Purpose of Policy
The purpose of this policy is to define how access is controlled in order to ensure compliance to the HIPAA Security Rule  (45 CFR Parts 160 and 164, Subparts A and C) and to set the expectations and requirements for University of Mississippi (UM) for controlling access to ensure the safeguarding of the confidentiality, integrity, and availability of UM’s information assets (HIPAA electronic protected health information and other confidential data) stored within the UM enterprise network or hosted with third parties.

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 individual 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. Access Control Policy
1. UM develops and implements access control through policies and procedures that (i) determine authorization and/or supervision of Users; (ii) determine appropriate access of the User; (iii) termination and/or revision of User access. The access policies and procedures are reviewed at least annually and updated as needed.
2. Access control rules account for and reflect UM’s policies for information dissemination and authorization. Access control rules are supported by formal procedures and clearly defined responsibilities.
3. Access to operating systems and departmental network drives is controlled by unique user identification (User ID) including but not limited to those systems containing electronic protected health information (ePHI). The User ID is a unique name and/or number for identifying and tracking user identity.
4. A screen saver is activated after not more than ten (10) minutes of inactivity on workstations. The system requires the User to re-establish access using appropriate identification and authentication procedures.

B. Unique User Identification and Authentication
1. UM requires every User to have a unique user ID. Duplicate User IDs are never to be issued to access systems containing PHI.
2. User are prohibited from sharing their User IDs.
3. Users are uniquely identified and authenticated for both local and remote access to information systems.
4. Third party users or processes acting on behalf of third-party users, are uniquely identified and authenticated.
5. Users who perform privileged functions (e.g., system administration) are to use separate accounts when performing those privileged functions (i.e. elevated, super user accounts). These Users do not perform regular user activities from privileged accounts or administrative activities.
6. Generic User IDs are restricted and never used to access systems containing PHI.

C. User Registration
1. UM develops and implements a formal, documented process for establishing, activating, modifying, reviewing, disabling, and removing accounts. This User registration and de-registration process includes workforce member transfers, third party accounts, maintenance accounts, and external access.
2. UM grants access to information systems based on need-to-know, need-to-share, and least privilege.
3. Proper User identification is required prior to the creation of an information system’s User account and prior to approval of all such requests.
4. UM defines account types (e.g., individual, system and application).
5. When the Office of Information Technology configures devices, it ensures that all default and unnecessary accounts (e.g., system, guest, administrator, vendor or other third-party accounts) are removed, disabled, or otherwise secured (e.g., change the default passwords, reduce privileges to the lowest levels of access, etc.)
D. Workforce Clearance Procedure
   1. The allocation and use of access to information systems and services is restricted and controlled.
   2. The allocation of access is controlled through a formal access authorization process administered by the Covered Entity University Administrators.
   3. Access is allocated to Users based on work roles, job function, and business requirements. Access is granted based upon the minimum necessary requirement for a User’s functional role.

E. Review of Access Rights
   1. User access roles are reviewed on an annual basis, unless there is a work role, job function or business requirement change that necessitates immediate revision of access.
   2. Reviews and follow-up actions are documented and submitted to the HIPAA Privacy and Security Committee.
   3. Covered Entity University Administrators are notified when User access rights change (e.g., termination, change in position) and modifies the Users access accordingly.
   4. Upon termination of employment and/or revocation of access for Users physical and logical access rights and associated materials are removed or modified to restrict access within 24 hours.
   5. Disciplinary terminations will have their physical and logical access rights removed immediately.
   6. Change in position access will be modified as relevant within 24 hours.

F. Remote Access
   1. To the extent possible, multi-factor authentication is implemented for all remote electronic protected health information access. Confidential information is protected where feasible.
   2. Accounts for remote maintenance and remote administration are specifically authorized by Covered Entity University Administrators or the Office of Information Technology.
   3. Encrypted VPN solutions are implemented for remote access to UM’s network.

G. Remote Diagnostic and Configuration Port Protection
   1. UM controls physical and logical access to diagnostic and configuration ports.
   2. Access to network equipment is physically protected (e.g., a router must be stored in a room that is only accessible by authorized workforce members or third parties) such that remote diagnostic and configuration ports are protected.
   3. Logical access to remote management of network equipment is protected.
   4. Management ports, services, and similar applications installed on a network system, which are not specifically required for business functionality, are disabled or removed.

H. Network Segregation
   1. Where feasible, groups of information services, Users, and information systems are segregated on networks.
   2. Firewalls are used to maintain segregation between internal network segments and external network segments (e.g., the Internet) and enforce access control policies for each of the domains.
   3. UM’s network is logically segmented by a defined security perimeter and traffic is controlled based on functionality required and classification of the associated data, applications, or systems.
   4. Network segregation architecture and security design logic are documented and reviewed at least annually.

I. Network Connection Controls
   1. For shared networks, especially those extending across UM boundaries, the capability of Users to connect to the network is restricted, in line with the access control policy and requirements of the business applications.
2. At external network interfaces, inbound network traffic is denied by default and allowed by exception (i.e., deny all, permit by exception).
3. Network traffic is controlled through firewall and other network-related restrictions.
4. Transmission protection is used to encrypt data in transit.

Policy Compliance

Enforcement
The Chief Information Security Officer (CISO), or 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 will collaborate with the Office of General Counsel 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 designee, can approve exceptions necessary to meet a business or patient care need. The CISO, or 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 designee.