The purpose of this policy is to ensure compliance to the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) by establishing the standards, expectations and requirements for University of Mississippi (UM) for safeguarding the confidentiality, integrity, and availability of UM’s Information Assets (HIPAA electronic protected health information and other confidential data) by preventing, detecting, containing, and correcting security violations for University of Mississippi’s (UM) Information Security Management Program (ISMP).

Scope

This policy applies only to the Covered Entities as defined in the UM HIPAA Hybrid Policy. This policy applies to all employees, students, contractors, and any other individuals with login credentials (Users) to UM Information Assets. This policy is available to all Users, including all individuals responsible for implementing its procedure.

Policy

A. Information Security Management Program (ISMP) Policy
   1. UM establishes formal information security and risk management programs based on the HIPAA Security Rule through:
      a. Risk analysis – by conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by UM or business associate.
      b. Risk management – by implementing security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA Security Rule.
c. Sanction policy – by applying appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

d. Information system activity review – by implementing procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. UM designs, implements, and maintains a comprehensive and effective ISMP to ensure acceptable levels of risk throughout UM. The ISMP is continuously assessed and improved upon through governance, risk management, information security protective operations, awareness and training, and incident response activities.

3. The ISMP is formally documented and actively monitored by the Chief Information Security Officer (CISO), or the CISO’s designee, as specified or documented in writing.

4. UM reviews and updates the ISMP annually to ensure program objectives continue to meet the needs of UM.

B. Information Security Management Program Strategy

The ISMP is staffed, organized, and supported by the CISO in order to ensure that it maintains its capability of accomplishing the primary tasks of information security:

- Governance
- Risk analysis
- Risk management
- Sanction policy
- Information system activity review
- Training and awareness
- Incident response activities

C. Information Security Management Program Content

At a minimum, the ISMP includes:

- UM approved information security policies and procedures
- Mission, vision, structure, and objectives of the information security program
- Governance structure
- Annual risk assessment
- Risk management measures and actions
- Education, training, awareness plan, and materials

D. Commitment to Information Security
2. UM Office of Information Technology actively supports information security through clear direction, demonstrated commitment, incorporation into strategic planning, and acknowledgment of information security responsibilities.

3. The CISO, or the CISO’s designee, is appointed and accountable for ensuring information security leadership and processes are in place, compliance with applicable laws and regulations is assured, and security risks are evaluated and accepted for UM.

4. Formal governance is chartered to ensure institutional oversight, coordination, and synchronization of information security at UM.

5. The formal governance body reviews the effectiveness of the ISMP and evaluates and accepts security risks.

6. Capital planning and investment requests consider information security. They include resources necessary for implementing information security capabilities necessary to address any risks associated with such capital plans and requests. UM ensures such resources are available for expenditure and applied appropriately.

E. Information Security Coordination
   1. UM risk reduction activities are coordinated and communicated by representatives from different parts of UM respective to roles and job functions.
   2. Security control implementations are coordinated in advance and communicated across UM.
   3. Security requirements for information systems are identified and resources are allocated as either capital or operating resources.

F. Information Security Responsibilities
   1. All information security responsibilities are formally defined and documented.
   2. The CISO, or the CISO’s designee is a senior-level employee who oversees the ISMP.

Policy Compliance

Enforcement
The Chief Information Security Officer (CISO), or the CISO’s designee, has general responsibility for the implementation and enforcement of this policy.

Future Revisions
UM periodically reviews and updates its policies and procedures as needed in response to environmental or operational changes affecting the security of ePHI. UM reserves the right to add, delete, or revise any provision of this Policy or any other Information Security policy at any time without prior notice as long as such changes are compliant with the Security Rule. All UM security policies are subject to a review process that includes, but is not limited to, designated representatives from the Office of Information Technology and the Office of General Counsel.

Sanctions
Any User violating this or any security policies or applicable local, state, or federal laws while using UM’s computing environment is subject to disciplinary actions deemed appropriate, up to
and including termination. In cases in which PHI is involved, the CISO, or designee, will collaborate with the Office of General Counsel and Human Resources to recommend appropriate sanctions.

**Exceptions**
The process to request exceptions to Information Security policies is available. Requests are documented, then evaluated based on the potential risks to business, as well as, HIPAA Security Rule. The CISO, or the CISO’s designee, can approve exceptions necessary to meet a business or patient care need. The CISO, or the CISO’s designee, may request compensating controls and processes to ensure UM adherence to the HIPAA Security Rule. All approved policy exceptions will be reviewed annually for appropriateness by the CISO, or the CISO’s designee.