Healthcare Component will analyze the nature of the data elements compromised in the impermissible acquisition, access, use, or disclosure. The nature of the data elements involved is a key factor to consider in determining if a Breach has occurred that requires notification. It is difficult to characterize data elements as creating a low, moderate, or high risk simply on the basis of the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive than in another context. In assessing the levels of risk and harm, Healthcare Component will consider the data element(s) in light of their contexts, including the types of identifiers in the data element(s), the likelihood of re-identification of the information, and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

2. **The Unauthorized Person Who Used the Unsecured PHI or to Whom the Disclosure Was Made**. Healthcare Component will consider who impermissibly used the Unsecured PHI or to whom a disclosure was made. If the person in receipt of the Unsecured PHI has an obligation to protect PHI (e.g., another covered entity governed by HIPAA), that fact will weigh in favor of a finding of low probability that the Unsecured PHI is compromised.

3. **Likelihood the Unsecured PHI Was Actually Acquired or Viewed**. Healthcare Component will assess the likelihood that Unsecured PHI will be or had been acquired or used by unauthorized individuals. The fact that Unsecured PHI is lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals. The number of physical, technical, and procedural safeguards utilized by Healthcare Component impact the risk that the information is accessible or useable.

4. **Extent to Which the Risk to the Unsecured PHI Has Been Mitigated**. The probability that Unsecured PHI has been compromised may depend, in part, upon whether, and to what extent, Healthcare Component has mitigated the effects of an impermissible use or disclosure. Appropriate countermeasures, such as monitoring of systems for use of personal information and patterns of suspicious behavior, will be taken by Healthcare Component. In assessing risk, Healthcare Component will consider, among other factors, whether the Unsecured PHI has been returned, remotely wiped, or destroyed, and whether the unauthorized recipient of the Unsecured PHI has provided satisfactory assurances that the Unsecured PHI will not be further used or disclosed.

5. The burden to determine whether there is a low probability that Unsecured PHI has been compromised belongs to Healthcare Component. In order to

make this determination, Healthcare Component will document each impermissible acquisition, access, use, and disclosure and the risk assessment outlined above will be conducted for each, except in the event that Healthcare Component elects to provide automatic notification. The Privacy Officer will be responsible for conducting the risk assessment, documenting the results of the assessment, and determining whether there exists a low probability that the Unsecured PHI has been compromised.

E. **Notification**

1. Individual Notification

a. If Healthcare Component elects to provide automatic notification, or if the risk assessment determines that a Breach has occurred and more than a low probability that the Unsecured PHI has been compromised exists, then without unreasonable delay and in no case later than 60 days from the Discovery of a Breach, Healthcare Component will provide written notice to the affected individual or:

i. If the individual is deceased, to the next of kin or personal representative.

ii. If the individual is incapacitated/incompetent, to the personal representative.

iii. If the individual is a minor, to the parent or guardian.

b. Written notification will be in plain language.

c. Written notification will be sent to the last known address of the affected individual or next of kin by first-class mail, or if specified by the affected individual, by encrypted electronic mail.

d. Written notification will contain the following information:

i. A brief description of what occurred with respect to the Breach, including, to the extent known, the date of the Breach and the date on which the Breach was discovered;

ii. A description of the types of Unsecured PHI that were disclosed during the Breach;

iii. A description of the steps the affected individual should take in order to protect himself or herself from potential harm caused by the Breach;

iv. A description of what Healthcare Component is doing to investigate and mitigate the Breach and to prevent future Breaches; and

v. Instructions for the individual to contact Healthcare Component.

e. In the case where there is insufficient or out-of-date contact information:

i. For less than ten (10) individuals, a substitute form of notice shall be provided, such as a telephone call.

ii. In the case that there are ten (10) or more individuals for which there is insufficient or out-of-date contact information and contact information is not obtained, Healthcare Component will:

(a) Post a conspicuous notice for 90 days on the homepage of its website that includes a toll-free number; or

(b) Provide notice in major print or broadcast media in the geographic area where an affected individual can learn whether or not his or her Unsecured PHI is possibly included in the Breach. A toll-free number will be included in the notice.

f. If Healthcare Component determines that the affected individual should be notified urgently of a Breach because of possible imminent misuse of Unsecured PHI, Healthcare Component may, in addition to providing notice as outlined above, contact the affected individual by telephone or other means, as appropriate.

2. **Media Notification**

a. In the case where a single Breach event affects more than 500 residents of a state or jurisdiction, notice shall be provided to prominent media outlets serving that state or jurisdiction. Healthcare Component will make any such media contact pursuant to its media communications policies and procedures.

3. **HHS Notification**

a. Notice will be provided by Healthcare Component without unreasonable delay, and in no case later than 60 days from the Discovery of a Breach, to the Secretary of the Department of Health

and Human Services (HHS) in the manner specified on the HHS website if a single Breach event affects 500 or more individuals.

b. If a Breach affects fewer than 500 individuals, Healthcare Component will maintain a log of the Breach occurrences in any given calendar year and annually will submit the log to HHS in the manner specified on the HHS website no later than 60 days after the end of the calendar year.

4. **Maintenance of Breach Information/Log**. The investigation, report and notice of Breach shall be retained in accordance with this Policy's record retention requirements.

5. **Business Associate Responsibilities**. The Business Associate of the Healthcare Component that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHI shall, without unreasonable delay and in no case later than 10 calendar days after discovery of a Breach, notify the Healthcare Component of such Breach. Such notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during such Breach. The Business Associate shall provide the Healthcare Component with any other available information that is required to include in Breach Notification to the individual or, in accordance with HIPAA, thereafter as information becomes available. Upon notification by the Business Associate of discovery of a Breach, the Healthcare Component will be responsible for Breach Notification to affected individuals.

