Information Technology Acceptable Use
HIPAA Policy: Security 26

Summary: Outlines the acceptable use policy for HIPAA covered entities

Affected Individuals: Employees of HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to set standards and expectations for University of Mississippi (UM) workforce members with regard to access to UM information assets.

Policy Scope

This policy applies to all workforce members, users, and all personnel affiliated with third parties who use UM information assets and related resources.

This policy applies to information technology administered centrally; personally-owned computing devices connected by wire or wireless to the UM network; and to off-site computing devices that connect remotely to the UM network.

Definitions

For a complete list of definitions, refer to the *Glossary*.

Policy Statement

A. User Responsibilities and Acceptable Use

1. UM provides information technology assets as resources to the UM workforce. It is the User's responsibility to properly use and protect those resources.
2. Use of information technology assets owned or operated by UM imposes certain responsibilities and obligations. UM considers use of IT resources to be a privilege that is granted on the condition that each user respects the integrity of IT resources and the rights of other users.
3. Users shall comply with all UM policies, state and federal laws, regulations, and contractual obligations when accessing UM information technology assets.

4. Workforce member's actions may be monitored and workforce members consent to such monitoring.
5. Users are responsible for protecting all UM information technology assets to which they are granted access.
6. User access to UM information assets shall be restricted based on need-to-know and in accordance with the minimum necessary principle.
7. Users shall be made aware of their responsibilities for maintaining effective access controls and shall be required to follow UM policies.
8. Users are responsible for the use and protection of UM information resources by using effective access controls (e.g., passwords) and by safeguarding those access controls.
9. Users are responsible for the security of their passwords and all data which they are authorized to access.
10. Users are required to handle, label, and store confidential data in accordance with the *Data Handling, Labeling, and Storage Policy*.
11. Users who are authorized to access confidential data are responsible for properly storing and securing it from unauthorized access, as well as for securing and protecting passwords and other forms of access control.
12. Copy, move, print (and print screen), and storage of sensitive data is prohibited when accessed remotely without a defined business need.
13. Users are allowed to use UM information technology assets:
    a. To which they have been granted authorized access.
    b. For UM business and research purposes only.

14. Each user bears 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 UM information technology assets.
15. Related UM policies that may apply to acceptable use of UM information assets include, but are not limited to, Human Resources personnel policies, Finance policies, Compliance and Administrative policies, all of which are subject to change.

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. Internet access is granted to workforce members and visitors with the expectation that users will act responsibly and use good judgment.
3. Internet access may be monitored at any time by UM. Any website or online activity may be blocked if it is determined to be harmful, potentially harmful, or disruptive to the organization or other workforce members.
4. Access to the Internet shall only be permitted though the UM corporate firewall.
5. A separate network shall be established to provide Internet access to visitors. The UM corporate network must not be accessible from the visitor network.
6. Individually assigned passwords and accounts must not be shared.
7. Personal and UM (business) passwords must be different.
8. Users shall utilize strong passwords:
    a. At least eight characters in length
    b. Containing at least one number or special character

c. Not the same as the username or email address

C. Responsibilities for Unattended Information Technology Assets

1. Users shall ensure that unattended equipment has appropriate protection.
2. Users shall log-off computing devices when the session is finished (i.e., not just switch off the PC screen or terminal) in accordance with the *Clear Desk and Clear Screen Policy*.
3. Users shall 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 that you do not have the right to post or use, for example, 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
3. Infringe upon copyrighted material of any kind, 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 information technology assets (e.g. network, email system, website, 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.

4. Post, use or transmit content that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or otherwise interfere with or disrupt UM information assets.
5. Post or transmit content that is harmful, offensive, obscene, abusive, invasive of privacy, defamatory, hateful or otherwise discriminatory, false or misleading, incites an illegal act, or is otherwise in breach of your obligations to any person or contrary to any applicable laws and regulations.
6. Intimidate or harass one another.
7. Allow unauthorized use or attempt to use another user's individual account, service, or personal information.
8. Modify workstations without IT approval or remove, circumvent, disable, damage or otherwise interfere with any security-related features.
9. Install or use unauthorized or malicious software, or obtain unauthorized data and software from external networks.
10. Transmit (e.g., messaging, email, texting, etc.) Confidential Data over open, unprotected wireless networks unless approved security controls such as strong encryption are in place.
11. Automatically forward Confidential Data to an external email address.
12. Use UM demographic data such as business email address for personal use (e.g., register for software, complete a web form).
13. Attempt to gain unauthorized access to UM information technology assets, other user's accounts, computing devices or networks connected to UM information

technology resources, through hacking, password mining or any other means, or interfere or attempt to interfere with the proper working of UM information assets or any activities conducted through those information assets.

14. Impersonate another person or entity, or falsely state or otherwise misrepresent your affiliation with a person or entity without authorization.
15. Connect personnel devices to the UM network prior to putting appropriate safeguards in place.
16. Conduct any activities with the intention of creating and/or distributing malicious programs using the UM network (e.g., viruses, worms, Trojan Horses, etc.).
17. Fail to exercise appropriate caution when opening emails, attachments or accessing external web sites.

E. Sanctions

Any user violating these policies or applicable local, state, or federal laws while using UM's computing environment is subject to loss of network privileges and any other disciplinary actions deemed appropriate, up to and including termination and criminal and/or civil prosecution in accordance with policy.

.

Regulatory References

HIPAA Regulatory References: HIPAA § 164.308(a)(5)(ii)(B), HIPAA § 164.308(a)(5)(ii)(D), HIPAA § 164.310(a)(1), HIPAA § 164.310(b), HIPAA § 164.310(c), HIPAA § 164.312(a)(2)(iii)
HITRUST References: 01.f Password Use, 01.g Unattended User Equipment, 09.j Controls Against Malicious Code

PCI References: PCI DSS v3 5.1.1, PCI DSS v3 8.5.11, PCI DSS v3 8.5.3, PCI DSS v3.1 5.1, PCI DSS v3.1 5.2, PCI DSS v3.1 8.2.4, PCI DSS v3.1 8.2.4, PCI DSS v3.1 8.2.5, PCI DSS v3.1 8.4