Clear Desk and Clear Screen
HIPAA Policy: Security 09

Summary: Steps to protect PHI on desk tops and computer screens from disclosure

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to ensure confidential data is kept private and protected from unauthorized access and viewing. The goal is to reduce the risks of unauthorized access to, or loss of, or damage to, the University of Mississippi's (UM) enterprise data.

Definitions

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

Scope

This policy applies only to covered entities as defined in the University of Mississippi (UM) HIPAA hybrid policy.

This policy applies to all UM confidential data, computing devices, and users.

1. Policy

A. Clear Desk and Clear Screen Policy

1. Confidential data on removable media is not left unattended and unsecured.
2. Confidential data on removable media is protected from access by unauthorized individuals when not in use according to the *Encryption Policy*.
3. Reproduction technology (e.g., printers, copiers, scanners, cameras, facsimile machines, etc.) is protected physically from use by unauthorized individuals to prevent unauthorized reproduction of confidential data.
4. Passwords are not posted on, under, or near a computer or other computing devices.

B. Workstation Security

1. All users close all applications, logout, or lock their computer when they are away from their desk to protect confidential data from unauthorized access and viewing.
2. Workstations are configured to automatically lock the screen in accordance with the *Access Control Policy*.
3. Workstations require a password to deactivate the screen saver.

C. Mail Services

1. Covered or critical information is protected when using internal or external (e.g., USPS) mail services.

Policy Compliance

Enforcement

The Chief Information Security Officer (CISO) has general responsibility for the implementation and enforcement of this policy.

Future Revisions

UM reserves the right to add, delete, or revise any provision of this Policy (approval by committee) at any time, or any other Information Security Policy without prior notice to users

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.

Clear Desk and Clear Screen
HIPAA Policy: Security 09

Exceptions

Exceptions to this policy must follow the approved exception process as outlined in the *Information Security Waiver Policy*. All approved policy exceptions will be reviewed periodically for appropriateness by the CISO and may be revoked at any time with or without notice.

Regulatory and Standards References

The following regulations and standards are applicable to this policy:

- **HIPAA Regulatory Reference**: HIPAA § 164.310(b), HIPAA § 164.312(a)(2)(i)
- **HITRUST Reference**: 01.h Clear Desk and Clear Screen Policy

Related Documents:

- Access Control Policy
- Data Classification and Storage Policy
- Encryption Policy
- Information Technology Acceptable Use Policy
- Glossary

Approval

Chief Information Security Officer	<date>