Title/Subject: **HIPAA: SAFEGUARDS**

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

Effective Date of This Revision: September 23, 2011

Contact for More Information:

HIPAA Privacy Officer
Plan Administrator
Rowe Hall 108
989.774.3661

Health Services Director
Foust Hall 249
989.774.3944

Carls Center Director
College of Health Professions
989.774.6624

☐ Board Policy ☒ Administrative Policy ☒ Procedure ☐ Guideline

---

BACKGROUND

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

PURPOSE

CMU has adopted this policy to comply with HIPAA and the privacy regulations, as well as to fulfill its duty to protect the confidentiality and integrity of confidential protected health information as required by law. This policy documents the most significant physical, administrative and technical safeguards followed by the units within Central Michigan University that make up the Hybrid Entity subject to HIPAA.

POLICY

I. Safeguards Followed by CMU Units that perform business associate functions.

The following safeguards apply to all units of the Hybrid Entity that fulfill a role similar to that of a business associate to the covered entity functions. These units include: Student Account Services & University Billing, Internal Audit, Office of General Counsel, Risk Management and Insurance, Faculty Personnel Services, Employee Relations, Human Resources, and Information Technology.

Authority: G.E. Ross, President
History: No Prior History
Indexed as: HIPAA Safeguards; HIPAA Protected Health Information

Administrative Safeguards

- Limiting use and disclosure of PHI to the minimum necessary for the intended purpose
- Training of workforce members on the Policies and Procedures

Technical Safeguards

- Restricting access to PHI on its computer systems to individuals who need to access PHI in order to perform their duties
- Using passwords to authenticate an individual's right to access PHI

Physical Safeguards

- Paper files containing PHI are kept in locked file cabinets
- Only employees with responsibilities requiring access to PHI will have access to records containing PHI; employees who do not have responsibilities requiring access to PHI are not given access to records containing PHI
- Reasonable precautions are taken to ensure that records containing PHI are not left out in the open or unattended

The following safeguards apply more specifically to those listed role within the Hybrid Entity.

II. Benefits and Wellness Department Safeguards

The Benefits and Wellness Department uses the following safeguards to protect PHI associated with the self-funded health benefit components of the Central Michigan University Flexible Benefits Plan.

Physical Safeguards:

- Benefits Department workforce members work in an area that is physically separate from other Human Resource workforce members. Computer monitors with access to health plan information are situated so that they are easily visible only to Benefits Department workforce members. Discussions between Department workforce members cannot easily be overheard by other Human Resource workforce members who are not part of the Benefits Department.
- The Benefits Department has its own paper filing area, which is locked when the Benefits Department employees are not present.

- The Benefits Department has private conference rooms available for confidential discussions with employees.
- Benefits Department workforce members monitor who enters into the Benefits Department area and will redirect people who do not belong in that department to other areas.
- the Benefits Department has kiosks available that employees can use to access their health plan information.
- the Benefits Department has a dedicated fax machine used to receive PHI that may be faxed to the Benefits Department.
- Paper records, when no longer needed, are disposed of in secure bins and ultimately shredded.

Administrative Safeguards

- Benefits Department workforce members are trained on HIPAA confidentiality requirements and CMU's HIPAA policies and procedures. Workforce members must successfully complete training before they are given access to PHI.
- Enrollment information is captured and maintained in SAP. CMU does not combine this information with claims information or other health plan records. Thus, the information is maintained as employment records and is not PHI. Functions such as payroll processing, compensation analysis, and assisting CMU employees with enrollment questions rely upon the SAP system and do not require access to PHI.
- The Benefits Department tries to limit the amount of PHI that it handles. Typically, Benefits Department workforce members encounter PHI when assisting CMU employees with health plan coverage or claims questions and in administering the wellness program.
- CMU has business associate agreements with third-party administrators and other service providers involved in the administration of the self-funded health plan benefits offered through the Central Michigan University Flexible Benefits Plan.
- The Benefits Department generally does not involve itself in claims administration or claims appeals. These functions are generally performed by insurers and third-party administrators, who maintain their own claims and claims appeals records. The exceptions to this general rule are that the Benefits Department handles second-level claims appeals of dental benefits and the administration of wellness program benefits. The Benefits Department limits the individuals who are involved in these processes and keeps these records confidential.
- Human Resources seeks to limit information received from insurers and TPAs to aggregate, de-identified information.
- CMU uses a service provider for wellness coaching services and to provide aggregate, de-identified information about participant health issues.

