Title/Subject: **HIPAA: Use and Disclosure of Protected Health Information**

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

Effective Date of This Revision: November 27, 2012

Contact for More Information: HIPAA Chief Privacy Officer
Associate Dean/Administration & Finance
College of Medicine
989-774-7547

☐ Board Policy ☒ Administrative Policy ☒ Procedure ☐ Guideline

---

**PURPOSE:**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) granted certain rights to patients/clients/employees regarding their protected health information (PHI). This policy has been drafted to assist CMU to comply with the law and to guide CMU staff in assisting patients/clients/employees to exercise their rights.

**DEFINITIONS:**

The 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. Minimum Necessary is not defined in the Privacy Rule, but is a term used to describe the amount of PHI needed to perform a particular task or function.

**Business Associate**: A "business associate" is a person (other than a member of CMU's workforce) or entity that arranges, performs or assists in the performance of functions or activities involving the use or disclosure of PHI. Such functions include:

- claims processing or administration;
- data analysis, processing or administration
- utilization review
- quality assurance
- billing
- benefit management
- any other function or activity regulated by the Privacy Rules

A business associates also includes a person or entity that provides the following types of services, if the services involve the disclosure of PHI:

- legal
- actuarial
- accounting

---

Authority: M. Rao, President
History: 4-6-2005; 9-23-11
Indexed as: HIPAA:Use and Disclosure of Protected Health Information; HIPAA: Protected Health Information: HIPAA: Disclosure of Protected Health Information

- consulting
- data aggregation
- management
- administrative
- accreditation
- financial services
- software and technology support

**Designated Record Set**: "Designated record set" means the enrollment, payment, claims adjudication and other records that are maintained by health care providers or the Health Plan but excluding enrollment information found in CMU's employment records. It includes Health Plan records that are maintained on behalf of the Health Plan by a third party that performs services for the Health Plan and medical records that CMU's health care providers receive from other health care providers. It also includes Health Plan records or medical provider records that may be used, in whole or in part, by or for the Health Plan to make decisions about an individual. For purposes of this definition, "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for the Health Plan or one of CMU's health care providers. The Designated record set does not include records that are created by students or for the assessment of students. Records created by students or for the assessment of students are education records subject to FERPA, but are not part of the Designated record set and are not subject to HIPAA.

**De-identified Information**: Information qualifies as "de-identified information" only if it does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. PHI can become de-identified in two ways:

- professional statistical analysis has determined that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the information; or
- the following identifiers of the individual or of relatives, employers, or household members of the individual, are removed and CMU does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information:
    - Names;
    - All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
        - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
        - ( 2 ) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
    - All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all

elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section

**Disclosure**: "Disclosure" of PHI means the release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within the Hybrid Entity.

**Health Care Operations**: "Health care operations" means any of the following activities to the extent that they are related to Health Plan administration or the provision of health care:

- evaluating Health Plan performance
- underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits
- ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance)
- conducting quality assessment and improvement activities
- conducting or arranging for medical review, legal services, and auditing functions
- business planning and development
- business management and general administrative activities

- conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination

- reviewing the competence or qualifications of health care professionals, evaluating provider performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities

**Limited Data Set**: A Limited Data Set is PHI that has had most identifiers of the individual, or of relatives, employers, or household members removed from it. A Limited Data Set is similar to De-identified Information (see above), except that a Limited Data Set may include city, state and zip code information and any dates related to an individual. Limited Data Set is further defined at 45 C.F.R. § 164.514(e).

**Minimum Necessary**: The Privacy Rules require that when PHI is used or disclosed, CMU must make reasonable efforts to limit the use or disclosure to the minimum amount necessary to accomplish the intended purpose of the use, disclosure or request. For example, if someone asks for an individual's Health Plan records in order to perform a function on behalf of the Health Plan, but the records include more information than is really needed for that function, CMU should only disclose the information needed (and not the entire record).

**Payment**: "Payment" means activities undertaken to obtain Health Plan premiums, insurance copayments for health care providers, or to determine or fulfill the Health Plan's responsibility for coverage and provision of benefits, or to obtain or provide reimbursement for the provision of health care. Payment includes:

- determinations of eligibility or coverage, including coordination of benefits or the determination of cost sharing amounts

- adjudication or subrogation of health benefit claims

- risk adjusting amounts due based on enrollee health status and demographic characteristics

- billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing

- review of health care services for purposes of determining coverage

**Use**: "Use" of PHI means the sharing, employment, application, utilization, examination or analysis of individually identifiable health information by any person working for, in connection with, or within CMU's Human Resources Department, The Carls Center for Clinical Care and Education, the College of Health Professions, University Health Services, Student Account Services & University Billing, Internal Audit, the Office of General Counsel, Faculty Personnel Services, Risk Management, Information Technology or by a business associate.

**Workforce/Employee**: CMU's workforce includes any individual who works directly under the control of CMU, whether or not they are paid by CMU. This includes not only employees, but also volunteers, trainees, interns/externs, workers employed by a temporary agency, and independent contractors. Whenever these policies and procedures discuss CMU's obligation to protect PHI, the discussion is intended to include anyone who is a member of CMU's workforce. The term "employee," when used in these polices and procedures, means any member of CMU's workforce.

**POLICY:**

CMU shall take reasonable steps to limit the uses, disclosures of, and requests for PHI to the minimum necessary to accomplish the intended purpose.