6. **Workforce Training**. The University shall train all members of its Workforce of the Healthcare Component upon hiring and periodically thereafter on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities Workforce members shall also be trained as to how to identify and report Breaches within the University.

a. The University will apply appropriate sanctions against any member of the Workforce who fails to comply with the University's HIPAA Policy.

b. The Department Chairs, Deans, Vice Presidents, Provost and President of the University, with the assistance of the Vice President for Human Resources or its designee, will enforce sanctions against members of the Workforce in accordance with applicable University's policies, and applicable collective bargaining agreements as set forth by the University's Division of Human Resources including but not limited to those set forth at http://www.montclair.edu/human-resources/policies-and-procedures/.

c. The Division of Human Resources will document all sanctions that are applied.

d. **Retaliation**. No employee within the University may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right granted by this Policy. The University may not require individuals to waive their privacy rights as a condition of the provision of Treatment, Payment, enrollment in a health plan, or eligibility for benefits.

XII. ACCOUNTING DISCLOSURES OF PHI

A. Requirements

1. Healthcare Component must provide an individual with an accounting of disclosures in accordance with HIPAA.

2. Healthcare Component must act on an individual's request for an accounting within sixty (60) days of receipt of the request. If a Healthcare Component is unable to provide the accounting within sixty (60) days, it may extend the time period to provide the accounting by no more than thirty (30) days; however, within the original sixty (60) days, the Healthcare Component must provide the individual with a written statement of the reasons for the delay and the date by which Healthcare Component will provide the accounting. Only one extension is permitted per request.

3. The first accounting in a twelve-month period to an individual must be provided without charge. However, Healthcare Component may impose a reasonable cost-based fee for each subsequent request for an accounting made by the same individual within the twelve-month period provided the Healthcare Component informs the individual of the fee prior to complying with the request, thus giving the individual the opportunity to withdraw or modify the request.

4. As part of the accounting of the disclosures, Healthcare Component will coordinate the release of PHI with Business Associates.

5. Healthcare Component must temporarily suspend an individual's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official, for the time specified by such agency or official, if such agency or official provides the Healthcare Component with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and it must include the time frame for which such a suspension is required.

6. Healthcare Component must temporarily suspend an individual's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official, for the time specified by such agency or official, if such agency or official provides the Healthcare Component with an oral statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and it must include the time frame for which such a suspension

is required. However, in as much as the statement was given orally, Healthcare Component must:

a. Document the statement, including the identity of the agency or official making the statement;

b. Limit the temporary suspension to no longer than thirty (30) days from the date of the oral statement, unless a written statement is submitted during that time.

7. Requests made for accountings of disclosures of PHI must be made to the individual designated by the Healthcare Component to receive such requests.

B. Responsibilities:

1. An accounting must cover a period of six (6) years, unless a shorter period is requested.

2. The accounting for each disclosure must include:

a. The date of the disclosure;

b. The name and address of the entity or person who received the PHI;

c. A brief description of the PHI disclosed; and

d. A brief statement to reasonably inform the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for the disclosure (i.e. subpoena).

3. If a Healthcare Component has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting with respect to such multiple disclosures should provide:

a. The information required for the first disclosure during the accounting period;

b. The frequency or number of the disclosures made during the accounting period; and

c. The date of the last disclosure during the accounting period.

4. If, during the period covered by the accounting, the Healthcare Component made disclosures of PHI for a particular research purpose in connection with the provision of Treatment in accordance with HIPAA for fifty (50) or more individuals, the accounting may provide:

a. The name of the protocol or other research activity;

b. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

c. A brief description of the type of PHI that was disclosed;

d. The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

e. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

f. A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

g. If the Healthcare Component provides an accounting for research disclosures in accordance with this section and it is reasonably likely that the PHI of the individual was disclosed for such research protocol or activity, the Healthcare Component must, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

XIII. DOCUMENT RETENTION, DESTRUCTION AND DISPOSAL

A. The Healthcare Component must document and retain all records in accordance with the State of New Jersey's record retention policy. In addition, the following documents shall be retained pursuant to HIPAA for no less than six (6) years:

1. The designation of Healthcare Components, as set forth in Exhibit A, following any decision to terminate any division or department from the University's Health Care Components. Designations that remain a Health Care Component of the University should be retained permanently.

2. The Notice of Privacy and any subsequent revisions to the Notice from the date of the creation of the Notice, or the date when it last was in effect, whichever is later.

3. The information required to be included in an accounting pursuant to this Policy and HIPAA;

4. The written accounting itself that was given to the requesting individual;

5. The title of positions or offices responsible for receiving and processing requests for an accounting.

6. Records concerning a Breach and notice of Breach, including:

a. A description of what happened, the date of the Breach, date of the discovery of the Breach, and the number of patients affected, if known.

b. A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security Number, date of birth, home address, account number, etc.).

c. A description of the action taken with regard to notify individuals of the Breach.

d. Resolution of the Breach and steps taken to mitigate the Breach and prevent future occurrences.

7. PHI

B. Records to be maintained under HIPAA will be disposed of properly, in accordance with HIPAA, New Jersey law and the State's record retention requirements.

1. Until such time as destruction or disposal of PHI is permissible, all PHI will be secured against unauthorized or inappropriate access.

2. If utilizing an outside agency for destruction of disposal of PHI, a contract and a Business Associate agreement must be executed between the University and the outside agency. The contract must provide that upon termination, the agency will return or destroy and dispose of all PHI, and provide proof of destruction and disposal and the methodology by which the material was destroyed.

XIV. LIMITED DATA SETS

A. The Privacy Officer may permit the use of PHI to create a Limited Data Set. A Limited Data Set is PHI that excludes certain direct identifiers of the patient, or of the patient's relatives, employers or household members.

