

HIPAA – Hybrid Entity Policy & Glossary

Summary/Purpose: This policy is to define the Oxford, MS Campus of the University of Mississippi (UM) as a Hybrid entity whose business activities include both covered and non-covered functions in accordance with the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH”).

As a Hybrid entity, UM is a single legal entity including both covered and non-covered entities. HIPAA Covered Entities must adhere to the privacy and security regulations designated in the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH”); specifically, the requirements defined in 45 CFR §§ 164.103 and 164.105.

This policy addresses only the hybrid entity status of the Oxford Campus of the University of Mississippi. The University of Mississippi Medical Center (UMMC) in Jackson, MS has separate and distinct policies on HIPAA compliance.

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted on August 21, 1996 to recognize and enforce the rights of patients to protect the privacy of their medical records. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information.

As an educational institution, UM contains academic, administrative and health care related functions. As a single legal entity that performs both covered and non-covered functions UM has designated itself as a Hybrid entity. As a Hybrid entity, UM excludes from its covered entity status areas of operation consisting of non-covered functions: (1) components of the organization performing non-health care functions and/or (2) health care services that do not engage in electronic transactions. To comply with HIPAA requirements, all HIPAA covered entities must comply with HIPAA regulations.

Designation of HIPAA Covered Entities

UM designates the following areas as HIPAA Covered Entities.

- Student Health Services
- Student Health Center Pharmacy
- Speech and Hearing Center

Together with the Chief Privacy Officer, general counsel of The University of Mississippi, and legal counsel at the University of Mississippi Medical Center, The University of Mississippi will determine, through periodic annual review and monitoring, which individual departments, clinics, or units at The University of Mississippi are considered a HIPAA Covered Entity (CE) and Business Associates of the covered entity. All CE's and Business Associates of CEs must comply with this policy and associated procedures.

General Standards for Safeguarding HIPAA Information

As required by the "Security standards: General Rules" (45 C.F.R. § 164.306(a)) section of the HIPAA Security Rule, each covered entity must:

- Ensure the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains or transmits;
- Protect against any reasonably anticipated threats and hazards to the security or integrity of EPHI; and
- Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the privacy rule.

As a Hybrid entity, UM areas/offices designated as HIPAA covered entities must comply with applicable requirements of HIPAA. The following are general guidelines and not meant to be all-inclusive:

- Employee training on HIPAA and protection of PHI and EPHI
- Encryption of all HIPAA data
- Firewall restrictions must be implemented to separate covered from non-covered entities.
- Designated HIPAA covered entities shall not disclose PHI to any non-health care functional areas.
- In areas where medical covered entities and non-medical covered entities coexist, physical separation must exist to prohibit exposure to non-covered entities.
- Select vendor partners and service providers that can maintain proper safeguards for covered medical information. Contractually require service providers to put into effect and maintain such safeguards.
- Periodically evaluate and adjust the departmental security program based on the results of testing and monitoring.

Disclosure of PHI in the following instances does not apply to the designated CE's on the Oxford campus and is forbidden for the following purposes:

- ☐ Fund raising activities
- ☐ Marketing disclosure reminder
- ☐ Disclosure through directory

All Policies for PHI on the Oxford Campus of the University of Mississippi apply only to the CE's designated in this Hybrid document.

All Policies will be reviewed annually by the HIPAA compliance Committee, CISO, or their designee and updated to reflect changes in law or UM practices.

Detailed Standards for Safeguarding Customer Information is within the UM Information Confidentiality/Security Policy.

HIPAA DEFINITIONS & GLOSSARY:

Abuse – Willful infliction of physical pain, injury, or mental anguish on a vulnerable adult, the unreasonable confinement of a vulnerable adult, or the willful deprivation by a caretaker or services which are necessary to maintain the mental and physical health of a vulnerable adult.

Designated Record Set - HIPAA requires each covered entity to define its own designated record set. As such, the UM Oxford campus defines its designated record set as:

- Clinical Records - All clinical information that is specific to an individual's treatment, as listed in the Mississippi code § 41-9-61, that is stored in one or more of the following locations:
 - Paper records kept and maintained in the designated CE's;
 - The Electronic Health Record System;
 - Graphic data generated by computer software within UM, such as EKGs;
 - All practitioner paper records; and
 - Research records, but only that clinical data that is specific to the individual's treatment.
- Billing Records – Certain billing records that pertain to the individual are included in the definition of designated record set and include the following:
 - Remittance advice from a payer;
 - Itemized bills;
 - Medicare Advance Beneficiary Notices (ABN); and
 - Standard transactions, as applicable
- Other Information – Other pieces of information are considered part of the designated record set including:
 - Signed consent forms;
 - Advance directives; and
 - Signed acknowledgements, such as the acknowledgement of receipt of the Notice of Privacy Practices;

The designated record set will not include the following types of information:

- Information used for health care operations as defined below;
- Any other records used strictly for administrative or business purposes;
- Compiled data for purposes of accreditation and other aggregate data; and
- Photographs, slides, films, or other source data that are developed for educational purposes only.

Exploitation – The illegal or improper use of a vulnerable adult or his resources for another's profit or advantage.

Health Oversight Activities - include any activities that are authorized by law, including audit; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil administrative, or criminal proceeding or actions; or other activities necessary for appropriate oversight of the healthcare system.

Exceptions to Health Oversight Activities -

A health oversight activity does not include an investigation or other activity in which the individual is the subject unless, such investigation or activity is directly related to:

- The receipt of health care;
- Claim for public benefits to health; or
- Qualification for, or receipt of, health care coverage from public benefits or services program.

Health Oversight Agency – means an agency of:

- The United States;
- A State;
- A territory;
- A political subdivision; or
- Person or entity acting under a grant of authority from or contract with such public agency.

Healthcare Operations– Activities that the UM Oxford Campus performs in order to continue operating. Such activities include but are not limited to: quality assessment and improvement activities, population-based activities relating to improving health or reducing healthcare costs, case management and care coordination, conduction of training programs, and compliance activities.

Healthcare System includes:

- Government benefit programs for which health information is relevant to beneficiary eligibility;
- Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
- Entities subject to civil rights laws for which health information is necessary for determining compliance.

Neglect – The inability of a vulnerable adult who is living alone to provide for himself the food, clothing, shelter, health care, or other services which are necessary to maintain his mental and physical health.

Payment Card Industry (PCI) – Any process to accept, process, store or transmit credit card information.

Protected Health Information (PHI) – PHI as defined by the HIPAA, section 160.103, is all individually identifiable health information transmitted or maintained by UM, that is (1) Transmitted by electronic media; (2) Maintained in any electronic medium; or (3) Transmitted in any other form (oral communication included) or medium. The definition of PHI encompasses that of hospital records defined by Mississippi Code (§41-9-61), which includes...

"Without restriction, those medical histories, records, reports, summaries, diagnoses and prognoses, records of treatment and medication ordered and given, notes, entries, x-ray, and other written or graphic data prepared, kept, made or maintained in hospitals..."

Systems Owners are the Covered Entity's University Administrator responsible for that area.

Vulnerable Adult – A person eighteen (18) years of age or older or any minor not covered by the Youth Court Act who is present in the state and who, regardless of residence, is unable to protect his or her own rights, interests, and/or vital concerns and who cannot seek help without assistance because of physical, mental, or emotional impairment. "Vulnerable Adult" should also include all residents or patients, regardless of age, in a care facility.