CMU shall maintain policies and procedures that identify persons or classes of persons within CMU and its business associates who need access to PHI to carry out their job duties, and the purposes for which PHI may be used.

The minimum necessary provisions contained in this policy and procedure do not apply to the following:

a. Disclosures to or requests by a health care provider for treatment purposes

b. Uses and disclosures to the patient/client/employee who is the subject of the information

c. Uses or disclosures made pursuant to an authorization provided by a patient/client/employee

d. Uses or disclosures required for compliance with the standardized HIPAA transactions

e. Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the rule for enforcement purposes

f. Uses or disclosures that are required by other law

h. Uses or disclosures that are required for compliance with the Privacy Rules

These policies and procedures are for CMU internal uses and disclosures. Uses and disclosures by third party administrators and/or service providers are governed by that party's business associate agreement with CMU and its own internal policies and procedures.

**PROCEDURE:**

**1.0 Use of PHI by CMU Units.**

CMU recognizes that a number of persons and groups of persons need access to some level of PHI to carry out their job duties. The Privacy Officer for each unit of the Hybrid Entity shall maintain a list of the classifications of personnel (including student clinicians/interns and volunteers) approved to have routine access to PHI in the performance of their duties ("Authorized Employees"). These Authorized Employees may use and disclose PHI to perform their job functions, and they may disclose PHI to other Authorized Employees who perform or support Health Plan administration functions or provide health care. Such uses and disclosures, however, must be limited to the minimum necessary to perform or support their job functions. Routine uses and disclosures must be made in accordance with these policies and procedures. Non-routine uses and disclosures must be approved by the appropriate Privacy Officer.

Student Account Services & University Billing: Employees in this unit of the university may have access to PHI to the extent necessary to fulfill their responsibilities. For example, this office may handle billing and collections for University Health Services or the Carls Center for Clinical Care and Education, and The Psychological Training & Consultation Center. The records to which this unit would have access are limited to those related to billing and usually include only personally identifying information (name, identifying numbers, address, telephone number), amount owed, date of service, general statement of service rendered, unit of University rendering service. All employees in Student Account Services & University Billing and student services advisors may have access to those records.

Internal Audit: Employees in this unit of the university may have access to PHI to the extent necessary to fulfill their responsibilities. For example, if an employee or unit of the university is accused or suspected of violating certain HIPAA and University policies regarding the security and privacy of PHI, this office may be involved in reviewing systems and safeguards, both in order to assess what occurred in the past and to recommend changes in the future. Also, this office may audit an area with PHI, such as Health Services or the Speech-Language Pathology and Audiology Clinics, to determine, among other things, if HIPAA regulations, as well as departmental or university policies and procedures, are being followed. In the process of conducting these reviews, the office may have access to PHI on employees, clients or patients. The Director and auditors would have primary access to those records needed to conduct the review. The support staff in that office might have some access to those records in order to assist (e.g., setting up and organizing the file; putting the file away and retrieving it, preparing letters, typing witness notes, etc.).

General Counsel: Employees in this unit of the university may have access to PHI to the extent necessary to fulfill their responsibilities. For example, the attorneys and legal assistant may be consulted about the application of HIPAA rules and University policies to specific situations where PHI must be disclosed to the attorneys or legal assistant in order to obtain legal advice. Employees may also handle PHI in order to respond to a subpoena, a discovery request or a court order requesting PHI. Also, if a faculty member or staff is accused or suspected of violating HIPAA and University policies regarding PHI, this office would provide advice in conducting an investigation and, if necessary, disciplining the employee. This office would be involved in handling allegations of violations of HIPAA by the University itself or its employees, if a complaint were filed with an outside administrative agency or court. Employees may also provide legal guidance to CMU Health Plans that may require access to PHI, such as issues relating to whether certain claims are covered by the Plans. The support staff in that office might have access to those records in order to assist (e.g., setting up and organizing the file, putting the file away and retrieving it, preparing correspondence, typing notes, etc.).

Risk Management and Insurance: Employees in this unit of the university may have access to PHI to the extent necessary to fulfill their responsibilities. For example, the employees may be consulted about specific situations where PHI must be disclosed in order to obtain an accurate assessment of legal and financial risk to the University. Also, if a student, faculty member, staff or guest is injured on campus, this office would provide advice in conducting an investigation and, if necessary, obtaining medical care on behalf of the injured person. This office would work with General Counsel to determine the risk of litigation and settlement strategy, if a complaint were filed with an outside administrative agency or court. The support staff in that office might have access to those records in order to assist (e.g., setting up and organizing the file, putting the file away and retrieving it, preparing correspondence, typing notes, etc.).

Faculty Personnel Services: Employees in this unit of the university may have access to PHI to the extent necessary to fulfill their responsibilities. For example, if a faculty member is accused or suspected of violating HIPAA or University policies regarding PHI, this office would be involved in conducting an investigation and, if necessary, disciplining the employee. The Director and Assistant Directors of Faculty Personnel Services would have primary access to those records needed. The support staff in that office might have some access to those records in order to assist (e.g., setting up and organizing the file; putting the file away and retrieving it, preparing letters, typing witness notes, etc.). Faculty Personnel Services may also receive inquiries from employees about claims payment issues, but will refer those requests to the Benefits and Wellness department.