1. Limited Data Sets may be used or disclosed only:

a. For the purposes of research, public health, and/or health care operations.

b. To or by a Business Associate for purposes of creating a Limited Data Set for the Healthcare Component or the Business Associate.

2. The Privacy Officer will define methods for creating the Limited Data Set.

B. Processing Requests for Limited Data Sets:

1. Requests for Limited Data Sets must be submitted in writing to the Privacy Officer.

2. A request for a Limited Data Set must include the following:

a. Requestor's name, address, telephone numbers, title, organization or department;

b. Date of request;

c. Purpose of the request (e.g., research, public health or health care operations), including the intended uses, any re-disclosures, and who will use or have access to the Limited Data Set;

d. Names of all recipients of the Limited Data Set;

e. Record parameters or selection criteria – time period included, minimum number of patient records, type of patient records (such as by diagnosis, procedure, drug use, or other criteria); and

f. Date the Limited Data Set is needed.

3. The requestor of a Limited Data Set shall be responsible for submitting payment to the Privacy Officer as reimbursement for the Healthcare Component's resource expenditures related to the request for the Limited Data Set.

4. Request for Limited Data Sets may be denied if:

a. The Healthcare Component cannot create the Limited Data Set;

b. The recipient refuses to compensate the Healthcare Component for generating the Limited Data Set; or

c. Creating the Limited Data Set is an imposition to the operations of the Healthcare Component.

5. The Limited Data Set Request must be reviewed, approved or denied by the Privacy Officer.

6. In the event the request is approved, the requestor will be asked to confirm acceptance of and submit payment for the production costs prior to actual creation of the Limited Data Set. Prior to releasing the Limited Data Set to recipient, Privacy Officer shall require the recipient to execute a written agreement defining the recipient's obligations concerning the Limited Data Set.

XV. BUSINESS ASSOCIATES

A. Business Associates that provide functions, activities, or services for or to Healthcare Component involving use and disclosure of PHI in order to assist Healthcare Component with carrying out Health Care Functions, other than for Treatment, must enter into a Business Associate contract with MSU prior to providing access to such information.

B. Identification of Business Associates:

1. Prior to contracting with any third party, whether an individual or an entity, it is the responsibility of the Healthcare Component to contact the Privacy Officer or his/her designee to determine whether the outside entity or person qualifies as a Business Associate.

2. If a determination is made that the third party is a Business Associate, the Healthcare Component should inquire if the third party will execute a Business Associate Agreement with the University in the form attached as Exhibit H. The Healthcare Component will be responsible for coordinating the execution of Business Associate Agreements. Any changes to the University's form of Business Associate Agreement shall be reviewed and approved by University Counsel.

3. If a Business Associate Agreement is required, the Business Associate Agreement must be signed by both parties before the Business Associate performs any services that involve the use and/or disclosure of PHI.

4. The Privacy Officer should periodically reevaluate the list of Business Associates to determine who has access to PHI in order to assess whether the list is complete and current.

5. The Healthcare Component shall identify systems covered by the Business Associate Agreement.

6. If a third party provides services requiring the use or disclosure of PHI and meets the definition of a Business Associate, and the third party has no known written Business Associate Agreement, Workforce shall notify the Privacy Officer of the need for a Business Associate Agreement. Failure by the using department to assist in obtaining a Business Associate Agreement, where appropriate, may result in disciplinary action.

C. Breach of a Business Associate Agreement:

1. Workforce shall contact the Privacy Officer if a Business Associate has violated a term or obligation of the Business Associate Agreement or any HIPAA requirement(s).

2. If Healthcare Component becomes aware of a violation, Healthcare Component shall notify the Business Associate and the parties will act to mitigate the Breach to the extent practicable. If mitigation is not possible, the Healthcare Component may terminate the Business Associate Agreement and the underlying business arrangements with such vendor that require vendor to use or disclosure PHI, and/or the Privacy Officer will notify the Secretary of HHS.

EXHIBIT A
HEALTH CARE COMPONENT DESIGNATION

Montclair State University is a public higher education institution created by the laws of New Jersey and is governed by its Board of Trustees. The University provides a comprehensive array of bachelor's, masters and doctoral degree programs to more than 19,000 undergraduate and graduate students, which are distributed among its College of Humanities and Social Sciences, College of Education and Human Services, College of Science and Mathematics, School of Business, and College of the Arts. The University is a hybrid entity as defined by HIPAA because a portion of its programs perform covered functions as defined by HIPAA.

In accordance with HIPAA, the following programs are designated as Health Care Components of Montclair State University:

- Montclair State University Center for Audiology and Speech Language Pathology (Audiology Clinic)
- Center for Autism and Early Childhood Mental Health
- Jeffrey Dworkin Early Intervention Program
- University Health Center

Any other University department, division, and program that is not explicitly designated by the University herein as a Health Care Component is not a Healthcare Component under HIPAA.

EXHIBIT B
LIST OF IDENTIFIERS AND DE-IDENTIFICATION PROCESS

A. The University may use PHI where the information that can identify the individual is not present and where there is no reasonable basis to believe that information can be used to identify the individual. The University can create de-identified information by removing or otherwise concealing the following information regarding the individual, relatives, employers, or household members:

1. Names
2. Street address, city, county, precinct, zip code, and equivalent geocodes
3. All elements of dates (except year) for dates directly related to the 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 90 or older
4. Birth date
5. Telephone numbers
6. Fax numbers
7. Electronic mail addresses
8. Social security number
9. Medical record number
10. Health plan beneficiary number
11. Account numbers
12. Certificate/license number
13. Any vehicle identifiers and serial numbers, including license plate numbers
14. Web Universal Resource Locator
15. Internet Protocol address number
16. Finger or voice prints; biometric identifiers
17. Full face Photographic images; and any comparable images
18. Any other unique identifying number, characteristic, or code that has reason to believe may be identifiable to an anticipated recipient of the information.

