Title/Subject: HIPAA: PROTECTING ELECTRONIC PERSONAL HEALTH INFORMATION POLICY

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

Effective Date of This Revision: November 16, 2018

Contact for More Information: HIPAA Privacy Officer
Foust 255
989-774-2829
hipaa@cmich.edu

BACKGROUND:

Central Michigan University is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) law 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 establishes compliance with the measures that CMU has implemented as a result of the security regulations of the HIPAA legislation. 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:

Hybrid Entity. A department or unit designated as within the Hybrid Definition (See the policies at https://www.cmich.edu/office_president/general_counsel/hipaa/Pages/Policies_and_Procedures.aspx).

Authority: M. Rao, President; Robert O. Davies, President
History: 2005-03-30
Indexed as: HIPAA Workstation; HIPAA Personal Security Policy; HIPAA Security Policy
Protected Health Information Network (PHIN). The secured network established by CMU for HIPAA protected health information. This network consists of appropriately protected segments of the broader CMU network and appropriately protected extensions established as a result of contractual relationships with third-party providers. Access to this network is only available from HIPAA workstations by authorized personnel who have been properly trained and granted the access appropriate to their job.

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.

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.

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 Workforce members are responsible for maintaining the privacy and security of all Electronic Protected Health Information (EPHI) at all times and in all locations. See also Safeguards policy #12-13 for protecting IIHI in other media (oral, paper).

2.0 CMU has adopted the following general strategy as a mechanism for protecting ePHI.
   a. OIT maintains a Protected Health Information Network (PHIN) as an added layer of defense to protect its EPHI.
   b. All systems housing EPHI must be housed on the PHIN.
   c. EPHI must remain in its primary host systems (which may include, but are not limited to, electronic medical records systems and HIPAA-certified fileshares) and may only be accessed using appropriately controlled devices/systems.
   d. EPHI removed from the PHIN, for any reason, must be encrypted both at rest and in transit.
   e. The HIPAA Privacy and Security Officers will jointly maintain procedures and guidelines for the protection of EPHI.
      i. The procedures and guidelines noted below will inherit or improve upon requirements found in CMU’s Secure Configurations – Workstations Policy, including those for malware defense, anti-virus, and encryption - https://www.cmich.edu/office_president/general_counsel/Documents/p03049.pdf
      ii. The procedures and guidelines noted below will inherit password controls from CMU’s Global ID Password Policy - https://www.cmich.edu/office_president/general_counsel/Documents/p03048.pdf
      iii. See also Safeguards policy #12-13.
      iv. The procedures and guidelines will include:
1. Administrative, Physical, and Technical Controls based upon where and how the EPHI is housed.
2. Administrative, Physical, and Technical Controls based upon how EPHI is being transmitted.
3. Administrative, Physical, and Technical Controls based on what type of device is accessing the data.
4. Administrative, Physical, and Technical Controls based on the location from and manner in which the device is connecting to EPHI.

PROCEDURE:

The HIPAA Privacy and Security Officers jointly maintain procedures for protecting EPHI across a number of scenarios. For more information, contact the HIPAA Privacy or Security Officer.

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.