Incident Management
HIPAA Policy: Security 24

Summary: Outlines procedures for responding to security breach incidents in HIPAA covered entities

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to ensure information security events, and weaknesses associated with information systems, are handled in a timely manner and allow corrective action to be taken.

This policy governs the actions required for reporting and responding to security incidents involving University of Mississippi's (UM) information assets. The policy ensures effective and consistent handling of such events to limit any potential impact to the confidentiality, availability and integrity of UM's information assets.

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 employees, contractors, students and all personnel affiliated with third parties who access or use UM's information assets, regardless of physical location.

Information Technology (IT) resources include all UM owned, licensed, leased, or managed hardware and software, and use of UM's network via a physical or wireless connection, regardless of the ownership of the computing device connected to the network. Management approves the use of information assets and takes appropriate action when unauthorized activity occurs.

This policy applies to information technology administered in individual departments; technology administered centrally; personally-owned computing devices connected by wire or wireless to UM's network; and to off-site computing devices that connect remotely to the network.

Incident Management
HIPAA Policy: Security 24

Policy

A. Information Security Incident Response Capability

1. UM establishes a formal Information Security Incident Response Capability (ISIRC) to respond, report (without fear of repercussion), escalate and treat breaches and reported security incidents.
2. The ISIRC is documented in the *Incident Response Plan* which shall include the following at a minimum:
   - Incident Response Team (IRT) roles and responsibilities
   - Incident Response Procedures
   - Incident Response Communications Plan
3. UM implements an insider threat program that includes a cross-discipline insider threat IRT.
4. All workforce members receive mandatory incident response training.
5. UM adheres to the HITECH Act requirements for responding to a data breach of protected health information (PHI) and reporting the breach to affected individuals, media, and federal agencies in accordance with federal and state laws and regulations.

B. Reporting Security Incidents

1. Security Incidents must be reported immediately to the Chief Information Security Officer (CISO). All workforce members and third party users are made aware of their responsibility to report any security incidents as quickly as possible.
2. Workforce members who report security incidents in good faith are protected against retaliation.
3. UM provides a means for anonymously reporting security incidents.

4. All workforce members and third party users of information assets and services reports any observed or suspected security weaknesses in information assets or services to the CISO.
5. Security Incidents involving civil or criminal charges are promptly reported to law enforcement (e.g., FBI, district attorney, state and local law enforcement, etc.).
6. Reports and communications are made without unreasonable delay and no later than 60 days after the discovery of a security incident, unless otherwise stated by law enforcement orally or in writing, according to the *Incident Response Communication Plan*.
7. A log of unauthorized access or disclosures of PHI is maintained by the Privacy Officer and submitted to the appropriate parties in accordance with the Data Breach Notification Policy.

C. Responding to Security Incidents

1. Management responsibilities and *Incident Response Procedures* are established to ensure a quick, effective, and orderly response to security incidents.
2. The CISO (or designee appointed by ISIRC) is the point of contact for coordinating security incident responses.
3. UM implements a formal *Incident Response Plan* to handle different types of information security incidents including, but not limited to:

   - information system failures and loss of service
   - malicious code
   - denial of service
   - errors resulting from incomplete or inaccurate business data
   - breaches of confidentiality and integrity
   - disclosures of unprotected health information
   - misuse of information systems
   - identity theft
   - unauthorized wireless access points

4. In addition to normal contingency plans, the Incident Response Plan also covers:
    a. analysis and identification of the cause of the incident
    b. containment
    c. increased monitoring of system use
    d. planning and implementation of corrective actions to prevent recurrence including:
        - Changing of passwords or security codes
        - Changing of devices that permit access to the systems or network
        - Modifying or terminating the account of individuals involved directly or indirectly by the incident (e.g., employees, third party, contractors, customers)
        - Assigning a single point of contact responsible for sharing information and coordinating responses.
5. The *Incident Response Plan* is communicated to the appropriate individuals in UM.
6. Following a security incident, audit trails and evidence are secured, system and data access controlled, emergency actions documented, actions reported to the Leadership Team, and system and control integrity confirmed.
7. A list of employees involved in security incidents is maintained with the resulting outcome from the investigation.
8. Change management requests are opened for events that require permanent fixes.
9. Where action against a person or UM after a security incident involves legal action (either civil or criminal), evidence is collected, retained, and presented in support of potential legal action in accordance with the rules for evidence in the relevant jurisdictions.

D. Reviewing Security Incidents

1. UM quantifies and monitors the types, volumes, and costs of security incidents.

2. The information gained from the evaluation of security incidents is used to identify recurring or high impact security incidents.
3. Security incidents (or a sample of security incidents) are reviewed on a periodic basis to identify necessary improvements to security controls.
4. Incident response testing exercises are planned at least annually. The results of the exercises must be documented and must be used to update the *Incident Response Plan* and *Incident Response Procedures*.

E. Sanctions

1. Workforce members cooperate with security incident investigations (e.g., federal and state investigations, disciplinary proceedings, etc.).
2. Workforce members that fail to report security incidents are disciplined in accordance with the *Sanctions Policy*.
3. UM takes disciplinary action against workforce members that fail to cooperate with federal, state and security incident investigations in accordance with the *Sanctions 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 (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:

- **HIPAA Regulatory References**: HIPAA §164.308(a)(1)(ii)(D), HIPAA §164.308(a)(6)(i), HIPAA §164.308(a)(6)(ii), HIPAA §164.314(a)(2)(i), HIPAA §164.404(a)(1), HIPAA §164.404(a)(2), HIPAA §164.404(b), HIPAA §164.404(c)(1), HIPAA §164.404(c)(2), HIPAA §164.404(d)(1), HIPAA §164.404(d)(2), HIPAA §164.404(d)(3), HIPAA §164.406(a), HIPAA §164.406(b), HIPAA §164.406(c), HIPAA §164.408(a), HIPAA §164.408(b), HIPAA §164.408(c), HIPAA §164.410(a)(1), HIPAA §164.410(a)(2), HIPAA §164.410(b), HIPAA §164.410(c)(1), HIPAA §164.410(c)(2), HIPAA §164.412, HIPAA §164.414(b)
- **HITRUST References**: 11.a Reporting Information Security Events, 11.b Reporting Security Weaknesses, 11.c Responsibilities and Procedures, 11.d Learning from Information Security Incidents, 11.e Collection of Evidence
- **PCI References**: PCI DSS v3 11.1.2, PCI DSS v3 12.10, PCI DSS v3 12.10.1, PCI DSS v3 12.10.2, PCI DSS v3 12.10.3, PCI DSS v3 12.10.4, PCI DSS v3 12.10.5

Incident Management
HIPAA Policy: Security 24

Related Documents:

- Glossary
- Incident Response Communications Log
- Incident Response Communications Plan
- Incident Response Contact List
- Incident Response Containment Form
- Incident Response Eradication Form
- Incident Response Form
- Incident Response Lessons Learned Survey
- Incident Response Plan
- Sanctions Policy

Approval

Chief Information Security Officer	<date>