EXHIBIT C
DISCLOSURE OF PHI
NO AUTHORIZATION REQUIRED

1. Public Health Activities	Healthcare Components may disclose PHI as follows: 1. To a public health authority that is authorized by law: a. To collect or receive such information for the purpose of preventing or controlling disease, injury or disability; b. To receive reports of child abuse or neglect; 2. To persons subject to the jurisdiction of the Food and Drug Administration with respect to an FDA regulated product or activity for which that person has responsibility for the purpose of activities related to the quality, safety or effectiveness of same. Such purposes include: a. To collect or report adverse events, product defects or problems, or biological product deviations; b. To track FDA regulated products; c. To enable product recalls, repairs, or replacement or lookback; or d. To conduct post-marketing surveillance. 3. To a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition if Healthcare Component is authorized by law to notify the person as necessary in the conduct of public health intervention or investigation; or 4. To an employer about an individual who is a member of the Workforce of the employer if: a. Healthcare Component is a covered healthcare provider who provides health care to the individual at the request of the employer to conduct medical surveillance of the workplace or to evaluate individuals for work-related illness or injury; b. The PHI consists of findings concerning work-related illness or injury or workplace related medical surveillance; c. The employer needs the findings to comply with its obligations under federal or state law, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; or d. The healthcare provider gives written notice to the individual that PHI relating to the medical surveillance of the workplace and workplace related illnesses and injuries is disclosed to the employer by giving a copy of the notice to the individual when the health care is provided or if the healthcare is provided on the worksite of the employer, by posting the notice prominently where the health care is provided. 5. A school, about an individual who is a student or prospective student of the school if: a. The PHI that is disclosed is limited to proof of immunization;

	b. The school is required by State or other law to have such proof of immunization prior to admitting the individual; and c. The Healthcare Component obtains and documents the agreement to the disclosure from either: (i) a parent, guardian or other person acting for a minor; and (ii) the individual if an adult or emancipated minor.
2. Victims of Abuse, Neglect, or Domestic Violence	Except for reports of child abuse or neglect permitted by Section 1 above, Healthcare Component may disclose PHI to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect or domestic violence. Such disclosures involving adults are permitted if: a. The disclosure is required by law and the disclosure is limited to the requirements of such law and: (i) Healthcare Component, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims, or (ii) if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents the PHI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure. b. The individual has been informed about the disclosure unless: (i) the Healthcare Component believes informing the individual would palce the individual at risk of serious harm; or (ii) the Healthcare Component would be informing a personal representative that the Healthcare Component believes is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interest of the individual.
3. Health oversight activities	Healthcare Component may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for the appropriate oversight of: a. the health care system, b. government benefit programs for which health information is relevant to beneficiary eligibility, c. entities subject to government regulatory programs that need health information to determine compliance with program standards, or entities subject to civil rights law that need health information to determine compliance. d. entities subject to civil rights law for which health information is necessary for determining compliance. Healthcare Components may not disclose PHI under this section if an investigation or other activity relates to an individual but does not arise out of and is not directly related to: a. the receipt of health care; b. a claim for public benefits related to health; or c. qualifications for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

4. Judicial and administrative proceedings	All requests for PHI in connection with judicial and administrative proceedings shall be referred to the Office of University Counsel. University Counsel will review the request and respond to the issuer of the request.
5. Law enforcement purposes	Healthcare Components may disclose PHI: 1. As required by law including laws that require the reporting of certain types of wounds or other physical injuries. 2. In compliance with and as limited by the relevant requirements of: a. A court order, warrant, subpoena, or summons issued by a judicial officer; b. A grand jury subpoena; or c. An administrative request, including an administrative subpoena or summons, a civil investigative demand, or similar process authorized under law, provided that: 2. The information sought is relevant and material to a legitimate law enforcement inquiry; 3. The request is as specific and narrowly drawn as is reasonably practicable in light of the purpose for which the information is sought; and 4. De-identified information could not reasonably be used. 5. For the purpose of identifying a suspect, fugitive, material witness, or missing person, Healthcare Component may disclose only the following information: a. Name and Address b. Date and Place of Birth c. Social security number d. ABO blood type and rh factor e. Type of injury f. Date and time of treatment. g. Date and time of death, if applicable, and h. A description of distinguishing physical characteristics like height, weight, gender, race, hair, eye color, facial hair, scars, tattoos. 6. If the disclosure is of the PHI of an individual who is suspected to be a victim of a crime, abuse, or other harm, Healthcare Component may disclose PHI if: a. such information is needed to determine whether a violation of law by a person other than the victim has occurred; and b. immediate law enforcement activity that depends upon obtaining such information would be materially and adversely affected by waiting until the individual is able to agree to the disclosure and c. The disclosure is in the best interest of the individual as determined by the Healthcare Component in the exercise of professional judgment. 7. For purposes of alerting law enforcement of the death of an individual if the covered entity has a suspicion that such death may have resulted from criminal conduct. 8. To alert law enforcement to: a. The commission and nature of a crime

