Title/Subject: **HIPAA: WORKFORCE SECURITY AND INFORMATION ACCESS MANAGEMENT**

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
Associate Dean/Administration & Finance
College of Medicine
989.774.7547

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, https://www.cmich.edu/office_president/general_counsel/hipaa/Pages/default.aspx.

PURPOSE:

This policy ensures that employees/students needing access to electronic protected health information (EPHI) have appropriate access, and prevents anyone who does not require access from obtaining access to EPHI. 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 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.

1.2 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

1.3 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 jobs.

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:

1.0 A unit that grants access to EPHI is required to document all access authorization and any changes in authorization for each workforce member to whom access is granted.

2.0 These units are required to grant only the access that is appropriate for the job as described in the Minimum Necessary Policy.

3.0 These units are required to assure that the workforce member has received appropriate training, understands appropriate information usage, and is aware of the Sanctions Policy and the Workstation Security Policy.

4.0 The appropriate Privacy Officer will designate in writing those managers/supervisors within that unit of the Hybrid entity who may authorize individual Workforce Members to have access to EPHI and at what levels. No manager/supervisor (except the Privacy Officer) may authorize access for her/himself. The manager/supervisor must approve access levels for individuals in writing.

5.0 Each system with access to EPHI must have one or more designated Access Coordinator(s) who will be responsible for controlling access. This person is responsible for granting and removing access to the EPHI maintained in the system. This person must be separate from the department managers who have authority to approve access levels.

6.0 Students fulfilling a clinical experience requirement do not need written authorization as long as they are supervised during the period they have access to PHI.

7.0 The clinical program director, or the faculty member who supervises these students, must provide a written statement that the program does and will train students on the privacy and security requirements of HIPAA before they are allowed access to PHI.

PROCEDURES:

1.0 Access Authorization Form

1.0 Each Access Coordinator will be responsible for maintaining an access authorization form for documenting the specific levels of access granted.

2.0 Managers/supervisors of individuals who need access to EPHI must complete an access authorization form for the appropriate system. The request must be approved by the manager/supervisor and the individual, and forwarded to the system's Access Coordinator.

3.0 All authorization forms must contain confirmation that the workforce member has received the necessary training and taken the appropriate test.

4.0 Once access has been granted, the Access Coordinator will keep the approved form on file for a minimum of six years from the time access is no longer used.

5.0 Managers/supervisors may request additional levels of access for a workforce member beyond that initially granted if needed. All requests for changes will be submitted on the appropriate access authorization form.

6.0 Managers/supervisors will notify the Access Coordinator immediately when a workforce member has terminated or needs reduced access to PHI. This notice may be via e-mail or any other expedient method, but it must be in writing.

7.0 The appropriate HIPAA Privacy Officer will resolve any issues regarding the level of access requested.

8.0 Student accounts will be reviewed by the supervisor at the end of each spring semester and notification given to the Access Coordinator of accounts requiring alteration or termination.

9.0 The Access Coordinator will meet with the appropriate HIPAA Privacy Officer at least once per year to review the types and/or levels of security being granted within each system, and to review the current users of the system and the access controls in place.

10.0 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.