Benefits and Wellness: Employees in this unit of the university administer the self funded health plans, and they may have access to PHI of employees and their dependents to the extent necessary to fulfill their responsibilities. For example, they handle requests from employees relating to benefit claims, decide second-level claims appeals for certain self-funded benefits

programs, determine whether employees have met wellness program requirements, and receive detailed reports from third party administrators for Health Plan evaluation and design purposes. Employees may also be involved in investigating complaints or data breaches relating to the self-funded health plans. All employees of this unit will have access to PHI maintained by the unit.

Employee Relations, Human Resources: Employees in this unit of the university may have access to PHI to the extent necessary to fulfill their responsibilities. For example, if an employee is accused or suspected of violating HIPAA and University policies regarding PHI, this office would be involved in conducting an investigation and, if necessary, disciplining the employee. The Director of Employee Relations and HR Consultants would have primary access to those records needed to conduct the investigation or discipline process. The support staff in that office might have some access to those records in order to assist (e.g., setting up and organizing the file; putting the file away and retrieving it, preparing letters, typing witness notes, etc.). Employee Relations also provides technical support for Benefits & Wellness IT Systems that use PHI, and may access PHI as reasonably necessary to provide such support.

University Health Services: University Health Services provides clinical services to University students, faculty, staff and members of the local community. Its employees may have access to PHI to the extent necessary to fulfill their responsibilities. For example, the receptionist will assist patients with insurance and appointments; physicians, nurses and other health care providers have access to the full medical record in order to provide treatment; laboratory staff will have access to the laboratory order and report information. Specific access will be permitted for each position as required to facilitate the treatment, payment and health care operations of the department. as permitted by HIPAA.

The Carls Center for Clinical Care and Education: The Center provides clinical services through several specialty clinics. Currently included are the Speech-Language Pathology and Audiology Clinics, the Driving Evaluation and Education Research Center, the Fall and Balance Center, the Psychological Training and Consultation Center and Physical Therapy Clinics. The Carls Center provides centralized scheduling and billing and other support services for each of these specialty clinics through the use of the Patient Care Management System (PCMS), and its employees may have access to PHI to the extent necessary to fulfill their responsibilities The specialty clinics also provide training for students in the College of Health Professions and the College of Humanities and Social and Behavioral Sciences, including supervised interaction of students with patients in clinical settings.

Information Technology: The Information Technology unit of CMU provides technical support for information systems that maintain PHI on behalf of the health care components that make up the CMU Hybrid Entity. Employees of this Unit may access information as necessary to maintain the proper functionality of the relevant information systems. Employees may also access information as necessary to ensure the confidentiality, integrity and accessibility of PHI consistent with the HIPAA Security Rule; to investigate complaints, security incidents and suspected breaches; and as reasonably necessary to document and demonstrate compliance with HIPAA requirements.

Business Associates: The Business Associates of units within the Hybrid Entity may have access to PHI as described in the Business Associate Agreements.

**2.0 Use, Disclosure and Requests for entire medical record.**

CMU will not use, disclose or request an entire medical record, except as allowed by 1.0 above, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request. In general, few members of the CMU workforce will have access to an entire clinical record.

Physicians, physician assistants, nurse practitioners, health information specialists, licensed and unlicensed therapists, and student clinicians/interns will be authorized to review an entire clinical record. Such access will be limited to the records of patients/clients/employees with which the professional has a current therapeutic relationship or for whom a professional consultation has been requested. Access to the entire clinical record of these patients/clients/employees has been determined to be critical to the continuity of the patient's/client's/employee's care as well as essential to diagnosis, treatment selection and the health and safety of the patient/client/employee and others.

Supervisory staff of CMU health care providers and student clinicians will also have full access to the entire medical record. This is necessary in order to evaluate health care provider/student clinician performance and ensure that CMU health care components provide health care consistent with community standards.

## 3.0 Routine Disclosures of and Requests for PHI.

CMU recognizes that the need for information varies according to the duties performed by the party obtaining the information. Routine disclosures and requests are those that do not require individual review or analysis by a Privacy Officer of the purpose and amount of information necessary before a disclosure/request may be made.

Each unit of the CMU Hybrid Entity shall maintain a list of the classes of persons within the workforce and the purposes for which PHI is routinely available to that class. The list shall be developed by taking into account the following characteristics:

- *The type of PHI to be used or disclosed,*
- *The types of persons who will use or who will receive the disclosure,*
- *The conditions that will apply to the use or disclosure, and*
- *The purpose for which the PHI will be used or disclosed.*

Workforce members will be trained on minimum necessary requirements relating to these routine uses and disclosures of PHI.

### 3.1 Routine Uses and Disclosures by The Carls Center for Clinical Care and Education.

The following are routine uses and disclosures of PHI by Carls Center workforce members:

- use of PHI by Clinical Supervisors, Clinical Faculty, and Clinical Students for purposes of treatment and training within the Carls Center and to coordinate care with other health care providers.
- documenting and management of patient files and insurance information for record keeping, reimbursement, billing, collection activities, obtaining insurance precertification, scheduling, archiving, and academic integrity purposes.
- conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines.
- reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, peer review, training programs, accreditation, certification, licensing and credentialing activities.

