Purpose

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) regarding the security of remote access. All terms with a definition set forth in the HIPAA Security Rule have the same meaning in this policy.

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 (workforce members) (“Users”) to UM Information Assets. This policy is available to all Users, including all individuals responsible for implementing its procedure.

Policy

A. Remote Access Policy

1. UM implements technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

2. UM manages and controls access to its internal and external networks. Users are only provided with access to internal and external networks that they have been specifically authorized to use. Appropriate authentication methods are used to control the access of remote users.

3. Users who connect to UM’s networks from a remote location are required to use UM approved and managed secure remote access technologies that comply to the HIPAA Security Rule.

4. To the extent possible, multifactor authentication is implemented for access to electronic protected health information.
5. Users are responsible for adhering to all of UM's policies, not engaging in illegal activities, and not using remote access for interests other than those of UM.

B. Requesting Remote Access
1. UM controls remote access and only provides access with least privilege required to meet the operational requirement for clinical, educational, research and operational business need.

2. Users register personal devices required for a multi-factor authentication. UM owned devices used and any form of tokens are implemented and controlled by UM.

3. Business associates and other third parties (e.g., contractors, vendors) are granted remote access for contractual requirements with which the business associates and UM maintain adherence to the HIPAA Security Rule and industry best practices.

C. Remote Security
1. All computing devices that remotely connect to UM’s network must apply the most up-to-date anti-malware software and security patches of UM.

2. UM maintains remote access logs which are monitored to detect suspicious activity.

3. Encryption is used to protect the confidentiality and integrity of remote access sessions.

D. Remote Privacy
1. Remote Users, including business associates and other third parties, must log-off and disconnect from UM’s network when access is no longer required to perform job responsibilities. UM performs appropriate oversight to restrict Users that no longer require access.

2. Remote Users lock the workstation and/or system(s) when unattended so that no other individual is able to access any Information Assets and/or UM Information Technology Assets (IT Assets) on which those assets reside or can be accessed.

3. Remote access is controlled to ensure that unauthorized individuals do not access UM’s network. At no time does access allow Users to disclose username or password to anyone.

4. Users must not configure devices to remember or automatically enter username and password.

5. Users must take necessary precautions to secure all Information Assets to which access has been granted.

Policy Compliance

Enforcement
The Chief Information Security Officer (CISO), or the CISO’s designee, as specified in documented in writing, 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 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 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.