Information Asset Management
HIPAA Policy: Security 13

Summary: Establishes requirements for management of information in HIPAA covered entities

Affected Individuals: Employees in HIPAA covered entities

Purpose of Policy

The purpose of this policy is to establish requirements for management of University of Mississippi's (UM) information assets. The recording, documenting, classifying, and maintenance of information assets is critical for protecting the confidentiality, integrity, and availability of confidential 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 addresses all information assets that are utilized at UM.

Policy

A. Information Asset Management Policy

1. UM information assets belong to UM, which possesses the exclusive right to manage and direct actions regarding those information assets in accordance with UM's policies and procedures so long as asserting and exercising this right does not conflict with federal or state law or regulations.
2. No expectation of privacy exists regarding UM information assets in accordance with UM's policies and procedures, except privacy rights explicitly protected according to federal or state law or regulation, or in UM's policies and procedures (e.g., privacy of PHI protected under HIPAA, etc.).
3. Data contained on UM's systems are the sole property of UM. Users do not own or have rights to UM data outside of its use in the performance of their UM duties.

4. UM workforce members and users safeguard and protect UM information assets. UM information assets are vital for the fulfillment of the business needs of UM workforce members and authorized users.

5. In order to ensure a reasonable and dependable level of access and service, it is essential that each individual exercise responsible, ethical behavior when using information assets. Misuse of UM information assets has the potential to disrupt business operations.

B. Inventory of Information Assets

1. All information assets are clearly identified and an inventory of all information assets is maintained.

2. The information asset inventory must include sufficient details to recover from a disaster.

3. The information lifecycle manages the secure use, transfer, exchange, and disposal of IT-related assets.

4. The information asset inventory does not duplicate other inventories unnecessarily, but it is ensured that the content of all inventories is in alignment.

5. UM is responsible for establishing procedures to issue information assets to employees and contractors.

6. The information asset inventory is reviewed annually.

C. Ownership of Information Assets

1. All information assets are owned by a designated information asset owner.

2. The information asset owner is assigned, at a minimum, the responsibility for creating, updating, and removing information assets from the information asset inventory.

D. Acceptable Use of Information Assets

   1. Rules for the acceptable use of information assets are identified, documented, and implemented.

E. Information Asset Classification Guidelines

   1. Information assets are classified in terms of their value, legal requirements, and criticality to UM.

   2. UM uses the *Data Classification and Handling Policy* to classify information assets into one of three sensitivity levels (tiers).

F. Information Asset Labeling, Handling and Storage

   1. Procedures for information asset labeling, handling, and storage are developed and implemented in accordance with the *Data Classification and Handling Policy*.

Policy Compliance

Enforcement

The 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 the Information Security Waiver Policy.

Information Asset Management
HIPAA Policy: Security 13

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 References**: HIPAA §164.310(b), HIPAA §164.310(c), HIPAA §164.310(d)(1), HIPAA §164.310(d)(2)(iii)
- **HITRUST References**: 07.a Inventory of Assets, 07.b Ownership of Assets, 07.c Acceptable Use of Assets, 07.d Classification Guidelines, 07.e Information Labeling and Handling
- **PCI References**: PCI DSS v3 11.1.1, PCI DSS v3 12.3, PCI DSS v3 12.3.3, PCI DSS v3 12.3.4, PCI DSS v3 12.3.5, PCI DSS v3 2.4, PCI DSS v3 9.7.1, PCI DSS v3 9.9, PCI DSS v3 9.9.1

Related Documents:

- Informatin Technology Acceptable Use Policy
- Data Classification and Handling Policy
- Glossary

Approval

____ ____________________

Chief Information Security Officer <date>