Montclair State University

HIPAA Security Policy

Effective: June 25, 2015

HIPAA Security Policy and Procedures

Montclair State University is a hybrid entity and has designated Healthcare Components that are subject to HIPAA. MSU's Healthcare Components and Business Associates must comply fully with the applicable HIPAA Security Rule requirements. To

H. “Personal Device” means an electronic asset used to access MSU e-PHI that is not owned or provided by MSU to the Workforce, including but not limited to a, laptop, smartphone and tablet that supports electronic assets regardless of whether or not they contain Mobile Media.

I. “Privacy Officer” shall mean the individual appointed by the Provost to assume the obligations of the Privacy Officer in the MSU HIPAA Privacy Policy.

J. “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, as amended and in effect.

K. “Workforce” means all members of the MSU’s workforce who have access to PHI in order to perform the functions of MSU Healthcare Components. Workforce includes individuals who would be considered part of MSU’s workforce under the Privacy Rule, such as volunteers, trainees, and other persons whose work performance is under the direct control of MSU, whether or not they are paid by MSU.

II. SECURITY OFFICIAL AND CONTACT PERSON

MSU designates the Vice President for Information Technology, or his or her designee, as the MSU Security Official. The Security Official serves as the person who is responsible for MSU’s compliance with the Security Rule and this Policy and who assists with compliance and enforcement of this Policy. Wherever this Policy refers to the Security Official, if applicable, such reference will include any person delegated by the Security Official, whether such delegation is verbal or written.

Contact information for the Security Official shall be posted on the website for MSU.

Complaints concerning MSU’s compliance with this Policy shall be referred to the Privacy Officer. Complaints received by the Privacy Officer that relate to the information technology and electronic information of the University shall be resolved in consultation with the Vice President for Information Technology. Complaints received by the Privacy Officer that relate to the physical premises of the University shall be resolved in consultation with the Vice President for University Facilities. Complaints received by the Privacy Officer that arise out of a University employee’s non-compliance with this Policy shall be referred to the Vice President for Human Resources.

Contact information for the Privacy Officer shall be posted on the website for MSU.

III. WORKFORCE TRAINING

A. Policy

Workforce members will receive the necessary and appropriate training to permit them to carry out their functions for MSU in accordance with this Policy.

B. Procedures

1. Identification of Workforce. The Privacy Officer, in consultation with the Security Official and University Counsel, will identify all employees and other personnel who are members of the Workforce for training under this Policy.

2. Training. The Security Official will provide for the delivery of training sessions for all current members of the Workforce regarding the Security Rule and this Policy. All individuals who join the Workforce will be trained within a reasonable time after joining the Workforce. Training for existing Workforce members will occur as MSU deems necessary and in accordance with applicable MSU policies or practices. If this Policy is materially changed, MSU will provide training related to the changes as appropriate or necessary for the Workforce within a reasonable time after this Policy is modified.

3. Documentation. The Security Official will document the time, date, place, and content of each training session, as well as the Workforce members who attend

(ii) Limitation of access to those sensitive areas where PHI or e-PHI are accessed or maintained to only that access that is reasonably necessary for an individual’s role or function;

(iii) Documentation of access authorizations and uses, in addition to ongoing monitoring and maintenance of such records by the Security Official or by his or her designee, as reasonable and appropriate;

(iv) Issuance of identification tokens, badges, or smart cards that describe a person’s identity, his or her approved areas of access, and an expiration date, if applicable;

(v) Updates to each individual access capabilities when the individual’s role, responsibility or position changes; and

(vi) Revocation or limitation of any access authorization in a timely manner when access is no longer needed.

c. MSU will develop and implement procedures to ensure that all physical safeguards are reviewed, tested, and revised on a regular basis.