- for public health activities, for workers compensation and similar programs, and to coroners, medical examiners and funeral directors.
- arranging for legal services and auditing functions, including fraud and abuse detection and compliance programs
- business management and general administrative activities for the Carls Center, business planning and development activities, fundraising for the Carls Center, customer service, and resolution of internal grievances and complaints.
- information technology support within the Carls Center for medical imaging software, electronic medical records, electronic clinical equipment, billing and scheduling systems, and similar systems using PHI.
- complying with HIPAA requirements.

3.2 Routine Uses and Disclosures by University Health Services.

The following are routine uses and disclosures of PHI by University Health Services workforce members:

- use of PHI by clinical staff for purposes of treatment within University Health Services and to coordinate care with other health care providers.
- documenting and management of patient files and insurance information for record keeping, reimbursement, billing, collection activities, obtaining insurance precertification, scheduling, archiving, and academic integrity purposes.
- conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines.
- reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, peer review, training programs, accreditation, certification, licensing and credentialing activities.
- for public health activities, for workers compensation and similar programs, and to coroners, medical examiners and funeral directors.
- arranging for legal services and auditing functions, including fraud and abuse detection and compliance programs
- business management and general administrative activities for the Carls Center, business planning and development activities, fundraising for University Health Services, customer service, and resolution of internal grievances and complaints.
- information technology support within University Health Services for medical imaging software, electronic medical records, electronic clinical equipment, billing and scheduling systems, and similar systems using PHI.
- complying with HIPAA requirements

3.3 Routine Uses and Disclosures by CMU self-funded health plan components of the Central Michigan University Flexible Benefits Plan.

- The Central Michigan University Flexible Benefits Plan is administered by the CMU Human Resources Department, relying upon contracts with insurers and third-party administrators for claims administration.

For the limited amount of PHI that the Human Resources Department handles, the following are routine uses and disclosures by Human Resources Department workforce members:

- assisting participants and beneficiaries with questions relating to health plan benefits, appeals and other inquiries and related discussions with insurers and third-party administrators.
- administration of wellness program benefits, including the determination of whether individuals have met requirements to receive incentive benefits.
- making second-level appeals decisions for the self-insured dental program
- responding to requests from Medicare Secondary Payer Contractors.
- working with legal counsel relating to the administration of the self-funded health plan components and HIPAA compliance issues.
- auditing functions relating to the operation of the self-funded health plan components and HIPAA compliance issues.
- for those insurers/TPAs who provide reports containing individually identifiable health claims information, aggregating data to be used for plan evaluation, plan design, and setting employee contributions and premiums.
- information technology support for Human Resources systems that use or store PHI.
- complying with HIPAA requirements.

## 4.0 Non Routine disclosures and requests.

All non-routine disclosures will be reviewed by the privacy officer for the unit of the Hybrid Entity that houses the information in order to determine that the disclosure is permissible and complies with the minimum necessary standard, in accordance with criteria contained in section 5.0 below.

## 5.0 Determining the Minimum Necessary – Use and Disclosure Criteria.

CMU's criteria for evaluating whether a use or disclosure is limited to the minimum necessary to accomplish the intended purposes are:

- the type of PHI needed for the particular use or disclosure
- whether disclosures and uses are to the persons or class of persons who need access to the information to carry out their job duties
- whether the use is for treatment, payment or health care operations, or is made pursuant to a valid authorization by the individual, or otherwise allowed under HIPAA
- whether the recipient has clearly stated the purpose for the request, use or disclosure of the PHI and has the authority/right to receive the requested information.
- Whether additional privacy restrictions apply (such as FERPA)

- whether the task can be accomplished with less information
- whether, under the circumstances, the use or disclosure seems to be reasonably necessary and appropriate
- the risk that the use or disclosure will result in an unauthorized use or disclosure of the PHI
- whether the use or disclosure is to another unit within the CMU Hybrid Entity, or some other unit of CMU that is not subject to these HIPAA policies.
- whether CMU has agreed to an additional restriction on the use or disclosure of PHI that would be violated by the use or disclosure

If the disclosure will be to a third party authorized to receive PHI, CMU will use the same criteria as above to determine whether the information to be disclosed is limited to the minimum necessary to accomplish the intended purposes. Examples of third parties include:

- a public official or agency for a permitted disclosure of PHI for legal or public policy purposes
- a professional who is an employee of a unit within the CMU Hybrid Entity.
- a professional or other service provider of CMU for the purpose of providing services to CMU that requires use of PHI, where the service provider has entered into a valid HIPAA business associate agreement with CMU; or
- a researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board

## 6.0 Mandatory Disclosures of PHI to Individuals and HHS

**6.1** The Privacy Rules require CMU to disclose an individual's PHI when requested by the individual or, under certain circumstances, by HHS. CMU's policy is to cooperate with these requests and to disclose the PHI in accordance with the Privacy Rules.

**6.2** An individual (or the individual's personal representative) may request a disclosure of his or her own PHI. CMU will respond to such requests by following the procedures set forth in Policy 12-11 "Individual Rights."

