Title/Subject: HIPAA: **SAFEGUARDS**

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

Effective Date of This Revision: November 21, 2019

Contact for More Information: **Office of HIPAA Compliance**
989-774-2829
hipaa@cmich.edu

☐ Board Policy ☒ Administrative Policy ☐ Procedure ☐ Guideline

---

BACKGROUND:

Central Michigan University (CMU) is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) law and regulations. CMU's business activities include both covered and non-covered functions. CMU has designated 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 individual. This IIHI is considered protected health information (PHI) and shall be safeguarded in compliance with the requirements of the Security and Privacy Rules and standards established under HIPAA.

The HIPAA law and regulations require CMU to have appropriate administrative, technical, and physical safeguards in place to protect the privacy, integrity, and confidentiality of PHI. CMU's policy is to maintain appropriate safeguards as required by HIPAA.

For additional information on the measures CMU is implementing in order to comply with this legislation, visit the official HIPAA web site at HIPAA.cmich.edu

PURPOSE:

In accordance with HIPAA Privacy and Security Rules, CMU has adopted this policy to fulfill its duty to protect the privacy, confidentiality, and integrity of PHI and electronic PHI (ePHI). CMU is committed to: safeguarding the flow of health information needed to provide and promote high quality health care, protecting the public's health and well-being, and carrying out the necessary functions of the self-funded health plan, as required by law. This policy identifies the most significant physical, administrative and technical safeguards to be followed by CMU's Hybrid Entity units.

DEFINITIONS:

Confidentiality: PHI/ePHI is not available or disclosed to unauthorized persons.

Integrity: PHI/ePHI is not altered or destroyed in an unauthorized manner.

Availability: PHI/ePHI is accessible and usable on demand by an authorized person.

Authority: Robert O. Davies, President
History: 2011-09-23; 2018-11-21
Indexed as: HIPAA Safeguards; HIPAA Protected Health Information

Hybrid Entity: A department or unit designated as within the HIPAA: Hybrid Entity Defined Policy #12-2. (See the policies at: HIPAA.cmich.edu)

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.

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 CMU will take reasonable precautions to prevent, detect, contain, and correct security violations. All workforce members and agents of CMU Hybrid Entity designation shall adhere to CMU policies and HIPAA rules in order to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI and ePHI.

2.0 The HIPAA risk management program shall include a collaboration between the HIPAA Privacy Officer, HIPAA Security Officer, and Chief Information Security Officer to recommend and monitor the effectiveness of security safeguards intended to reduce risks and vulnerability to a reasonable and appropriate level in order to:

a. To ensure the confidentiality, integrity, and availability of all PHI/ePHI that is created, received, maintained, or transmitted.
b. To identify and protect against reasonably anticipated threats to the security or integrity of the information.
c. To protect against reasonably anticipated, impermissible uses or disclosures.
d. To ensure workforce compliance with HIPAA Rules and the CMU HIPAA policies.

3.0 The HIPAA Security Officer will identify and maintain an inventory of the information systems that house ePHI. When a new system is implemented a security and privacy review will be conducted.

4.0 CMU will regularly perform reviews of information system activity (e.g., audit logs and trails, information system activity records, facility access records) for the purpose of detecting:

a. Unauthorized access to ePHI.
b. Unusual patterns of use or activity.
c. Other potential security violations.

5.0 The HIPAA Privacy Officer and HIPAA Security Officer will collaborate with other HIPAA Security Incident Response Team (HSIRT) members to assure procedures are developed, implemented, and documented to:

a. Identify possible security incidents.
b. Respond to suspected or known security incidents.
c. Mitigate, to the extent practical, harmful effects of known security incidents.
d. Document and report security incidents and their outcomes.

6.0 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 established guidelines for personal login, password, and workstation controls.

7.0 Documentation of risk assessment and system activity reviews shall be retained for at least six years, in accordance with HIPAA documentation requirements.

8.0 All workforce members and agents of CMU Hybrid units shall be guided by the examples in Exhibit A to safeguard PHI/ePHI. This list of examples in Exhibit A is not all inclusive. Exhibit A may be updated and revised by the HIPAA Privacy Officer and HIPAA Security Officer as necessary and upon technological changes.

Central Michigan University reserves the right to make exceptions to, modify or eliminate this policy and or its content. This document supersedes all previous policies, procedures or guidelines relative to this subject.

---Remainder of page left blank intentionally, please see Exhibit A on following page---

SAFEGUARD POLICY
Examples and Guidance for HIPAA Workforce and Agents

Exhibit A

1.0 Protect from malware:
- a. Be aware of phishing attacks, such as an email tricking you to send sensitive information.
- b. Never provide your username or password in response to an email request. CMU would never ask you for a Global ID account password through email.
- c. Do not reply to an email that may be a phishing attempt.
- d. Do not open questionable links or attachments sent through email.
  - i. Report all phishing attempts to the CMU IT Help Desk.
  - ii. To report phishing, forward the email as an attachment to spambusters@cmich.edu
  - iii. If you have any uncertainties, contact the CMU IT Help Desk.