	b. The location of such crime or of the victims of such crime, and c. The identity, description and location of the perpetrator of such crime. 9. If a medical emergency is the result of abuse, neglect or domestic violence of the individual in need of emergency care.
6. Deceased Individuals	The PHI of a deceased individual may be disclosed: a. To a coroner or medical examiner for the purpose of identifying the deceased, determining cause of death, or other duties as authorized by law. b. To funeral directors to carry out their duties; c. To facilitate an organ donation.
7. Research Purposes	1. Healthcare Components may use or disclose PHI for research, regardless of the source of funding of the research, provided that: a. Healthcare Component has obtained a written waiver, in whole or in part, of authorization for use or disclosure of PHI that has been approved by the IRB; and b. The researcher represents that: i. The use or disclosure of PHI is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research; ii. No PHI is to be removed from the Healthcare Component by the researcher in the course of the review; and iii. The PHI for which use or access is sought is necessary for the research. 2. If the research involves a decedent's PHI, the Healthcare Component must obtain from the researcher: a. Representation that the use or disclosure sought is solely for research on the PHI of decedents; b. Documentation of the death of such individual; and c. Representation that the PHI for which the use or disclosure is sought is necessary for research purposes. 3. IRB shall issue a statement identifying the date on which the waiver of authorization was approved. IRB's statement shall include a determination that the waiver of authorization satisfies the following: a. The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals based on at least the presence of the following: i. An adequate plan to protect the identifies from improper use and disclosure ii. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and iii. Adequate written assurance that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study or for other research for which the use or disclosure of PHI would be permitted by HIPAA. iv. The research could not practicably be conducted with the waiver or alteration; and v. The research could not practicably be conducted without access to and use of the PHI. b. A brief description of the PHI for which use or access has been determined to be necessary for the IRB.

	c. The alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures as required by law. d. Approval is indicated by signature of the chair or other member as designated by the chair of the IRB.
8. Emergency Circumstances to Avert Threats to Safety	1. Healthcare Components may, consistent with applicable law and standards of ethical conduct and based on a reasonable belief that the use or disclosure is: a. necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual and is to a person reasonably able to prevent or less the threat, including target of the threat; or b. necessary for law enforcement to identify or apprehend an individual based upon a statement by an individual admitting participation in a violent crime that the Healthcare Component reasonably believes may have caused serious physical harm to the victim or where it appears from the circumstances that the individual has escaped from a correctional institution or from lawful custody. 2. Disclosure of PHI may not be made if learned by Healthcare Component: a. In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure; or b. Through a request by the individual to initiate or to be referred for treatment, counseling or therapy. 3. Specific information that may be disclosed is limited by HIPAA.
9. Specialized Government Functions	Disclosure of PHI may be made in connection with military and veteran activities, national security and intelligence activities, protective services for the President and others, medical suitability for the U.S. Department of State, to obtain security clearance, and correctional institutions and other law enforcement custodial situations, and to government programs providing benefits. In the event PHI is needed for such a purpose, the Privacy Officer must be consulted prior to making such a disclosure, and any disclosure of PHI shall comply with HIPAA.

EXHIBIT D

AUTHORIZATION FORM

Name of Patient:	**Date of Birth:**
Home Telephone:	**Social Security #:**
Home Address:	

1. I authorize the use and disclosure of the above named individual's health information as described below. The following individual or organization is authorized to make the disclosure:

2. Specify information to be disclosed:

3. Type of Admission	**DATES**
_____ Inpatient	_____
_____ Emergency Room	_____
_____ Clinic/Physical Therapy	_____
_____ Other	_____

4. Specific Confidential Information Authorized for this Release:
I specifically authorize the use and/or disclosure of the type of highly confidential information listed below by signing my name next to the category indicated, if any such information will be used or disclosed pursuant to this authorization:

Psychotherapy Notes _____ Venereal Disease Information _____
Genetic Information _____ Drug and Alcohol Information_____
Tuberculosis Information_____ Mental Health Information_____
HIV/AIDS Related Information_____
(Including the fact that HIV test ordered, performed or reported, regardless of whether the results of such tests were positive or negative)

5. Release Information to:
[ ] Myself (the patient or authorized representative) [ ] To Organization/Individual Below
I authorize the use or disclosure of my health information to:

Organization: **Individual Name:**

Street Address:

Phone #:

6. Purpose of Release:

_____
_____
_____

I understand that I may refuse to sign or may revoke this authorization for any reason at any time and that such refusal or revocation will not affect the commencement, continuation or quality of my treatment. I understand that if I revoke this authorization I must do so in writing and present my written revocation to the Privacy Officer. I understand that the revocation will not apply to information that has already been released in response to this authorization. I understand that the revocation will not apply to my insurance company when the law provides my insurer with the right to contest a claim under my policy. Unless otherwise revoked, this authorization will expire on the following date, event or condition: _____. If I fail to specify and expiration date, event or condition, this authorization will expire in six months.

I understand I may inspect or copy the information to be used or disclosed, as provided in CFR 164.524. I understand any disclosure of information carries with it the potential for an unauthorized re-disclosure and the information may not be protected by federal confidentiality rules.

I have read and understand the terms of this Authorization and I have had the opportunity to ask questions about the use and disclosure of my health information. If I have questions about disclosure of my health information, I can contact the Montclair State University Privacy Officer. By my signature below, I hereby, knowingly and voluntarily, authorize _____ to use or disclose my health information in the manner described above.

Patient Signature: _____Date:_____

If the patient is a minor or otherwise unable to sign this Authorization, then obtain the signature of the legally authorized representative/individual below.

Description of Authority: _____

Signature: _____Date:_____

EXHIBIT E

NOTICE OF PRIVACY PRACTICES & ACKNOWLEDGMENT OF RECEIPT

NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY, SIGN THE ACKNOWLEDGEMENT OF RECEIPT, AND GIVE TO THE RECEPTIONIST.

Protecting Your Personal and Health Information

MSU is committed to protecting the privacy of its patients' health information. MSU is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information. This Notice explains MSU's privacy practices, legal duties, and your rights concerning your health information. In this Notice your health information is referred to as "health information" and includes information regarding your health care and treatment with identifiable factors including your name, age, address, income or other financial information. MSU is required to abide by the terms of the Notice of Privacy Practices in effect as required by 45 C.F.R. 164.520(b)(v)(B). This Notice takes effect **April __, 2014** and will remain in effect until replaced.