**6.3** CMU will respond to a request from an HHS official for disclosure of PHI as follows:

- verify the identity of the HHS official using the procedures set forth in section 12.0 entitled "Verifying the Identity of Those Requesting PHI"
- document the disclosure as required under the Privacy Rules' documentation requirements and as explained in this Policy

## 7.0 Permitted Uses and Disclosures of PHI for Legal and Public Policy Purposes

From time to time, CMU may receive requests from courts, parties to litigation, law enforcement officials, public health authorities, or various other government agencies or officials to use or disclose an individual's PHI. The Privacy Rules set forth guidelines under which CMU may use or disclose PHI in such circumstances. CMU's policy is that CMU will respond to such a request only if the use or disclosure meets the following conditions:

- The Privacy Officer for the unit receiving the request approves the use or disclosure after consultation with the Office of General Counsel
- the disclosure complies with the minimum necessary standard or is specifically exempted from the minimum necessary standard
- the disclosure falls within one of the following categories, and the specific requirements set forth in the Privacy Rules have been followed (45 CFR § 164.512):
    - in response to an order of a court or an administrative tribunal
    - in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, provided that there is an appropriate protective order in place and, where medical records are involved, the individual has waived his or her physician-patient privilege
    - pursuant to process (such as a court-ordered warrant or an administrative summons) and as otherwise required by law
    - to a law enforcement official (1) about an individual who has died; (2) for identification and location purposes; (3) about an individual who is, or is suspected of being, a victim of a crime; or (4) about an individual relating to a crime on CMU premises
    - about an individual that CMU reasonably believes is the victim of abuse, neglect, or domestic violence, to a government authority, including a social service or protective service agency, that is authorized by law to receive such information
    - to appropriate public health authorities for public health activities
    - to a health oversight agency for health oversight activities
    - to coroners, medical examiners, and funeral directors about a deceased individual
    - for organ, eye or tissue donation purposes
    - for certain research purposes, when the need for an authorization has been waived or is otherwise not required
    - in order to avert a serious threat to health or safety
    - about armed forces personnel to appropriate military command authorities
    - for national security and intelligence activities
    - for protective services to the President of the United States and other designated persons
    - to correctional institutions and law enforcement custodians
    - in connection with workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault
- if the disclosure is to a public official, verify the identity of the HHS official using the procedures set forth in section 12.0 entitled "Verifying the Identity of Those Requesting PHI"

- check state laws for any additional restrictions on the right to use or disclose PHI. If the Carls Center or University Health Services receives a subpoena seeking information about a patient, CMU will not release the patient's medical records without an accompanying court order, administrative order, or patient's waiver of the physician-patient privilege

- document the disclosure according to the Privacy Rules' documentation requirements, except that documentation is not required if the disclosure is for:

  - national security or intelligence purposes; or

  - to correctional institutions or law enforcement custodians

## 8.0 Uses and Disclosures of PHI with an Individual's Authorization

**8.1** The Privacy Rules provide that unless expressly authorized by the individual who is the subject of the PHI (or the individual's personal representative), any use or disclosure of that individual's PHI is prohibited unless it falls within one of the categories for which disclosure is permitted or required. An individual may, however, expressly authorize a use or disclosure of PHI for any purpose.

**8.2** CMU's policy is that any use or disclosure made pursuant to an authorization will be made only if CMU: (1) determines that the authorization is valid (as described below); (2) verifies the identity of the individual who signed the authorization as described in this Policy; and (3) ensures that the use or disclosure is made consistent with the terms of the authorization.

**8.3** An authorization is valid only if it is written in plain language and contains the following required core elements and statements:

**8.3.1** In order to be valid, an authorization must contain all of the following core elements:

- a specific and meaningful description of the PHI to be used or disclosed

- the name or other specific identification of the person or class of persons authorized to use or disclose the PHI

- the name or a description of the person or class of persons to whom CMU may make the requested use or disclosure

- the purpose(s) of the requested use or disclosure. (If the individual initiates the authorization and does not provide a statement of purpose, the statement "at the request of the individual" is sufficient)

- a valid expiration date (e.g., December 31, 2012) or expiration event (e.g., termination from the Health Plan, rejection of an insurance application, etc.)

- the signature of the individual and the date the authorization was signed. (If signed by the individual's personal representative, a description of the representative's authority to act for the individual must also be provided)

**8.3.2** In order to be valid, an authorization must contain all of the following statements:

- a statement of the individual's right to revoke the authorization in writing, and either (1) a list of the exceptions to the right to revoke and a description of how the individual may revoke the authorization; or (2) a reference to the

Notice of Privacy Practices, if the Notice lists the exceptions to the right to revoke and provides a description of how the individual may revoke the authorization

- a statement informing the individual that CMU may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization; or the consequences to the individual if he or she refuses to sign the authorization when:
    - the authorization is to be used to for the Health Plan's eligibility or enrollment determinations or for its underwriting or risk rating determinations, and the authorization is not for the use or disclosure of psychotherapy notes; or
    - a covered entity will be providing health care solely for the purpose of creating PHI for disclosure to a third party and the authorization is to allow the disclosure to the third party (e.g., a physician releasing the results of pre-employment drug testing to CMU)

**8.4** If CMU is seeking the authorization from the individual, CMU must provide the individual with a copy of the signed authorization.

**8.5** An individual may revoke an authorization at any time, although the revocation will not be effective to the extent that CMU has previously used or disclosed information in reliance on the authorization.

**8.6** A copy of the authorization must be maintained as required under the Privacy Rules' documentation requirements as described in this Policy.

## 9.0 Uses and Disclosures by Business Associates

**9.1** The Privacy Rules require that before CMU may share PHI with outside service providers, the outside service providers must contractually obligate themselves to protect the PHI. CMU's policy is that it will not share PHI with a third party that performs services for a Hybrid Entity unit until that third party has entered into an agreement in which the party agrees to appropriately protect PHI.