2. Technical Safeguards

a. As applicable, technical safeguards will be implemented, such as reasonable and appropriate firewalls, security software, and encryption programs as well as a requirement for unique usernames and passwords for access to MSU computer files and Mobile Devices that contain PHI. Members of the Workforce will have such unique usernames and passwords.

b. All e-PHI maintained in an MSU e-mail, on a MSU hard drive, or on a Mobile Device will be authorized and will necessitate the Workforce to coordinate the activation of MSU’s encryption technology to ensure that the e-PHI is secure. Workforce are prohibited from accessing Mobile Media containing e-PHI using a Personal Device unless the Personal Device contains encryption technology provided by MSU.

c. When PHI is removed from electronic media, MSU Workforce will delete all e-PHI in a commercially reasonable manner to ensure that the information is permanently unreadable prior to disposal. When a Mobile Device is returned by the Workforce to the University, the Division of Information Technology shall delete all Mobile Media, including but not limited to e-PHI, before the Mobile Device is reassigned, returned to the lessor, or disposed.

V. SECURITY OF ELECTRONIC PHI

A. Policy

MSU requires reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of e-PHI; to protect against any reasonably anticipated threats or hazards to the security or integrity of the e-PHI; to protect against any reasonably anticipated uses or disclosures that are not permitted by the Security Rule; and to support Workforce compliance with this Policy and with the Security Rule.

MSU will review and modify its security measures as needed and will update documentation of such security measures periodically and as needed.

B. Procedures

1. Security Management Process

MSU maintains a security management process to prevent, detect, contain, and correct security violations of applications and/or systems that contain e-PHI.

a. Risk Analysis: MSU will conduct an assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by MSU, annually or upon a significant change in the system. Such review will include the assessment of the reasonableness of encryption or other enciphering tools.

b. Risk Management: On the basis of its risk analysis, MSU will manage risks to its e-PHI by limiting vulnerabilities to a reasonable and appropriate level by taking into account various factors such as the complexity of the vulnerability; MSU's technical infrastructure, hardware, software, and security capabilities; the costs of security measures; and the criticality of the e-PHI potentially affected.

2. Information System Activity Review

MSU will regularly review records of information system activity; such activity may include system and application audit logs, access reports, and other security documentation and reporting set forth in this Policy. The Security Official or another appropriate administrator will regularly monitor access to information systems to ensure compliance with this Policy. Access audit trails will be maintained and reviewed at least annually or in response to suspicious activity to determine whether unsuccessful logons and access attempts are occurring. The Security Official will also periodically run reports of user identification names, send a report to the administrator of the Healthcare Component(s), and update user access after a response.

3. Workforce Security

MSU maintains workforce security procedures to ensure that all members of the Workforce have only appropriate access to e-PHI.

c. <u>Emergency Mode Operation Plan</u>: MSU administrators from the IT Departments will design and implement strategies to prioritize system restoration, mitigate loss, and identify chains of command and response.

In addition, regular planned testing and response training will be performed to ensure readiness.

8. Evaluation

MSU will perform periodic technical and nontechnical evaluations based on the standards set forth in the Security Rule, to ensure that MSU's policies and procedures are updated as warranted by changes in MSU's environmental or operational conditions affecting the security of e-PHI. Such evaluation will be achieved through the collective efforts of MSU's Security Official, Vice President for Facilities and University Counsel.

VI. SANCTIONS FOR VIOLATIONS OF SECURITY POLICY

A. Policy

Employees who violate this Policy may be subject to disciplinary measures, consistent with any applicable collective bargaining agreement, up to and including suspension, dismissal, and termination.

B. Procedures

During training, the Workforce will be informed that disciplinary actions may be imposed if this Policy is violated. Appropriate disciplinary actions will be determined on the basis of the nature of the violation, its severity, and whether it was intentional or unintentional. Such disciplinary actions may include, without limitation, verbal warnings, written warnings, probationary periods, and termination of employment. Application of any disciplinary actions will be documented in accordance with MSU's record retention procedures.

The Vice President for Human Resources will determine whether, and to what extent, disciplinary action should be imposed for a violation of this Policy.

VII. UNAUTHORIZED DISCLOSURES OF PHI

A. Policy

To the extent possible, MSU will mitigate any harmful effects that become known to it of a use or disclosure of an individual's PHI in violation of this Policy.

The Security Official and Privacy Officer, in consultation with University Counsel, will coordinate the reporting of any use or disclosure of PHI that is not permitted or required in accordance with HIPAA, the Security Rule, and any applicable underlying contractual agreement. This includes reporting Breaches and Security Incidents of which it becomes aware, in accordance with HIPAA reporting requirements and the MSU HIPAA Privacy Policy.