- When making decisions about plan performance, plan design, employee contributions and COBRA premiums, Human Resources management will use only aggregate, de-identified information.
- When insurance or administration contracts are renewed, de-identified information or summary health information necessary for obtaining bids is communicated directly from current insurers/administrators to the insurers/administrators bidding to provide the coverage/services.
- In connection with the wellness program, CMU employees will sometimes submit to the Benefits Department medical reports or other documents with detailed PHI to demonstrate that the employee has satisfied wellness program requirements. The Benefits Department will use these medical reports only to record the fact that requirements have been satisfied and will then destroy the documents.

Technical Safeguards

- Benefits Department workforce members and IT staff with access to electronic PHI are trained on HIPAA security rule requirements as set forth in CMU HIPAA security rule policies and procedures.
- Health Plan records are stored in secure folders on a Human Resources-dedicated server, with access limited to Benefits Department employees.
- When a TPA or insurer provides reports that contain individually identifiable health information, the report is downloaded from the TPA or insurer using a secure messaging system or a secure connection. The reports are stores in a secure folder on the Human-Resources-dedicated server with access limited to Benefits Department workforce members.
- Generally, reports received from a TPA or insurer contain only aggregate information without individually identifiable health information. If a report does contain individually identifiable health information, the Benefits Department will not access the full report, but will only run programs to cull aggregate data from the report. Reports that contain individually identifiable health information are deleted from the system at least on a quarterly basis.

III. University Health Services

University Health Services uses the following safeguards to protect PHI associated with the health care services that it provides.

Physical Safeguards:

- University Health Services ("UHS") policy is only those individuals requiring access to the records to fulfill their job functions will have access to records containing PHI.
- UHS workforce members work in an area that is physically separate from other departments. The front doors to the records area, pharmacy, and clinic are all locked, accessible only by key fob. An individual's key fob is either returned or immediately deactivated when that individual no longer needs access to UHS.
- Computer monitors with access to medical records and protected health information are situated so that they are easily visible only to UHS workforce members. Discussions between UHS workforce members or workforce members and patients will be conducted in a way so that they cannot easily be overheard by others.
- UHS has its own locked paper filing area for medical records. The office is accessible only to an individual who has been trained regarding the Privacy Rule and verified as having an employment responsibility requiring access to PHI.
- Archived paper medical records are stored in a locked storage area when not in use.
- UHS has private conference rooms available for confidential discussions with patients and employees.
- UHS workforce members monitor who enters into the UHS area and will redirect people who do not belong in that department to other areas.
- UHS has a dedicated fax machine used to receive PHI that may be faxed to the Department.
- Paper records, when no longer needed, are disposed of in secure bins and ultimately shredded. UHS' policy is that prior to sending records off site to be destroyed UHS will have entered into a business associate agreement with the certified destruction service that has been approved by the Office of Legal Counsel. CMU will receive a certificate of destruction each time the outside agency picks up and destroys materials.
- Buildings and grounds, security and telecommunications personnel may have limited access to UHS facilities. Such personnel will not have access to documents stored in locked filing cabinets.
- Only UHS employees who have need for keys will have keys to the cabinets or offices containing medical records.

Administrative Safeguards

- UHS workforce members are trained on FERPA and HIPAA confidentiality requirements and CMU's HIPAA policies and procedures. Workforce members must successfully complete training before they are given access to PHI.
- CMU has business associate agreements with service providers involved in the provision of services ancillary to UHS, including medical record software, servicing equipment and disposal services. UHS policy is that any outside provider who may have access to

medical records must enter into a HIPAA-compliant business associate agreement with CMU and agree to operate in conformance with the Privacy Rules before any services may be provided to UHS.

- When making decisions about resource utilization, appointment scheduling optimization and wellness programs, UHS management will use only aggregate, de-identified information.
- When vendor contracts are renewed, only de-identified information or summary health information necessary for obtaining bids is provided to vendors bidding for services.

Technical Safeguards

- UHS workforce members and IT staff with access to electronic PHI are trained on HIPAA security rule requirements as set forth in CMU HIPAA security rule policies and procedures.
- Medical records are stored in the Patient Care Management System or in secure electronic folders on a UHS-dedicated server, with access limited to UHS employees.
- When an outside physician or insurer provides reports that contain individually identifiable health information, the report is downloaded from the physician or insurer using a secure messaging system or a secure connection. The reports are stores in a secure folder on the UHS-dedicated server with access limited to UHS workforce members.
- Generally, reports received from outside vendors contain only aggregate information without individually identifiable health information. If a report does contain individually identifiable health information, UHS will file it appropriately in an individual's medical record.