Uses and Disclosures of Your Health Information

We will use and disclose health information about you for treatment, payment and health care operations. For example:

Treatment: We may provide another physician or subsequent healthcare provider who is treating you with copies of your treatment records created by the University Health Center or Center of Psychological Services to assist him or her with your treatment.

Payment: The Center for Audiology and Speech Language Pathology may disclose your health information to obtain payment by Medicare for services we provide to you.

Your Authorization: In addition to our use of your health information for treatment, payment, or healthcare operations, you may give us written authorization to use your health information or to disclose it to anyone for any purpose. If you give us an authorization, you may revoke it in writing at any time. Your revocation will not affect any use or disclosures permitted by your authorization while it was in effect. Unless you give us a written authorization, we cannot use or disclose your health information for any reason except those described in this Notice.

To Your Family and Friends: We must disclose your health information to you, as described in the Patient Rights section of this Notice. We may disclose your health information to a family member, friend, or other person to the extent necessary to help with your healthcare under HIPAA, but only if you agree that we may do so.

Persons Involved in Care: We may use or disclose health information to notify, or assist in the notification of (including identifying or locating) a family member, your personal representative, or another person responsible for your care, of your location, your general condition, or death. If you are present, then prior to use or disclosure of your health information, we will provide you with an opportunity to object to such uses or disclosures. In the event of your incapacity or emergency circumstances, we will disclose health information based on a determination using our professional judgment disclosing only health information that is directly relevant to the person's involvement in your healthcare. We will also use our professional judgment and our experience with common practice to make reasonable inferences of your best interest in allowing a person to pick up filled prescriptions, medical supplies, x-rays, or other similar forms of health information.

Marketing Health-Related Services: We will not use your health information for marketing without a written authorization from you.

Required by Law: We may use or disclose your health information when we are required to do so by law, including, but not limited to, court or administrative orders, subpoenas, discovery requests, or other lawful process.

Abuse or Neglect: We may disclose your health information to appropriate authorities if we reasonably believe that you are a possible victim of abuse, neglect, or domestic violence, or the possible victim of other crimes. We may disclose your health information to the extent necessary to avert a serious threat to your health or safety or the health or safety of others.

National Security: We may disclose to military authorities the health information of Armed Forces personnel under certain circumstances. We may disclose to authorized federal officials health information required for lawful intelligence, counterintelligence, and other national security activities. We may disclose health information to a correctional institution or law enforcement official having lawful custody of protected health information of an inmate or patient under certain circumstances.

Appointment Reminders: We may also use health information about you to call, leave a voice message, or send a postcard or letter to you as a reminder about an appointment.

Research: Under certain limited circumstances, we may use and disclose health information about you for research purposes. All research projects, however, are subject to a special approval process through MSU's Institutional Review Board.

Miscellaneous. We may also disclose your health information when there is a serious threat to health or safety of a person or to the public, or in connection with disaster relief efforts, workers compensation programs, public health activities, health care oversight, to coroners, medical examiners and funeral directors, the facilitation of organ/tissue donation, military/veteran benefits, protective Services for the President and others, and for use in civil, criminal, or administrative actions or proceedings or in anticipation of litigation).

Selling Protected Health Information (PHI) or Electronic Health Records (EHR): We will not sell your PHI or EHR without your prior authorization.

Rights You Have Regarding the Use and Disclosure of Your Health Information. You have the right to request all of the following:

Access to Your Health Information: You have the right to inspect, copy and request a copy of your health information subject to certain exceptions permitted by HIPAA. A nominal fee may be charged for providing copies. Access to your records may also be limited if it is determined that by providing the information it could possibly be harmful to you or another person. If access is limited for this reason, you have a right to request a review of that decision.

Amendment: You have the right to request in writing an amendment to your health information. The request must identify which information is incorrect and an explanation of why you think it should be amended. If the request is denied, a written explanation stating why will be provided to you. You may also make a statement disagreeing with the denial which will be added to the information of the original request. If your original request is approved, we will make reasonable effort to include the amended information in future disclosures. (Amending a record does not mean that any portion of your health information will be deleted.)

Accounting of Disclosures: If your health information is disclosed for any reason other than treatment, payment, or operation, you have the right to an accounting for each disclosure in accordance with HIPAA.

Restriction Requests: You have the right to request that the clinic place additional restrictions on uses and disclosures of your health information. We may not be able to accept your request, but if we do, we will uphold the restriction unless it is an emergency.

Communication: MSU must accommodate reasonable requests to receive communications of PHI from the health care provider by alternative means or at alternative locations.

Electronic Notice: If you received this notice by accessing a Web site or by e-mail, you are also entitled to have a paper copy which is available by request from the clinic or department.

Changes to this Notice

We reserve the right to change our privacy practices and terms of this Notice at any time, as permitted by applicable law. We reserve the right to make the changes in our privacy practices and the new terms of our Notice effective for all health information that we maintain, including health information we created or received before we made the changes. Before we make such changes, we will update this Notice and post the changes in the waiting room or lobby of the facility or our webpage. You may also request a copy of this Notice at any time.

Questions and Complaints
For questions regarding this Notice, please contact MSU's Privacy Officer at:

Privacy Officer
Montclair State University
Academic Affairs
1 Normal Avenue, Montclair, NJ 07043
Phone: 973/655-7781 Fax: 973/655-3022
E-mail: PrivacyOfficer@montclair.edu

If you are concerned that your privacy rights may have been violated, you may contact any of the people listed below to make a complaint. **Complaints may also be made directly to the U.S. Department of Health and Human Services by following the instructions on the HHS/OCR Website at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html**.

If you choose to make a complaint with us or the U.S. Department of Health and Human Services, we will not retaliate in any way.

ACKNOWLEDGMENT OF RECEIPT OF HIPAA PRIVACY NOTICE

I, _____ have received a copy of the HIPAA Privacy Notice.
PLEASE PRINT

_____ _____
Patient Signature
Date:

HIPAA requires the Healthcare Components of Montclair State University with direct treatment relationships make a good faith effort to obtain an individual's written acknowledgment of the receipt of the Practice's privacy notice at the time of the first service delivery (except in emergencies).

