Encryption
HIPAA Policy: Security 18

Summary: Using encryption to protect PHI in HIPAA covered entities

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to establish the methods for protecting the confidentiality, authenticity and integrity of University of Mississippi's (UM) data at rest, in transit, and in storage by cryptographic methods, and to ensure that encryption standards meet national and international regulations and industry standards.

The intent of this policy is to provide guidance regarding the use of encryption to protect confidential data. Mobile computing devices, removable media, and confidential data in storage and transmission must be encrypted to protect against unauthorized access, loss, or alteration.

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. All workforce members and users, including third parties, who have access or exposure to UM's confidential data are required to comply with this policy.

1. Policy

A. Regulation of Encryption

1. Cryptographic controls are used in compliance with all relevant agreements, laws, and regulatory requirements.
2. Compliance with all relevant regulations is reviewed on an annual basis.

B. Policy on the Use of Encryption

1. This policy is supported by formal procedures on the use of cryptographic controls for protection of confidential data.
2. All encryption mechanisms must be approved by the Chief Information Security Officer (CISO).
3. All encryption mechanisms implemented to comply with this policy must support a minimum of 128-bit AES (Advanced Encryption Standard) encryption, or equivalent.
4. Encryption based on pre-determined criteria protects confidential data on mobile computing devices, on removable media, and across communication paths.
5. Any "write" operation (e.g., file copy) of confidential data to any removable media connected to UM computing devices must employ an approved encryption mechanism to protect against unauthorized access to or modification of the data.
6. When transmitting confidential data using removable media the sending party must:
   - Use an encryption mechanism to protect against unauthorized access or modification.
   - Authenticate the requesting person or entity.
   - Send the minimum amount of confidential data required by the receiving person or entity.
7. If un-encrypted confidential data is discovered on removable media, the confidential data is transferred either to an UM-managed computing device or to an approved, encrypted removable media format.
8. If un-encrypted media has been used for confidential data storage, the unencrypted media must be turned in to the CISO (or designee) for proper disposal as soon as the data has been transferred to an approved, encrypted media and format.
9. Encryption keys and/or passwords are not printed nor allowed to directly accompany removable media. They must be kept physically and electronically separate.

10. All communications of encryption keys and/or passwords must take place via a secure method (e.g., telephone, secure email, etc.).

C. Encryption Key Management

1. Encryption key management is implemented based on specific roles and responsibilities and in consideration of regulatory requirements, restrictions and issues.
2. Encryption keys and the equipment to generate, store and archive keys is logically and physically protected against modification, loss, destruction and disclosure.
3. A formal key management system is defined and implemented consistent with federal and industry-recognized guidelines to securely manage keys issued by trusted Certificate Authorities.
4. Access to encryption keys is limited to designated UM employees and not revealed to consultants, contractors, vendors, or other third parties.
5. Where feasible, encryption keys are generated and maintained in such a way that no single person has full knowledge of any single encryption key.
6. Where feasible, encryption keys are encrypted in storage using a key vault solution.
7. Encryption keys are limited to a period of time not to exceed one year. This may be waived by the CISO in accordance with the Information Security Waiver Policy.

D. Data Protection

1. The confidentiality and integrity of covered information at rest is protected using an encryption method appropriate to the medium anywhere it is stored, or documentation is maintained.

2. In instances where covered information is not encrypted, a documented rationale for not doing so must be provided.

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 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.

Encryption
HIPAA Policy: Security 18

Regulatory and Standards References

The following regulations and standards are applicable to this policy:

- **HIPAA Regulatory References**: HIPAA § 164.308(a)(1)(ii)(D), HIPAA § 164.312(a)(2)(iv), HIPAA § 164.312(e)(2)(ii)
- **HITRUST References**: 06.f Regulation of Cryptographic Controls, 10.f Policy on the Use of Cryptographic Controls, 10.g Key Management
- **PCI References**: PCI DSS v3 3.5, PCI DSS v3 3.5.1, PCI DSS v3 3.5.2, PCI DSS v3 3.6, PCI DSS v3 3.6.1, PCI DSS v3 3.6.2, PCI DSS v3 3.6.3, PCI DSS v3 3.6.4, PCI DSS v3 3.6.5, PCI DSS v3 3.6.6, PCI DSS v3 3.6.7, PCI DSS v3 3.6.8, PCI DSS v3 8.2.2

Related Documents:

- Glossary
- Information Exchange Policy
- Media Protection Policy
- Mobile Computing Device Security Policy

Approval

Chief Information Security Officer	<date>