Information Exchange
HIPAA Policy: Security 11

Summary: Requirements for protecting PHI when transferring information electronically

Affected Individuals: Employees in HIPAA covered entities

Purpose of Policy

The purpose of this policy is to protect the exchange of University of Mississippi (UM) enterprise data in transit through various communication applications and media including but not limited to email, texting, messaging, paging, file transfer, virtual private networks, application interfaces, and other communication channels.

This policy also includes the requirement for establishing information exchange agreements with third parties and protecting physical media in transit.

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 workforce members, including users and students, and all personnel affiliated with third parties who access UM information assets regardless of physical location.

Policy

A. Information Exchange Policy

1. UM shall protect the exchange and sharing of UM enterprise data.
2. Formal procedures and controls shall be in place to protect the exchange of UM enterprise data through the use of all forms of communication media.
3. The *Information Technology Acceptable Use Policy* shall define the acceptable use of electronic communication applications and systems.
4. The *Endpoint Protection Policy* shall define the use of anti-malware software to protect electronic communications against malicious code.
5. The *Wireless Network Security Policy* shall define the network controls necessary to

protect electronic communications accessed via the UM wireless network.

6. The *Encryption Policy* shall define the use of encryption to protect the exchange of electronic communications containing confidential data.
7. The *Media Protection Policy* shall define the retention and disposal guidelines for electronic communications containing confidential data.
8. The *Remote Access Policy* shall define the terms and conditions of access to UM's information assets and access to external information assets (over which the organization has no control) to protect electronic communications during remote access sessions.
9. The *Third Party Risk Management Policy* shall define the terms and conditions of electronic communications with other organizations owning, operating, and/or maintaining external information systems.
10. Workforce Members shall be educated according to the *Security Awareness and Training Policy* regarding UM policies and safe and approved practices for information exchange.

B. Information Exchange Agreements

1. Information exchange agreements shall be established and implemented for the exchange of information and software between UM and third parties.
2. Information exchange agreements shall not conflict with, nor shall they lower the standards and requirements stated, in any business associate agreement between UM and third parties.
3. Information exchange agreements may either be incorporated into a business associate agreement between UM and third parties or they may be a separate agreement.
4. Information exchange agreements shall specify the minimum set of controls for an information sharing arrangement, such as: responsibilities, procedures, technical standards, technical solutions, incident management, reporting and notification, access controls, auditing, logging and monitoring, and physical safeguards.
5. Information exchange agreements shall specify all applicable UM policies when

feasible.

6. UM policies, procedures, and standards regarding protection of the exchange of UM enterprise data shall be referenced in information exchange agreements when feasible.

C. Physical Media in Transit

1. Physical media containing confidential data shall be protected against unauthorized access, misuse, corruption, or destruction during transportation beyond UM's physical boundaries. Said media shall be encrypted meeting FIPS 140-2 encryption standard. Passphrases and other decryption means shall be provided via a separate transport medium from the data.
2. Controls and procedures shall be established to protect confidential data residing on physical media from unauthorized disclosure or modification while intransit.

D. Electronic Messaging, Texting, and Paging

1. Information involved in electronic messaging, texting, and textual paging shall be appropriately protected in accordance with UM information security policies, and federal and state laws and regulations.
2. Approval shall be obtained from the Chief Information Security Officer (CISO) prior to using external public services (e.g., instant messaging, file sharing, etc.) that are not approved by or managed by UM.
3. Electronic messages shall be encrypted throughout the duration of their end-to-end transport path according to the *Encryption Policy*.
4. Users shall never send unencrypted confidential data via end-user messaging technologies (e.g., email, instant messaging, textual paging, SMS texting, chat, etc.).

E. Interconnected Information Systems

1. Procedures shall be developed and implemented to protect confidential data associated with the interconnection of information systems.

2. Security and business implications shall be addressed for interconnecting information assets.

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 (approved 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.

Regulatory and Standards References

The following regulations and standards are applicable to this policy:

Information Exchange
HIPAA Policy: Security 11

- **HIPAA Regulatory References:** HIPAA § 164.308(b)(1), HIPAA § 164.308(b)(3), HIPAA § 164.310(b), HIPAA § 164.310(d)(1), HIPAA § 164.310(d)(2)(iii), HIPAA § 164.312(c)(1), HIPAA§ 164.312(c)(2), HIPAA § 164.312(e)(1), HIPAA § 164.312(e)(2)(i), HIPAA § 164.312(e)(2)(ii)

- **HITRUST References**: 09.s Information Exchange Policies and Procedures, 09.t Exchange Agreements, 09.u Physical Media in Transit, 09.v Electronic Messaging, 09.w Interconnected Business Information Systems
- **PCI References**: PCI DSS v3 4.1, PCI DSS v3 4.1.1, PCI DSS v3 4.2, PCI DSS v3 9.6.2

Related Documents:

- Information Technology Acceptable Use Policy
- Encryption Policy
- Glossary
- Media Protection Policy
- Remote Access Policy
- Privacy and Security Awareness and Training Policy
- Third Party Risk Management Policy
- Virus and Malware Protection Policy
- Wireless Network Security Policy

Approval

Chief Information Security Officer

<date>