PERMITTED DISCLOSURE OF INFORMATION TO FAMILY:

I authorize Montclair State University's Healthcare Components to disclose information regarding my medical condition and care to the following:

_____ _____
Name/Relationship

_____ _____
Name/Relationship

_____ _____
Name/Relationship

This authorization shall remain in effect unless revoked in writing.

_____ _____
Patient Signature
Date:

REASON IF ACKNOWLEDGEM ENT IS NOT SIGNED:

EMPLOYEE WITNESS:
DATE:

EXHIBIT F

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT (this "**Agreement**") is entered into as of the ___ day of _____, 2014 to be effective as of _____ ___, 2014 (the "**Effective Date**"), by and between Montclair State University, 1 Normal Avenue, Montclair, NJ 07043 ("**Covered Entity**"**)** and _____ (**"Business Associate**").

RECITALS

WHEREAS, Business Associate performs services ("**Services**") on behalf of Covered Entity pursuant to that certain _____ Agreement dated _____ ("**Underlying Agreement**"), which Services involve the Use and/or Disclosure of Protected Health Information (defined below); and

WHEREAS, the parties desire to enter into this Agreement in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") and its implementing regulations, as amended and in effect.

NOW, THEREFORE, the parties do hereby agree as follows:

1. **Definitions.** Capitalized terms not otherwise defined in this Agreement shall have the same meaning as those terms in the Privacy Rule and the Security Rule (defined below).

    a) "**Breach**" when capitalized, "Breach" shall have the meaning set forth in 45 CFR § 164.402 (including all of its subsections); with respect to all other uses of the word "breach" in this Agreement, the word shall have its ordinary contract meaning.

    b) "**Electronic Protected Health Information**" or "**EPHI**" shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103, limited to information that Business Associate creates, accesses, receives, or maintains on behalf of Covered Entity.

    c) "**Protected Health Information**" or "**PHI**" shall have the meaning set forth in the Privacy Rule, limited to information that Business Associate creates, accesses, receives, or maintains on behalf of Covered Entity. PHI includes EPHI.

    d) "**Privacy Rule**" means the Standards for Privacy of Individually Identifiable Health Information, codified at 45 CFR parts 160 and 164, Subparts A, D, and E, as currently in effect.

e) "**Security Rule**" means the Standards for Security for the Protection of Electronic Protected Health Information, codified at 45 CFR parts 160 and 164, Subpart C.

f) "**Unsecured Protected Health Information**" shall have the same meaning as the term "unsecured protected health information" in 45 CFR § 164.402, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

2. Business Associate Obligations. Business Associate acknowledges and agrees that it is considered a "business associate" as defined by HIPAA. As a Business Associate of Covered Entity, Business Associate shall, in addition to complying with the terms of this Agreement, comply with the following and any state provisions that are more restrictive:

a) Uses and Disclosures. Business Associate shall not Use or further Disclose PHI other than as permitted or required by this Agreement, to perform Services under the Underlying Agreement or as Required By Law, provided that:

i) Such Use or Disclosure would not violate HIPAA if done by Covered Entity; and

ii) Such Use or Disclosure shall be limited to the minimum necessary to accomplish the permissible purpose(s) of the Use or Disclosure.

b) Uses and Disclosures Permitted By Law. As permitted by the Privacy Rule, Business Associate may Use or Disclose PHI: (i) as is necessary for the proper management and administration of Business Associate's organization, (ii) to provide data aggregation services relating to the health care services of the Covered Entity; and (iii) to carry out the legal responsibilities of Business Associate; provided, however, that any permitted Disclosure of PHI to a third party must be either Required By Law or subject to reasonable assurances obtained by Business Associate from the third party that PHI will be held confidentially, and securely, and Used or Disclosed only as Required By Law or for the purposes for which it was disclosed to such third party, and that any breaches of confidentiality of PHI which become known to such third party will be immediately reported to Business Associate.

c) Privacy Rule. To the extent Business Associate carries out one or more of Covered Entity's obligations under the Privacy Rule, Business Associate shall comply with the requirements of HIPAA that apply to Covered Entity in the performance of such obligation(s).

d) Security Rule. Business Associate agrees to comply with the requirements of the Security Rule that apply to business associates.

e) Safeguards. Business Associate shall use safeguards that are appropriate and sufficient to prevent Use or Disclosure of PHI other than the Uses and Disclosures permitted or required by this Agreement, including but not limited to implementing Administrative Safeguards, Physical Safeguards, and Technical Safeguards that

reasonably and appropriately protect the Confidentiality, Integrity and Availability of EPHI.

f) Reporting. Business Associate shall report to Covered Entity any Use or Disclosure of PHI not permitted or required by this Agreement and any Security Incident of which it becomes aware in accordance with HIPAA reporting requirements.

g) Agents and Subcontractors. Business Associate shall ensure that any and all subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree, in writing prior to the subcontractors' receipt of such PHI, to the same terms and conditions that apply to Business Associate with respect to PHI, including without limitation the provisions of this Agreement. Business Associate shall make such agreements with its subcontractors available to Covered Entity upon Covered Entity's request.

h) Patient Rights.

i) Patient Right to Access. Business Associate shall make PHI in a Designated Records Set that it maintains available to Covered Entity at the request of Covered Entity or an Individual, so that Covered Entity may meet the requirements of 45 C.F.R. §164.524. If any Individual requests access to his or her own PHI from Business Associate, Business Associate shall, within two (2) business days, notify Covered Entity of the details of such request.

ii) Patient Right to Amend. Business Associate shall incorporate amendment(s) to PHI in a Designated Records Set that it maintains at Covered Entity's request and in compliance with 45 C.F.R. §164.526. If any Individual submits to Business Associate a request to amend his or her own PHI, Business Associate shall, within two (2) business days, notify Covered Entity of the details of such request.

iii) Patient Right to Request Accounting. Business Associate shall document and make available to Covered Entity the information required to provide an accounting of disclosures or, as requested by Covered Entity, to the subject of the PHI, so that Covered Entity may meet the requirements of 45 C.F.R. §164.528. If any Individual requests an accounting from Business Associate, Business Associate shall, within two (2) business days, notify Covered Entity of the details of such request.

