Media Protection
HIPAA Policy: Security 19

Summary: Protecting PHI recorded on removable media in HIPAA covered entities

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to protect all University of Mississippi's (UM) media containing confidential data in digital format, to ensure destruction before disposal, and to ensure compliance with federal and state laws and regulations concerning the security and privacy of confidential data copied onto removable media.

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 media and removable media containing UM's data regardless of physical location.

Policy

A. Media Protection Policy

1. UM physically and logically protects media containing confidential data while at rest, stored, or actively being accessed.
2. UM develops and implements media protection processes and procedures.

B. Data Exchange Policy and Procedures

1. UM disposes of all UM confidential data in any format including media and paper media according to the *Secure Disposal Policy*.
2. UM restricts access of media and paper media containing confidential data according to the *Access Control Policy*.

C. Management of Removable Media

1. UM develops and implements processes and procedures for the management of removable media.
2. UM restricts the types and use of removable media to maintain security of confidential data.
3. UM requires the registration of removable media before use.
4. Removable media is encrypted in accordance with the *Encryption Policy*.
5. Removable media is handled, labeled and stored in accordance with the *Data Classification and Handling Policy* in addition to this policy.

D. Media Transport and Storage

1. UM physically controls and securely stores media within a controlled area such as a locked drawer or room.
2. UM protects and controls all media during transport outside of controlled areas to prevent unauthorized access or use.
3. UM maintains accountability for all media during transport outside of controlled areas.
4. UM restricts the transport of media outside of controlled areas to authorized personnel.
5. All media backups must be encrypted according to the *Information Backup and Storage Policy*.
6. UM protects the confidentiality and integrity of media during transport outside of controlled areas according to the *Encryption Policy*.
7. If a third party is responsible for transporting backup media offsite, they are responsible for maintaining security according to the *Third Party Risk Management Policy*.

E. Secure Disposal of Media

1. Media and paper media is disposed of securely and safely when no longer needed according to the *Secure Disposal Policy*.
2. UM maintains a log and an audit trail of media and paper media disposal activities according to the Secure Disposal Policy.

F. Approval of Encrypted Portable Media

USB drives and other types of removable disks appointed by the Covered Entity (CE) to store or transport PHI and/or for use with HIPAA systems must be individually approved by IT prior to use. The device owner or their manager should follow the process below for approval.

https://itsecurity.olemiss.edu/media-protection

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 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.

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.

Media Protection
HIPAA Policy: Security 19

Regulatory and Standards References

The following regulations and standards are applicable to this policy:

- **HIPAA Regulatory References**: HIPAA §164.310(c), HIPAA §164.310(d)(1), HIPAA §164.310(d)(2)(i), HIPAA §164.310(d)(2)(ii), HIPAA §164.310(d)(2)(iii), HIPAA §164.310(d)(2)(iv), HIPAA §164.312(c)(1)
- **HITRUST References**: 09.o Management of Removable Media, 09.p Disposal of Media, 09.s Information Exchange Policies and Procedures
- **PCI References**: PCI DSS v1.2 9.8, PCI DSS v3 9.8

Related Documents:

- Information Technology Access Control Policy
- Data Classification and Handling Policy
- Encryption Policy
- Glossary
- Secure Disposal Policy
- Third Party Risk Management Policy

Approval

Chief Information Security Officer	<date>