2.0 Mobile computing devices:
- a. Devices used to access ePHI must be encrypted and password protected.
- b. Protect against unauthorized viewing or listening to ePHI when using a mobile computing device.
- c. Protect from theft by locking the device in safe locations.

3.0 Workforce members may not access ePHI over unsecured public networks, such as at a coffee shop. Home networks must be secured according to CMU requirements-Contact CMU IT Help Desk for assistance.

4.0 PHI shall remain in the CMU system intended to house it.
- a. If ePHI has been authorized to leave the confines of the CMU systems, it must be encrypted.
  - i. For help with encrypting, call the CMU IT Help Desk.

5.0 Only access, store, or transmit PHI/ ePHI using CMU HIPAA approved systems or devices.

6.0 Workforce members are to use strong passwords that meet or exceed CMU's Password Policy #3-48. https://www.cmich.edu/office_president/general_counsel/Documents/p03048.pdf

7.0 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 REPORTING AND INVESTIGATING PRIVACY AND SECURITY INCIDENTS/COMPLAINTS.

8.0 Password sharing is prohibited.

9.0 PHI must not be stored on personally owned devices.

10.0 PHI must not be stored on online services (such as Google Drive for example).

11.0 Only print and/or fax PHI or ePHI using CMU approved HIPAA printers and fax machines.

12.0 All information systems containing ePHI must be located in areas where general access to those areas is not permitted.

13.0 Removable media including, but not limited to, external hard drives, flash drives, tapes, CDs, DVDs, floppy disks, containing PHI must be kept in a secured location (e.g. vault, locked cabinet, safe deposit box) when not in use.

14.0 Secure all PHI that is transported, stored, or accessed offsite.

- a. Not leaving PHI unattended in a vehicle or in public areas where the information is vulnerable to theft.
- b. When transporting paper documents containing PHI, securing the documents in a briefcase, backpack, box, or other transportation container that conceals the documents and prevents others from seeing the content of the documents.
- c. When transporting electronic media that contain or that can be used to access PHI/ EPHI, such as computers, smart phones, and USB memory devices, securing the media in a briefcase, backpack, purse, or pocket in a manner that conceals the device and prevents it from being mislaid.

15.0 Logoff or lock the system when leaving a workstation unattended so that it prompts for a password upon return to the workstation. Instructions for locking your workstation: press the Windows key and the L key at the same time.

16.0 Disposal or reuse of media containing ePHI must follow the CMU Disposal or Transfer of Computers and Other Digital Assets Policy #3-12. https://www.cmich.edu/office_president/general_counsel/Documents/p03012.pdf.

17.0 Only use the CMU approved vendor SHRED bins to dispose of paper PHI.
- a. Do not put printed PHI into trash or recycle bins.
- b. Recycle bins are not permitted in clinics or CMU areas that are subject to HIPAA regulations.

18.0 Keys and key fobs to areas that contain PHI shall only be given to authorized workforce members.
19.0 Areas with paper files containing PHI, are kept in locked rooms and if necessary locked file cabinets.
20.0 Reasonable precautions are taken to ensure that records containing PHI are not left out in the open or unattended.
21.0 Records containing PHI may only be printed within the secured areas of the Hybrid units and on approved printers.
22.0 Have dedicated fax machines to receive PHI that may be faxed to the Hybrid units. Fax machines must be located in a secure area accessible only to authorized persons.
23.0 Computer monitors with access to medical records and protected health information are situated so that they are not easily visible to the public.
24.0 Archived paper medical records are stored in a locked storage area when not in use and are not stored directly on the floor.
25.0 Only workforce members who have need for keys will have keys to the cabinets or offices containing medical records.
26.0 Adhere to all CMU HIPAA Policies-know where they are on the CMU HIPAA website HIPAA.cmich.edu
27.0 Adhere to all CMU OIT policies-know where they are on the CMU OIT website. https://www.cmich.edu/office_provost/OIT/About/Policies/Pages/default.aspx.
28.0 Access to PHI/ePHI is restricted to individuals when it is a required part of a workforce members job duties and as described in HIPAA Workforce Security Access Management Policy #12-8.
29.0 Know and apply the Minimum Necessary Rule when accessing or disclosing PHI/ePHI.
30.0 Business Associate Agreements must be established as per HIPAA regulations.
31.0 A Workforce member is expected to apply the same confidentiality principles in remote locations as apply in the office.
32.0 PHI/ePHI is only disclosed to those who are authorized to receive the PHI/ePHI.
33.0 If it is necessary to discuss PHI/ePHI in a public location, individuals are to take reasonable efforts to protect others from overhearing the conversation.
    a. Telephone calls relating to PHI must be made in a private location where others cannot overhear the conversation. Wireless, cellular and cordless telephones shall be used for communicating PHI only if no other means of communicating is available and the communication is necessary at the time to complete a work-related function.
34.0 Records shall be scanned by trained staff only, and follow scanning procedures that include a quality check procedure.
35.0 Adhere to CMU record retention policy, including the need to obtain certification of destruction of records when applicable.
36.0 PHOTOS and MEDIA allowed only with written authorization on a HIPAA approved authorization form.
37.0 Workforce members must not post about patients or work on social media.