Audit Logging and Monitor Policy
HIPAA Policy: Security 23

Summary: Outlines the auditing, logging, and monitoring activities to be conducted in HIPAA covered entities

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

The purpose of this policy is to address the regulatory requirements for safeguarding the confidentiality, integrity, and availability of the University of Mississippi's (UM) information assets through auditing, logging, and monitoring activities.

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, users, and all personnel affiliated with third parties who access or use UM information assets, regardless of physical location.

IT resources include all UM owned, licensed, leased, or managed hardware and software, and use of the UM network via a physical or wireless connection, regardless of the ownership of the computing device connected to the network.

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

Policy

A. Audit Policy

1. UM is committed to conducting business in compliance with all applicable laws, regulations and UM policies. In particular, UM is committed to compliance with the HIPAA Security Rule requiring security activity reviews for systems processing enterprise PHI data.

2. UM provides notice that the employee's actions may be monitored, and that the employee consents to such monitoring.

3. The planning activities for the annual audit that is required to comply with the *Information Security Management Program Policy* gives consideration to risk, involvement of technical and business staff, other ongoing projects, and business impacts that may impact the effectiveness of the audit.

4. Whenever possible, Business Associate Agreements (BAAs) with third parties define auditing and logging requirements and require monitoring of access to detect unauthorized activity and access to UM confidential data in accordance with the *Third Party Risk Management Policy*.

5. To ensure that appropriate safeguards are in place and effective, UM audits, logs, and monitors access and events to detect, report, and guard against:

    - Network vulnerabilities and intrusions
    - Performance problems and flaws in applications
    - Security violations
    - Unauthorized access to confidential data
    - Breaches in confidentiality and security of confidential data
    - Degradation or loss of information integrity (e.g., improper alteration or destruction of confidential data)

B. Auditable Events

1. UM develops and implements an *Audit Event Plan* to identify which systems, applications, and processes carry out auditing activities.

2. The *Audit Event Plan* defines what types of events are subject to auditing. At a minimum, the following events must be audited where feasible for each user:

    - Normal system events (e.g., startup, shutdown, login attempts, errors, security policy changes, software installations, etc.).

- Information changes (e.g., create, read, update, delete) including confidential data.
- Unauthorized access to confidential data.

3. The Chief Information Security Officer (CISO) periodically reviews and updates the *Audit Event Plan*. This review includes consideration of events that require auditing on a continuous basis, and events that require auditing in response to specific situations based upon an assessment of risk.

C. Content of Audit Records

1. UM defines the content for each type of audit record in the *Audit Event Plan*. Audit record content provides sufficient detail to determine whether a given individual took a particular action.

2. Audit records of information exchanges containing confidential data include the date, time, origin and destination of the message, but not its contents.

3. Disclosures of confidential data are logged according to the *Audit Event Plan*.

D. Audit Record Retention

1. UM retains audit records for a minimum of 90 days to provide support for after-the-fact investigations of security incidents and to meet regulatory and UM's record retention requirements.

2. Audit Records are archived for a minimum of six (6) years in accordance with the *Record Retention Policy*.

E. Audit Record Storage Capacity

1. UM allocates sufficient audit record storage capacity to reduce the likelihood of such capacity being exceeded.

2. UM configures auditing processes to reduce the likelihood of the audit record storage capacity being exceeded.

F. Audit Record Generation

1. Audit records recording user activities including access to Protected Health Information (PHI), exceptions, and events are generated and retained in accordance with the *Record Retention Policy* to assist in future investigations and access control monitoring.
2. Systems provide audit record generation capability as defined in the *Audit Event Plan*.
3. Where possible, systems allow system administrators to select which auditable events are audited by specific components of the system.
4. Systems generate audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. Audit record content also provides sufficient detail to determine whether a given individual took a particular action associated with an event.
5. Systems generate audit records that contain the activities of privileged users as defined in the *Audit Event Plan*.

G. Protection of Audit Records

1. Access to audit logging systems and system audit tools is limited to those with a job-related need according to the *Access Control Policy* to protect against possible misuse of the tools or compromise to the audit records.
2. Access to audit records is limited to those with a job-related need according to the *Access Control Policy* to prevent misuse or compromise of audit records.
3. Audit records are protected against modification and deletion according to the *Access Control Policy* to prevent unauthorized use.

4. Audit records for external-facing technologies (e.g., wireless, firewalls, DNS, etc.) are stored on a server located on the internal network.

