Purpose

The purpose of this policy is to ensure compliance with the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) by establishing 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) and to establish specific requirements for Users of Information Assets. 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 (Users) to UM Information Assets. This policy is available to all Users, including all individuals responsible for implementing its procedure.

Policy

A. User Responsibilities and Acceptable Use

1. UM provides Information Technology Assets (IT Assets) as resources to UM Users. It is the user's responsibility to properly use and protect those resources.

2. Use of IT Assets owned and/or operated by UM imposes certain responsibilities and obligations. UM considers use of IT Assets to be a privilege that is granted on the condition that each user respects the integrity of such resources and the rights of others.

3. UM’s annual Information Security Awareness training is mandatory for all Users. New Users must complete the training within the first thirty (30) days of onboarding.
4. Users shall comply with all UM policies, state and federal laws, regulations, and contractual obligations when accessing Information Assets and IT Assets.

5. Users’ actions may be monitored and use of IT Assets is consent to such monitoring.

6. Users are responsible for protecting all IT Assets utilized for business and clinical use.

7. Access to Information Assets is restricted based on need-to-know and in accordance with the minimum necessary principle. IT Assets are enterprise configured accordingly.

8. Users are responsible for the security of their passwords and all Information Assets for which access is authorized.

9. Users who are authorized to access Information Assets are responsible for properly storing and securing from unauthorized access.

10. The use of cut, copy, paste, move, print, and print screen commands and/or storage of Information Assets is prohibited.

11. Users are allowed to use UM IT Assets:
   - To which they have been granted authorized access
   - For UM business, clinical, academic and research purposes only
   - Users bear the responsibility for knowing and complying with applicable laws, policies, and rules; for appropriately securing their computers and other electronic devices from misuse or theft by others; and for avoiding any use that interferes with others’ legitimate access to and use of IT Assets

B. Internet Access from UM Locations

1. Connection to the Internet or use of a website is a privilege and not a right. Any abuse of that privilege can result in legal and/or administrative action.

2. UM monitors and logs Internet access. Any website or online activity may be blocked if it is determined to be harmful, potentially harmful, or disruptive to the organization or other Users.

3. Access to the Internet shall only be permitted through the UM corporate firewall.

4. Individually assigned passwords and accounts must not be shared.

5. Personal and UM (business) passwords must be different.

6. Passwords require at least eight (8) characters which are:
   - Not easy to remember
   - Not based on anything easily guessable or obtained using personally related information (e.g. names, telephone numbers, addresses, dates of birth, etc.)
• Not vulnerable to dictionary attack (describes words normally included in dictionaries)
• Free of consecutive identical characters
• And must include a combination of upper- and lower-case alphabetic characters, numbers, and special characters (combination of any three (3) of the four (4) listed is acceptable).

7. Passwords are prohibited from being reused for at least six (6) generations.

C. User Responsibilities for Unattended UM Information Technology Assets

1. Users must ensure that unattended devices have the appropriate physical protections (e.g. locked rooms, locked drawers) when not in the Users’ custody.

2. Users must lock the screen or log off computer devices when the device is unattended in order to protect any information available onscreen and to prevent access to the device by others.

3. Users must safeguard unattended information system output devices (e.g., printers) to prevent unauthorized individuals from obtaining the output.

D. Code of Conduct

Users of UM Information Technology Assets agree to NOT:

1. Post, use, or transmit content to which they do not have the right to post or use under intellectual property, confidentiality, privacy, or other applicable laws.

2. Post, use, or transmit unsolicited or unauthorized content, including:
   • Advertising or promotional materials
   • “Junk mail”
   • “Spam”
   • “Chain letters”
   • “Pyramid schemes”
   • Political campaign promotional material
   • Any other form of unsolicited or unwelcome solicitation or advertising
   • Material of any kind that infringes upon copyright laws, including the unauthorized downloading, copying, displaying, and/or distributing of copyrighted material. All such works should be considered protected by copyright law unless specifically stated otherwise. Any use of UM IT Assets (e.g., networks, email systems, websites, etc.) to access, display, send, transfer, modify, store or distribute copyrighted material (e.g., video/movies, music/audio, images, documents, software, text, etc.) is strictly prohibited.
3. Post, use, or transmit content that contains software viruses, computer code, files, or programs designed to interrupt, destroy, limit the functionality, or otherwise interfere with any computer software, hardware, telecommunications equipment, or other Information Assets.

4. Post or transmit content that is harmful, offensive, obscene, abusive, invasive of privacy, defamatory, hateful or otherwise discriminatory, false, misleading, illegal, in breach of obligations to any person, or contrary to any applicable laws and regulations.

5. Intimidate or harass one another.

6. Allow unauthorized use or attempt to use another user’s individual account, service, or personal information.

7. Modify workstations without IT approval or remove, circumvent, disable, damage or otherwise interfere with any security-related features.

8. Install or use unauthorized or malicious software or obtain unauthorized data and software from external networks.

9. Transmit (e.g., instant message, email, text, etc.) Information Assets over open, unprotected, wireless networks unless approved security controls such as strong encryption are in place.

10. Automatically forward Information Assets to an external email address.

11. Use UM demographic data such as business email address for personal use (e.g., register for software, complete a web form).

12. Attempt to gain unauthorized access to IT Assets or other Users' accounts through hacking, password mining or any other means, or interfere or attempt to interfere with the proper working of IT Assets or any activities conducted through those assets.

13. Impersonate another person or entity, or falsely state or otherwise misrepresent affiliation with a person or entity without authorization.

14. Connect personally owned devices to the UM enterprise network. This includes UM wireless and network ports on UM’s wired network.

15. Conduct any activities with the intention of creating and/or distributing malicious programs using the UM network (e.g., viruses, worms, Trojan Horses, etc.).

16. Fail to exercise appropriate caution when opening emails, attachments, or accessing external websites.

Policy Compliance

Enforcement

The Chief Information Security Officer (CISO), or the CISO’s designee, as specified and 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, or the CISO’s 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.