

Title/Subject: **HIPAA: WORKSTATION AND PERSONAL SECURITY 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 Chief Privacy Officer      HIPAA Security Officer  
1303A W. Campus      Foust Hall 019  
989.774.3971      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](http://www.cmich.edu/hipaa)

### PURPOSE:

This policy establishes minimum policies for workstation and personal use of systems that have access to Electronic Protected Health Information (EPHI) that has been stored within the Protected Health Information Network (PHIN). These policies and procedures are needed to comply with CFR 164.308 of the HIPAA security regulation. 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 Workstation. A personal computer that has access to the PHI that is stored within the protected health information network (PHIN). This definition includes personal computers in a typical work area or at home, laptop computers used on campus or in a remote location, and wireless devices, such as PDA's that have been configured to provide access to PHI, and electronic media stored in their immediate environment.

---

Authority: M. Rao, President  
History: No Prior History  
Indexed as: HIPAA Workstation; HIPAA Personal Security Policy; HIPAA Security Policy

Title/Subject: **HIPAA: WORKSTATION AND PERSONAL SECURITY POLICY**

---

- 1.2 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.
- 1.3 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 IIHI 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.
- 1.4 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 workstation that needs access to EPHI that is stored within the PHIN must be certified by a qualified technician according to the HIPAA Workstation Certification Checklist. This checklist should be considered a guideline for those workstations that need access to PHI that is not stored within the PHIN.
2. Once a workstation has been certified, a drive will be mapped to enable access to the appropriate system and folders within the PHIN by the technician.
3. EPHI should only be saved inside PHIN. It should not be saved on your computer hard drive, CD, Floppy Disk or Desktop. The protected folders on PHIN can be shared among authorized individuals if the access groups and rights are established correctly.
4. Once access to the PHIN has been provided, the workstation integrity will be maintained through a group policy that controls new software from being installed. Repairs will only be done by a certified PC repair technician.
5. Personnel who are allowed access to EPHI assume personal responsibility to maintain the integrity and security of the system and the network they use by following the established guidelines for personal login, password, and workstation controls.
6. All information systems and removable hard drives, etc. containing EPHI should be located in areas where general access to those systems is not permitted.
7. Removable media including, but not limited to, all tapes, CDs, DVDs, floppy disks, containing PHI should be kept in a secured location (e.g. vault, locked cabinet, safe deposit box) when not in use.
8. EPHI should only be printed when necessary and then only the data needed should be printed. A printer located within a unit of the Hybrid must be used and the printed data must be kept in a secure location and shredded when no longer needed.
9. Disposal or reuse of media containing EPHI should follow the CMU Computer Disposal Policy ([http://cmich.edu/Documents/information\\_technology/docs/policies\\_computer\\_disposal.pdf](http://cmich.edu/Documents/information_technology/docs/policies_computer_disposal.pdf)) such that the PHI data is not recoverable.

**PROCEDURE:**

Workstation security procedures:

1. Each workstation connected to the PHIN must comply with the HIPAA workstation compliance checklist. To request a copy of the HIPAA Workstation Certification Checklist, please contact your area Access Coordinator.

Title/Subject: **HIPAA: WORKSTATION AND PERSONAL SECURITY POLICY**

---

2. If the system that contains EPHI is not within the PHIN, documentation must be provided that EPHI has been isolated within the system and procedures have been implemented that will restrict access to authorized individuals only. This documentation and procedures will be stored on the secure documents link to the HIPAA web site.
3. Once a workstation has been certified, all work orders for that system must contain an indicator that the system is certified.
4. Each HIPAA certified system is subject to the Active Directory based Group policy, which will include automatic locking, access to approved software, automatic virus detection updates and configuration restrictions.
5. Repairs made to a HIPAA certified workstation will only be performed by someone qualified to work on HIPAA certified systems.
6. All HIPAA certified workstations must be physically secured to prevent public access. If an authorized user is not physically present in the immediate area, the system should be locked as described in Workstation Locking in the Personal Security Procedures (See #4 below), or there should be locked doors and only authorized personnel with keys.
7. The Active Directory based Group policy will enforce implementation of system logs that will record not less than 10 days of activity logs. These logs will be examined retroactively in the event of workstation security violation. The objective of this examination will be to determine the cause of the violation and the appropriate remedial action.
8. 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 make appropriate recommendations for improvement as needed.

Personal security procedures:

1. Security Reminders: Twice a year, in September and in February, a reminder notice will be sent via e-mail to everyone who works in a HIPAA classified position. The reminder notice will also be posted on the official HIPAA web site, [www.cmich.edu/hipaa](http://www.cmich.edu/hipaa)
2. Login Monitoring: If a Workforce Member thinks someone else has been trying to use his/her account, the individual must report it to the supervisor immediately. Please refer to the existing policy on [Investigation of Complaints](#) if further investigation is needed.
3. Password Reset: If a Workforce Member contacts the help desk to get a password reset, or to get work done on his/her computer, the individual is required to report that he/she is using a HIPAA certified workstation.
4. Workstation Locking: If the individual leaves his/her workstation unattended, he/she must lock the system by entering Ctrl/Alt/Delete and then pressing enter. When the individual returns, he/she can unlock the system by entering Ctrl/Alt/Delete and the individual's password.

**GUIDELINES:**

1. See Password Guidelines in the secure documents section of [www.cmich.edu/hipaa](http://www.cmich.edu/hipaa).

*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.*