IV. The Carls Center for Clinical Care and Education

The Carls Center is a multidisciplinary clinic that includes several different services – Audiology; Physical Therapy; Psychology; Speech Language Pathology; Driving Evaluation, Education, and Research; and a Fall and Balance Clinic. The Carls Center, in providing services, oversees records imaging, storage, retention, and destruction. These records are in a variety of media, including electronic, film, video, and paper. Among other things, the Carls Center maintains health records that include PHI. The Carls Center has a variety of full-time employees, staff, and students that access the medical records stored within the Carls Center. All Carls Center workforce members will receive appropriate training on CMU's HIPAA policies and procedures. To the extent that the Carls Center stores records for other departments or programs within Central Michigan University, the Carls Center will store those records consistent with HIPAA.

Physical Safeguards:

- Individuals will only access records needed to fulfill their duties. The Carls Center maintains a list of the classes of persons within the Carls Center and the purposes for which PHI is routinely available to that class.
- All current paper medical records are stored in the medical records office. The medical records office is only accessible by key fob to workforce members who have been trained regarding the Privacy Rule and verified as having an employment responsibility requiring access to PHI.
- Archived medical records are stored in a locked storage area when not in use. Access to the archived paper medical records is limited to those individuals who need access to fulfill their job duties.
- Electronic medical records may only be printed within the secured areas of the Carls Center.
- As part of the education and training mission of the Carls Center, some treatment sessions may be tape recorded. All patients are notified prior to being recorded and are given the opportunity to withhold their consent to being recorded. Videotapes are stored within the secured areas of the Carls Center.
- All fax machines are located in the medical records office. Any faxes received containing PHI are treated in the same manner as current paper medical records.
- The Carls Center places secured lockboxes within the medical records office and throughout the Carls Center. Individuals are instructed that any documents containing PHI are to be disposed of in the lockboxes. The Carls Center uses a document destruction service to destroy those documents. The Carls Center has a business associate agreement with the destruction service that has been approved by the Office of

General Counsel. CMU will receive a certificate of destruction each time the outside agency picks up and destroys materials.

- the front door leading into the Carls Center will have a lock, accessible only by key fob. The key fob must be used outside normal business hours. An individual's key fob will either be returned or deactivated when that individual no longer needs to access the Carls Center.
- Carls Center employees will remain alert to the presence of any unauthorized individual in restricted areas who are not accompanied by a Carl Center workforce member.
- The Medical records office will be locked if no one is present.
- The cabinets containing medical records will be locked every night.
- Scanning projects will be conducted in a locked room
- At the end of each day, the lead medical records office employee will do a final walk-through to ensure that all files are locked up
- Some buildings and grounds, security, and telecommunications personnel may have access to the Carls Center. Such personnel will not have access to documents stored in locked filing cabinets
- Only Carls Center employees who have need for keys will have keys to the cabinets or offices containing medical records
- Videotape recordings of treatment sessions will be stored within the Carls Center and accessed only by Clinical Faculty and Clinical Graduate Students involved in the treatment of the patient appearing on the videotape.

Administrative Safeguards

- The Carls Center trains its workforce members on the Privacy Rules requirements. All Carls Center workforce members who encounter PHI will keep the information confidential.
- The Clinical Manager also determines level of access for Clinical Supervisors and Clinical Faculty to the electronic medical records.
- The Carls Center may use various outside service providers for software support, servicing equipment, and disposal services. Before any outside service provider will have access to medical records, the service provider must enter into a HIPAA-compliant business associate agreement with CMU and operate in conformance with the Privacy Rules.
- Research requests submitted by the Office for Research and Sponsored Programs, if the research requires access to PHI housed in the Carls Center, must be approved by the Clinical Manager. The Clinical Manager will confirm that any individuals that access

PHI as part of the research study have received appropriate HIPAA training and that all disclosures are done in accordance with HIPAA.

Technical Safeguards

- Electronic medical records may be stored in the ImageNow database, in the Patient Care Management System, or in electronic folders within the Carls Center Network. All electronic files are stored in a secured, password protected drive accessible only from the Carls Center.
- IT staff will grant a workforce member access to the electronic medical records only if that person has successfully completed the appropriate HIPAA training.
- Clinical Student must also complete HIPAA training, and will then be given access rights to certain folders based on input from the Clinical Supervisor.