**9.2** The Privacy Rules call these third parties that provide services to or on behalf of the Hybrid Entity "business associates." A copy of the business associate agreement must be maintained according to the Privacy Rules' documentation requirements as described in this Policy.

**9.3** CMU may provide PHI to a business associate under the following conditions:

- CMU has verified that a valid business associate contract is in place
- the disclosure is consistent with the terms of the business associate agreement
- the disclosure complies with the minimum necessary standard
- the disclosure is documented in accordance with the Privacy Rules' documentation requirements if it is for:
    - public health activities, except disclosures to report child abuse or neglect
    - judicial and administrative proceedings

- law enforcement purposes
- adverting a serious threat to health or safety
- military and veterans activities, the Department of State's medical suitability determinations, and government programs providing public benefits
- workers' compensation

**9.4** If CMU learns that a business associate has used or disclosed PHI in an unauthorized manner, CMU will take the following steps:

- the Privacy Officer for the unit that contracted with the business associate will promptly notify the business associate in writing of the alleged unauthorized use or disclosure
- the Privacy Officer for the unit that contracted with the business associate will telephone the business associate to discuss the alleged unauthorized use or disclosure and to determine whether the unauthorized use or disclosure will cease
- if the business associate does not agree to stop the unauthorized use or disclosure, if CMU learns that the use or disclosure has not stopped, or if the unauthorized use or disclosure is part of a pattern of conduct in violation of the business associate's agreement with CMU, then CMU will:
  - terminate its relationship with the business associate; or
  - if termination is not possible (for example, because there is no other entity in the area that can provide the service), then CMU will report the business associate to HHS
- the Chief Privacy Officer will document the known details of the unauthorized use or disclosure for purposes of responding to requests for an accounting of disclosures
- if appropriate, the Chief Privacy Officer will follow the procedures set forth in "Mitigation of Inadvertent Disclosures of PHI" in Policy 12-5
- the Chief Privacy Officer will follow the Breach Notification Policy contained in Policy 12-5.

## 10.0 Requests for Disclosure of PHI from Spouses, Family Members, and Friends

**10.1** Generally, CMU's health care providers will not disclose an individual's PHI to third parties, except as required or permitted under the Privacy Rules or as expressly authorized by the individual. The individual units of the Hybrid Entity may, however, allow disclosures to family members and close friends who are involved in the individual's care or payment for the individual's care, and the Hybrid Entity may do so after the individual is aware that such disclosures may be made, has had an opportunity to object to the Hybrid Entity's making such disclosure and has failed to object. If CMU is unable to notify the individual of the disclosure to family members and close friends, CMU may still disclose the information if the health care professional determines that the disclosure is in the individual's best interest. Additionally, if a spouse, family member, or friend accompanies an individual to his or her appointment with a health care provider, and the individual does not object to the presence of the spouse, family member, or friend during the appointment, CMU will consider that the individual has consented to the

health care provider sharing the PHI with the spouse, family member, or friend during that appointment.

**10.2** For requests by a spouse, family member or friend to access an individual's PHI in circumstances not governed by section 10.1, CMU will adhere to the following procedures:

**10.2.1** If a workforce member receives a request for a disclosure from a person claiming to be an individual's spouse, other family member, close friend, or personal representative, the workforce member must seek to verify that person's identity as set forth section 12.0 of this Policy.

**10.2.2** Once the identity of the person has been established, the workforce member should check health plan or medical records to determine if this person has been designated by the individual as being an authorized recipient of his or her PHI. If the person is not designated to receive the PHI , the workforce member may not make the disclosure except that either parent of a minor child may access the minor child's records absent a court order prohibiting such access.

**10.3.3** If the workforce member is unable to verify the identity or authority of the person, then no disclosure will be made unless the individual expressly authorizes it. If workforce member is uncertain whether disclosure is appropriate, the workforce member should contact the appropriate Privacy Officer.

## 11.0 Uses and Disclosures of De-Identified Information

**11.1** Under the Privacy Rules, health information from which all individual identifiers have been removed is called de-identified information, and can be used and disclosed without an individual's authorization . CMU's policy is that information must be approved by the appropriate Privacy Officer as de-identified information before it can be disclosed as such.

**11.2** CMU will use and disclose de-identified information only if the appropriate Privacy Officer has verified that the information is in fact de-identified, as set forth in the definitions section of this Policy. De-identified information is not PHI, so once the information has been approved as de-identified information, CMU may freely use and disclose the de-identified information.

## 12.0 Verifying the Identity of Those Requesting PHI

**12.1** The Privacy Rules require that CMU verify the identity and authority of persons or entities exercising their individual rights or otherwise seeking access to PHI. CMU's policy is to verify both the identity of such person or entity and the authority of the person or entity making the request (if the identity or authority is not known).

**12.2** CMU will disclose PHI in response to a request by the individual who is the subject of the PHI by using the following verification procedures:

**12.2.1** If the individual making the request is not known to the workforce member, the workforce member will take appropriate steps to verify the identity of the individual which may include making a copy of a valid photo identification issued by a government agency. When the workforce member has successfully verified the individual's identity, the workforce member will follow the applicable procedures set forth in Policy 12-11 "Individual Rights."

