

Title/Subject: **HIPAA: PROTECTED HEALTH INFORMATION NETWORK POLICY**

Title/Subject: **HIPAA: PROTECTED HEALTH INFORMATION NETWORK POLICY**

Applies to: faculty staff students student employees visitors contractors student
clinicians

Effective Date of This Revision: March 30, 2005

Contact for More Information: HIPAA Security Officer
Foust Hall 019
989.774.6633

Board Policy Administrative Policy Procedure Guideline

BACKGROUND:

Central Michigan University is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations. Its business activities include both covered and non-covered functions. It has decided to designate itself as a Hybrid Entity.

According to the law, all CMU officers, employees and agents of units within the Hybrid Entity must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client. This IIHI is protected health information (PHI) and shall be safeguarded in compliance with the requirements of the security and privacy rules and standards established under HIPAA.

For additional information on the measures Central Michigan University is implementing in order to comply with this legislation, visit the official HIPAA web site, www.cmich.edu/hipaa.

PURPOSE:

This policy enforces compliance with the measures that CMU has implemented as a result of the security regulations of the HIPAA legislation. Compliance by all units in the HIPAA Hybrid entity is necessary in order to minimize any liability the university may face as a result of this legislation. For CMU, this policy applies if the IIHI is obtained by a unit that has been defined by CMU as a part of the Hybrid entity. In addition, some units may elect to protect personally identifiable health information within the secured network, even if they are not within the hybrid entity. In those cases, these policies will also apply.

DEFINITIONS:

- 1.1 Electronic Protected Health Information (EPHI). Individually identifiable health information (IIHI) that is transmitted by electronic media; maintained in electronic media, such as magnetic tape, disc, optical file; or transmitted or maintained in any other form or medium, except that it does not include

Authority: M. Rao, President
History: No Prior History
Indexed as: HIPAA Protected Health Information Policy; HIPAA Health Information

Title/Subject: **HIPAA: PROTECTED HEALTH INFORMATION NETWORK POLICY**

PHI in education records covered by the Family Educational Rights and Privacy Act, certain treatment records of CMU students as described at 20 USC 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer.

- 1.2 Hybrid Entity – A department or unit designated as within the Hybrid Definition (See the policies link on www.cmich.edu/hipaa).
- 1.3 Protected Health Information Network (PHIN). The secured network established by CMU for HIPAA protected health information. Access to this data is only available from certified workstations by authorized personnel who have been properly trained and granted the access appropriate to their job.
- 1.4 Individually Identifiable Health Information (IIHI). A subset of health information, including demographic information collected from a patient/client/employee, that is created or received by a health care provider, health plan or employer and relates to the past, present, or future physical or mental health or condition of a patient/client/employee, the provision of health care to a patient/client/employee, or the past, present or future payment for the provision of health care to a patient/client/employee, and which identifies the patient/client/employee, or with respect to which there is a reasonable basis to believe that the information can be used to identify the patient/client/employee.
- 1.5 Workforce Member. A “Workforce Member” includes employees (and student employees), volunteers, trainees, and other persons whose conduct, in the performance of work for a unit in the CMU Hybrid entity is under the direct control of such entity, whether or not they are paid by the entity. This includes students who have access to PHI in order to satisfy a clinical experience requirement for a program of study.

All other terms used in this policy have the same meaning as those terms in the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 and the regulations at 45 CFR Parts 160, 162, and 164.

POLICY:

1. A PHIN will be created to provide security for protected health information by protecting both servers and workstations from unauthorized access. Using encryption (IPSEC) the data is protected between the workstations and servers.
2. Electronic protected health information may be stored on computers outside of this network, if the host system procedures are compliant with the HIPAA regulations.
3. To be compliant, these systems must provide evidence that they have isolated EPHI data and have implemented procedures that will restrict access to authorized persons only.
4. All EPHI that is not protected by appropriate application software must be housed within the secure network (PHIN).
5. All EPHI on PHIN will be protected by encryption and authentication protocols.
6. Non-EPHI data should never be stored on PHIN. The network is provided for EPHI only.
7. Each user needs to be activated on PHIN for the appropriate folder(s) and access rights.
8. Access to this network will be restricted to those who are authorized and limited to an appropriate use for the purpose stated.
9. Removal of systems containing EPHI for repair must be documented as to who removed the system, when it was removed, when it is scheduled to return and who authorized it. The technicians removing the system must be qualified by successfully completing the appropriate training.

PROCEDURE:

An individual who needs access to EPHI and PHIN must:

1. Obtain a completed Access Authorization form that grants access to the appropriate EPHI for their job. This will include which folders on PHIN the individual will need to access as Read Only or Read/Write.

Title/Subject: **HIPAA: PROTECTED HEALTH INFORMATION NETWORK POLICY**

2. Contact the help desk or the unit systems administrator and ask for “HIPAA Certification” of his/her workstation.
3. Download a copy of the Workstation and Personal Security Policy and the Workforce Security and Information Access Management Policy from www.cmich.edu/hipaa and read and understand these policies.
4. Contact the HIPAA Training Officer and ask to be scheduled for a HIPAA Security training session and the quiz that follows. HIPAA Security Training consists of:
 - a. Successful completion of the HIPAA Privacy Training and quiz.
 - b. Reading this Protected Health Information Network Policy, the Workstation and Personal Security Policy, the Workforce Security and Information Access Management Policy and the Contingency Plans Policy.
 - c. Completion of the HIPAA End User Security Training
 - d. Successful completion of the End User Security Quiz.Units may provide additional security training at their discretion.
5. Ask the technical representative for his/her area to move all EPHI to protected folders within the PHIN and to certify each workstation that will need access.
6. Note: It is important to schedule this migration for an appropriate time and to schedule the workstation certification in a sequence that does not disrupt normal work flow. Once the EPHI has been moved to a protected environment, a user will not be able to access the data until his/her workstation is certified.

The HIPAA Compliance Council is the enforcement entity for these policies and the Internal Audit department is a member of this council. The compliance council may ask for periodic audits for HIPAA compliance and to make appropriate recommendations for improvement as needed.

Central Michigan University reserves the right to make exceptions to, modify or eliminate these guidelines. This document supersedes all previous guidelines relative to its subject.