B. Procedures

If a member of the Workforce becomes aware of a disclosure of PHI, either by a member of the Workforce or by an outside consultant or contractor, that is not in compliance with this Policy, the Workforce member will report the disclosure to the Privacy Officer. This may be accomplished through the Workforce member's supervisor.

X. RECORD RETENTION AND DISPOSAL

A. Policy

MSU will maintain documentation supporting compliance with this Policy, including audit logs, risk analyses, training completions, and Workforce sanctions, in accordance with internal and state record-retention requirements and in no case for less than six (6) years.

MSU will dispose of records, including PHI, in accordance with its HIPAA Privacy Policy.

XI. Related Policies.

MSU Compliance Plan
HIPAA Privacy Policy
Policy on Responsible Use of Computing
Data Classification and Handling (Safeguarding Sensitive and Confidential Information Policy)

Exhibit A

Personal Device Terms of Use

Personal Device Terms of Use

Montclair State University takes the safety and security of the protected health information generated by its Healthcare Components and Business Associates very seriously. The loss of this information could have serious detrimental effects on the University and/or the patients of its Healthcare Components. In order to use a device not issued by the University (such as an appropriate laptop, smartphone, or tablet) (collectively, “Personal Device”) to access electronic protected health information (“ePHI”) as defined by the Standards for Privacy of Individually Identifiable Health Information, codified at 45 CFR parts 160 information, or I subsequently withdraw my consent to these terms and conditions, I understand and acknowledge that University has the right to physically or remotely remove any and all ePHI from my Personal Device. I further understand and acknowledge that in these circumstances that the University has no obligation before exercising this right to prove any disclosure, or threat of disclosure, of any ePHI or any other harm to University, or to provide me with any further notice.

Likelihood of permanent loss of personal information connected with physical or remote removal procedure. In the event of a removal of ePHI from my Personal Device, I understand and acknowledge that it is likely that all or a portion of personal information on my Personal Device (for example, my contacts, audio files, video files, applications, photos) may be permanently deleted or destroyed. I further understand and acknowledge that University recommends that I save or store such personal information on another device or on other equipment to avoid its permanent deletion or destruction, and I undertake the sole responsibility to do this. Should I fail to do this, I accept the risk that personal information may be permanently deleted or destroyed as described above.

Mobile device security compatibility. I agree that I will download and install all applications that University may require in order to permit my Personal Device to access University’s systems and networks or to otherwise gain access to ePHI. I agree to keep the device current with security patches and updates as approved by University and will not “jailbreak” the device (installing software that allows the user to bypass built-in security features and controls). I understand that to ensure that my Personal Device continues to meet information security requirements, University’s mobile device management software may be used to periodically verify that my Personal Device has the required applications installed and that it continues to meet compatibility requirements including operating system requirements. I understand that the applications may require use of a unique password and/or another authentication process in order for my Personal Device to access or use University’s systems and information.

Duty to take reasonable security measures and report loss, theft or unauthorized access. In order to protect ePHI, I agree to use a “PIN code” or unique password access system on my Personal Device. I further agree to employ other reasonable measures to protect my Personal Device against unauthorized use. For example, to not leave my Personal Device unattended in a visible or accessible place, not use it on networks that are not specifically known by me to be secure, and not accept or download content from suspicious or unknown sources. In the event that my Personal Device is lost or stolen or an unauthorized third party gains access to it or to my University email account or ePHI via my Personal Device, I agree to immediately report this to my supervisor or ealk” .5.4(wile)-that I fullest extent possible under applicable laws, any and all rights to make any claim whatsoever against the University for any such loss or damage.

By signing this form, I expressly consent to and agree with the above terms and conditions associated with using a Personal Device for professional work purposes to access ePHI. I understand that if I am an employee or volunteer and I breach the terms of this form, I may be subject to disciplinary action, up to and including the termination of my employment and/or contract with the University without notice or payment in lieu of notice. I understand that if I am a student of the University and I breach these terms, I may be subject to discipline under the Student Code of Conduct.

____________________ __________________________________

Date Workforce Member Signature

TABLE OF CONTENTS

Page