**12.2.2** If the individual requests PHI over the telephone and the workforce member is reasonably able to positively identify the individual over the telephone, the workforce member may provide the PHI as set forth in Policy 12-11 "Individual Rights." If the workforce member cannot identify the individual, the workforce member will instruct the individual to make the request in person, or direct the individual to send the request in writing.

**12.2.3** If the request from an individual originates by e-mail the individual should be informed that it is CMU's policy to provide PHI requested by e-mail only in paper form and only to the address on file. The individual may also be instructed to make the request in person, or should be directed to send the request in writing if delivery to an alternate address is requested.

**12.2.4** If the individual submits a written request for PHI:

- compare the information in the written request with information in the individual's Health Plan or medical records. If the information does not match, or if there is any doubt as to the identity of the person making the request, contact the appropriate Privacy Officer
- determine whether the person submitting the request has been designated in the Health Plan or medical record as an individual who is authorized to receive the PHI. If the workforce member determines that this is the case the request for PHI will be granted on a case by case basis
- file a copy of the request with the Health Plan or medical record of the individual whose records are being accessed, in accordance with the documentation requirements in this Policy
- follow the appropriate procedures set forth in Policy 12-11 "Individual Rights"

**12.3** CMU will respond to the request made by either parent seeking PHI of the parent's minor child using the following verification procedures:

- verify the identity of the person making the request following the procedures above for responding to a request by an individual
- verify the person's relationship with the child. The relationship may be verified by confirming enrollment of the child as a dependent in the Health Plan, for example
  - generally, a non-custodial parent will not be denied access to records or information concerning his or her minor child, unless prohibited by court order
- verify from the Health Plan or medical records that the child is a minor
- verify from the Health Plan or medical records that there is no restriction in place, such as a court order prohibiting release of information to the parent
- follow the appropriate procedures set forth in Policy 12-11 "Individual Rights"

In certain circumstances, CMU is prohibited by Michigan law from providing the medical record of a minor to the minor's parents. If the minor child has been emancipated; has received prenatal or pregnancy related health care; has received treatment for a venereal disease or HIV; or has received substance abuse related medical care, then CMU may not disclose the medical record without the minor's consent.

Additionally, if a minor child has obtained outpatient mental health services without the consent or knowledge of the minor's parents, the minor's parents shall not be informed of the services unless the mental health professional treating the minor determines that there is a compelling need for disclosure.

**12.4** CMU will respond to a request for an individual's PHI made by a personal representative of the individual using the following verification procedures:

- verify the identity of the person making the request using the procedures above for responding to a request by an individual
- verify the personal representative's authority to access the individual's record:
  - check the individual's file for a copy of a valid power of attorney, order of court, guardianship order, or similar documentation establishing the personal representative's authority. If there is a question as to the scope of authority conferred upon the individual, contact the Privacy Officer to review the document
  - if the file does not have such documentation:
    - obtain from the personal representative a copy of a valid power of attorney, order of court, guardianship order or similar documentation establishing the authority of the personal representative. If there is a question about the validity or sufficiency of the document, or the scope of authority conferred upon the personal representative, contact the appropriate Privacy Officer to review the document
    - verify that the personal representative has not been excluded from receiving PHI by the documentation in the individual's Health Plan or medical record
    - file a copy of the document in the individual's Health Plan or medical record according to the documentation requirements in this Policy
- follow the appropriate procedures set forth in Policy 12-11 "Individual Rights."
- A health care provider or unit of the Hybrid Entity may elect not to treat a person as the personal representative of an individual if the health care provider or unit of the Hybrid Entity:
  - has a reasonable belief that:
    - the individual has been or may be subjected to domestic violence, abuse or neglect by such person; or
    - treating such person as the personal representative could endanger the individual; and
  - in the exercise of professional judgment decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.
- In the event that a health care provider or unit of the Hybrid Entity decides not to treat a person as a personal representative, the health care provider or unit shall document and retain a clear statement explaining the basis for the decision.

**12.5** CMU will respond to a request for an individual's PHI made by a public official using the following verification procedures:

- verify that the request is for one of the purposes set forth above in the sections entitled "Mandatory Disclosures of PHI to Individuals and HHS" or "Permitted Uses and Disclosures of PHI for Legal and Public Policy Purposes"
- verify that the person is a public official or acting on behalf of a government agency:
  - if the request is made in person:
    - ask to see an agency identification badge, official credentials, or other proof of government status
    - make a copy of the identification provided, write on it the date of the request, and file it with the individual's Health Plan or medical record
  - if the request is in writing:
    - verify that the request is on appropriate letterhead
    - make a copy of the writing and file it with the individual's Health Plan or medical record
  - if the request is by a person purporting to act on behalf of a public official:
    - establish that the individual is acting on behalf of the public official, which may be established by one of the following documents:
      - a written statement on appropriate government letterhead that the person is acting under the government's authority
      - a contract for services with the government agency
      - a memorandum of understanding with the government agency
      - a purchase order with the government agency
    - make a copy of the document and file it with the individual's Health Plan or medical record
  - if there is any question as to the person's identity or affiliation with the government agency, contact the appropriate Privacy Officer
- verify that the person is authorized to access the PHI:
  - request a written statement setting forth the legal authority under which the information is being requested
    - if under the circumstances a written statement would be impracticable, obtain an oral statement of such legal authority (and document the oral statement)
    - if the request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact the appropriate Privacy Officer

- make a copy of the document setting forth the legal authority and file it with the individual's Health Plan or medical record

- follow the applicable procedures set forth above in the sections entitled "Mandatory Disclosures of PHI to Individuals and HHS" or "Permitted Uses and Disclosures of PHI for Legal and Public Policy Purposes"

## 13.0 Documentation and Record Retention Requirements

**13.1** The Privacy Rules require CMU to maintain documentation of its compliance with the Privacy Rules. CMU's policy is to maintain the required documentation for the required retention period which is six years from the date the document was made, or, if later, six years from the date the documents was in effect.