H. Audit Monitoring, Review, Analysis and Reporting

1. UM reviews and analyzes audit records for evidence of suspicious, unusual, and inappropriate activity.
2. UM reports anomalous auditable events and related security incidents to the CISO, who is responsible for reporting security issues to the Leadership Team as appropriate.
3. UM adjusts the level of audit review, analysis, and reporting within systems when there is a change in risk to operations, assets, individuals, and other organizations, based on law enforcement information, intelligence information, or other credible sources of information.
4. UM establishes procedures for monitoring the use of systems and facilities to test the effectiveness of access control and security mechanisms. The results of the monitoring activities are reviewed on a regular basis.
5. Monitoring activities include execution of privileged operations, authorized access, unauthorized access attempts, and system alerts or failures.
6. UM meets all applicable legal requirements related to monitoring authorized access and unauthorized access attempts.
7. System Administrator activities are logged and reviewed on a regular basis.

I. Audit Reduction and Report Generation

1. UM utilizes audit reduction, review, and reporting techniques while ensuring that original audit records needed to support after-the-fact investigations are not altered.
2. Auditing and monitoring systems have the capability to automatically process audit records for events of interest based upon selectable event criteria.

J. Response to Alerts

1. Systems alert Office of Information Security (OIS) in the event of an audit processing failure and then OIS takes remediation action so gaps in the audit trail can be identified.
2. Systems generate alerts for suspicious activity and security alerts. The System Administrator analyzes the alerts and investigate suspicious activity or suspected violations.
3. System faults are logged and analyzed and the System Administrator takes appropriate remediation action.

K. Clock Synchronization

1. UM synchronizes system clocks with a central time server to support tracing and reconstitution of activity timelines.
2. System clocks are synchronized daily and at system boot.
3. UM restricts authorization to change system time settings to those with a job-related need.
4. Changes to system clocks on critical systems are logged, monitored and reviewed.

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 (with Committee approval) 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 Reference**: HIPAA §164.308(a)(1)(ii)(B), HIPAA §164.308(a)(1)(ii)(C), HIPAA §164.308(a)(1)(ii)(D), HIPAA §164.308(a)(3)(ii)(A), HIPAA §164.308(a)(4)(i), HIPAA §164.308(a)(4)(ii)(B), HIPAA §164.308(a)(5)(ii)(C), HIPAA §164.310(a)(2)(ii), HIPAA §164.312(b), HIPAA §164.316(a), HIPAA §164.316(b)(1), HIPAA §164.316(b)(2)(iii)
- **HITRUST Reference**: 06.i Information Systems Audit Controls, 06.j Protection of Information Systems Audit Tools, 09.aa Audit Logging, 09.ab Monitoring System Use, 09.ac Protection of Log Information, 09.ad Administrator and Operator Logs, 09.ae Fault Logging, 09.af Clock Synchronization
- **PCI Reference**: PCI DSS v3 10.1, PCI DSS v3 10.2, PCI DSS v3 10.2.1, PCI DSS v3 10.2.2, PCI DSS v3 10.2.3, PCI DSS v3 10.2.4, PCI DSS v3 10.2.5, PCI DSS v3 10.2.6, PCI DSS v3 10.2.7, PCI DSS v3 10.3, PCI DSS v3 10.3.1, PCI DSS v3 10.3.2, PCI DSS v3 10.3.3, PCI DSS v3 10.3.4, PCI DSS v3 10.3.5, PCI DSS v3 10.3.6, PCI DSS v3 10.4, PCI DSS v3 10.4.1, PCI DSS v3 10.4.3, PCI DSS v3 10.5, PCI DSS v3 10.5.1, PCI DSS v3 10.5.2, PCI DSS v3 10.5.3, PCI DSS v3 10.5.4, PCI DSS v3 10.5.5, PCI

Audit Logging and Monitor Policy
HIPAA Policy: Security 23

DSS v3 10.6, PCI DSS v3 10.6.1, PCI DSS v3 10.6.2, PCI DSS v3 10.6.3, PCI DSS v3 10.7,
PCI DSS v3 11.5, PCI DSS v3 11.5.1, PCI DSS v3 A.1.3

Related Documents:

- Access Control Policy
- Audit Event Plan
- Business Associate Agreement Template (BAA)
- Glossary
- Information Security Management Program Policy
- Network Protection Policy
- Record Retention Policy
- Third Party Risk Management Policy

Approval

Chief Information Security Officer

<date>