(1) Business Associate agrees to implement an appropriate record keeping process to enable it to comply with the requirements of this Section.

(2) Business Associate agrees to provide PHI it maintains electronically in a Designated Record Set in an electronic form at the request of Covered Entity or an Individual.

i) Audit. Business Associate shall make its internal practices, books, and records relating to the Use and Disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity available to the Secretary of Health and Human Services, upon request, for purposes of determining compliance with HIPAA.

j) Mitigation. Business Associate shall mitigate promptly, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of this Agreement, the Privacy Rule, the Security Rule, or other applicable federal or state law.

k) Breach. If Business Associate has knowledge or a reasonable belief that a Breach or potential Breach of Unsecured Protected Health Information has occurred or may have occurred, Business Associate shall notify the Covered Entity in accordance with the requirements of 45 CFR § 164.410. Such notification shall include, to the extent possible, the identification of each Individual whose PHI has been or is reasonably believed to have been accessed, acquired, Used or Disclosed during the Breach, along with any other information that the Covered Entity will be required to include in its notification to the Individual, the media and/or the Secretary, as applicable, including, without limitation, a description of the Breach, the date of the Breach and its discovery, the types of Unsecured Protected Health Information involved and a description of the Business Associate's investigation, mitigation, and prevention efforts.

3. Term & Termination.

a) Term. The Term of this Agreement shall begin on the Effective Date, and shall continue until all PHI provided by or on behalf of Covered Entity to Business Associate is destroyed or returned to Covered Entity. If it is infeasible to return or destroy all PHI, this Agreement shall continue for so long as PHI is maintained by Business Associate, which maintenance shall be in accordance with Section 3.c herein.

b) Termination.

i) By Covered Entity. Upon determination by Covered Entity in its reasonable discretion of a material breach by Business Associate of this Agreement, Covered Entity may terminate this Agreement and the Underlying Agreement upon thirty (30) days' notice; provided however, Covered Entity shall not terminate if Business Associate takes reasonable steps to mitigate harm resulting from the breach and otherwise agrees to comply with the terms of this Agreement on a forward-looking basis within such thirty (30) day notice period.

ii) By Business Associate. Upon determination by Business Associate in its reasonable discretion of a material breach by Covered Entity of this Agreement, Business Associate may terminate this Agreement and the

Underlying Agreement upon thirty (30) days' notice; provided however, Business Associate shall not terminate if Covered Entity takes reasonable steps to mitigate harm resulting from the breach and otherwise agrees to comply with the terms of this Agreement on a forward-looking basis within such thirty (30) day notice period.

c) Return on Termination. At termination of this Agreement or the Underlying Agreement, to the extent feasible, Business Associate shall return or destroy all PHI that Business Associate maintains in any form and shall retain no copies of PHI. Notwithstanding anything herein to the contrary, if Business Associate determines, in its reasonable discretion, that the return or destruction of such PHI is not feasible, Business Associate shall extend the protections of this Agreement to the remaining information and limit further Uses and Disclosures of PHI to those purposes that make the return or destruction of PHI infeasible.

d) Survival. The terms of this Section shall survive the termination or expiration of this Agreement.

4. **Required Disclosure.** If Business Associate is confronted with legal action to disclose any PHI, Business Associate shall promptly notify and assist Covered Entity in obtaining a protective order or other similar order, and shall thereafter disclose only the minimum amount of PHI that is required to be disclosed in order to comply with the legal action, whether or not a protective order or other order has been obtained.

5. **Indemnification.** Business Associate agrees to indemnify, defend, and hold harmless Covered Entity and its directors, officers, affiliates, employees, agents, and permitted successors from and against any and all claims, losses, liabilities, damages, costs, and expenses (including reasonable attorneys' fees) arising out of or related to Business Associate's breach of its obligations under this Agreement, including, but not limited to a Breach of Unsecured Protected Health Information by Business Associate.

6. **Compliance with Laws.** Business Associate shall comply with all applicable federal, state and local laws, rules and regulations, including, without limitation, the requirements of HIPAA.

7. **Underlying Agreement.** Except as specifically required to implement the purposes of this Agreement, and except to the extent inconsistent with this Agreement, all terms of the Underlying Agreement shall remain in full force and effect. In the event of a conflict between the terms of the Underlying Agreement and this Agreement, this Agreement shall control.

8. **No Third-Party Beneficiaries.** Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Covered Entity, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

9. **Ownership.** Covered Entity shall be and remain the sole and exclusive owner of its PHI.

10. **Amendment.** The parties shall amend this Agreement from time to time by mutual written agreement in order to keep this Agreement consistent with any changes made to the HIPAA laws

or regulations in effect as of the Effective Date and with any new regulations promulgated under HIPAA. Covered Entity may terminate this Agreement in whole or in part if the parties are unable to agree to such changes by the compliance date for such new or revised HIPAA laws or regulations.

11. Counterparts. This Agreement may be executed in two or more counterparts, each of which shall be an original, but all of which taken together shall constitute one and the same agreement.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

MONTCLAIR STATE UNIVERSITY	**BUSINESS ASSOCIATE**
By: _____	By: _____
Name: _____	Name: _____
Its: _____	Its: _____