**13.2** The Chief Privacy Officer will maintain a copy of the Policies and Procedures and the Notice of Privacy Practices for six years beyond the date the documents cease to be effective.

**13.3** The Privacy Rules require that certain uses and disclosures be documented so that CMU can respond to an individual's request for an accounting of disclosures as outlined in Policy 12-11 "Individual Rights."

**13.3.1** For the disclosures that are subject to the right of an accounting (defined below in Section 13.3.2), each unit of the CMU Hybrid Entity will retain documentation of the following:

- the individual whose PHI was disclosed
- the date of the disclosure
- to the extent known, the name and address of the entity or person who received the PHI
- a brief description of the PHI disclosed
- a brief statement of the purpose of the disclosure

**13.3.2** The following disclosures of PHI must be documented for purposes of an accounting:

- all unauthorized disclosures known to CMU
- disclosures to law enforcement
- disclosures to HHS
- any disclosures required by law, including those made:
  - in response to the order of a court or an administration tribunal
  - in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, provided that there is an appropriate protective order in place and, where medical records are involved, the individual has waived his or her physician-patient privilege

- pursuant to process (such as a court-ordered warrant or an administrative summons), and as otherwise required by law

- any of the following permitted disclosures:

  - to a law enforcement official (1) about an individual who has died; (2) for identification and location purposes; (3) about an individual who is, or is suspected of being, a victim of a crime; or (4) about an individual relating to a crime on CMU premises

  - about an individual that CMU reasonably believes is the victim of abuse, neglect, or domestic violence, to a government authority, including a social service or protective service agency, that is authorized by law to receive such information

  - to appropriate public health authorities for public health activities

  - to a health oversight agency for health oversight activities

  - to coroners, medical examiners, and funeral directors about a deceased individual

  - for organ, eye or tissue donation purposes

  - for certain research purposes, when the need for an authorization has been waived or is otherwise not required

  - in order to avert serious threat to health or safety

  - about armed forces personnel to appropriate military command authorities

  - for protective services to the President of the United States and other designated persons

  - to correctional institutions and law enforcement custodians

  - in connection with workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault

**13.3.3** The following uses and disclosures do not need to be documented for purposes of an accounting:

- to carry out treatment, payment and health care operations

- to the individual that is the subject of the PHI (except formal requests to inspect and/or copy as described below)

- uses and disclosures incidental to permitted uses and disclosures

- pursuant to a valid authorization signed by the individual who is the subject of the use or disclosure

- for national security or intelligence purposes

- to correctional institutions or law enforcement custodians when the disclosure was permitted without an authorization

**13.3.4** The appropriate Privacy Officer will maintain for a period of six years from the date the following documents related to authorizations and individual rights were last effective:

- individual authorizations for the use or disclosure of PHI
- requests for an accounting of disclosures, and all accountings and related communications provided in response to the request
- temporary suspensions of an individual's right to an accounting by:
  - a health oversight agency conducting health oversight activities authorized by law, pursuant to 45 CFR § 164.512(d)
  - a law enforcement official, conducting an activity described in 45 CFR § 164.512(f)
- requests for confidential communications and all documents relating to their disposition
- requests to inspect and copy and all documents relating to their disposition
- requests to amend and all documents relating to their disposition (if CMU elects to amend PHI, the amendment must be maintained as long as the record is maintained; if CMU elects not to grant the amendment and the individual files a disagreement, the disagreement must be maintained as long as the record is maintained)
- requests for additional restrictions and all documents relating to their disposition
- individual complaint forms, complaint tracking forms, and all other documents relating to their disposition
- an individual's written agreement to receive a Notice of Privacy Practices by e-mail, and any withdrawal of such agreement

**13.4** The appropriate Privacy Officer will maintain documentation demonstrating the dates when employees with access to PHI were trained concerning the Privacy Rules and any applicable Policies and Procedures, for a period of six years from the date each training session was concluded.

**13.5** The Chief Privacy Officer will maintain documentation of all complaints that CMU receives of violations of these Policies and Procedures or the Privacy Rules, and all documentation relating to disposition of the complaints. CMU will maintain these documents for six years from the date of a complaint's final disposition.

**13.6** The Chief Privacy Officer will maintain documentation of all disciplinary action that CMU has taken against employees for violations of these Policies and Procedures or the Privacy Rules, for a period of six years from the date of the disciplinary action.

**13.7** The Chief Privacy Officer will maintain all documents relating to CMU's efforts to minimize the harmful effects of any unauthorized use or disclosure of an individual's PHI, for a period of six years from the date of the action. Such documentation will

include known details of the unauthorized use or disclosure, details of CMU's efforts to retrieve PHI or halt the improper use or disclosure, and all correspondence relating to the unauthorized use or disclosure.

**13.8** The Office of General Counsel will maintain copies of all business associate agreements for a period of six years from the date the contract was last in effect.

*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.*

5549545-10