Audit Logging and Monitor Policy
HIPAA Policy: Security 23

Purpose
The purpose of this policy is to ensure compliance to the HIPAA Security Rule (45 CFR Parts 160 and 164, Subparts A and C) and to set the expectations and requirements for University of Mississippi (UM) for safeguarding the confidentiality, integrity, and availability of the UM’s information assets (HIPAA electronic protected health information and other confidential data) through auditing, logging, and monitoring activities.

Scope
This policy applies only to the Covered Entities as defined in the UM HIPAA Hybrid Policy. This policy applies to all employees, students, contractors, and any other individual with login credentials (“Users”) to UM information assets. This policy is available to all Users and to all individuals responsible for implementing procedures for this policy.

Policy
A. Audit Policy
1. UM is committed to conducting business in compliance with all applicable laws, regulations, and UM policies, including compliance with the HIPAA Security Rule requiring security activity reviews for systems processing enterprise electronic protected health information (ePHI) data.
2. UM provides notice that all Users can be monitored/audited for all information systems that contain ePHI, including departmental shared network drives, and other systems as relevant.
3. UM implements audit controls and procedural mechanisms that record and examine access and disclosure for all systems that contain ePHI, including departmental shared network drives, and other systems as relevant.
4. To ensure that appropriate safeguards are in place and effective, UM conducts information system activity reviews by regularly reviewing records of information system activity such as audit logs, access reports and security incident tracking reports.

B. Auditable Events
1. UM develops and implements audit plans to identify which systems, applications, and processes carry out auditing activities.
2. The audit plans define what types of events are subject to auditing, as well as, which auditable events will be required to be retained within systems activity and security incident tracking reports.
3. UM ensures at least the following can be audited for information systems that contain ePHI:
   - 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 ePHI and confidential data.
   - Unauthorized access to ePHI and confidential data.
4. UM periodically reviews and updates its audit plans. 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.

Pursuant to UM’s Access Control Policy all Users have a unique user id. that can be identified tracked and monitored.
C. Audit Monitoring, Review, Analysis, and Reporting

1. UM tracks activities of all Users by unique user identification.
2. UM monitors log-in attempts and reporting discrepancies.
3. Access to audit logging systems and system audit tools is limited to those with a job-related function.
4. UM reviews and analyzes audit logs and security related information systems alerts for evidence of suspicious or unusual activity.
5. UM investigates these possible security incidents and determines whether such events were false positives or confirmed security incidents.
6. 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.
7. 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.
8. Monitoring activities include execution of privileged operations, authorized access, unauthorized access attempts, and system alerts or failures.
9. UM meets all applicable legal requirements related to monitoring authorized access and unauthorized access attempts.

D. System Activity Review and Security Incident Records

1. UM retains system-level security logs for at least six (6) years.
2. UM retains ePHI access and modification reports, system activity reviews and security incident tracking report for at least six (6) years.
3. UM protects these records from modification or deletion.
4. System-level security logs for external-facing technologies (e.g., wireless, firewalls, domain name service, etc.) are stored on a server located on the internal network.
5. UM allocates sufficient record storage capacity to reduce the likelihood of such capacity being exceeded.

Policy Compliance

Enforcement

The Chief Information Security Officer (CISO), or designee, has general responsibility for the implementation and enforcement of this policy.

Future Revisions

UM periodically reviews and updates its policies and procedures as needed in response to environmental or operational changes affecting the security of ePHI. UM reserves the right to add, delete, or revise any provision of this Policy or any other Information Security policy at any time without prior notice as long as such changes are compliant with the Security Rule. All UM security policies are subject to a review process that includes, but is not limited to, designated representatives from the Office of Information Technology and the Office of General Counsel.

Sanctions
Any User violating this or any security policies or applicable local, state, or federal laws while using UM’s computing environment is subject to disciplinary actions deemed appropriate, up to and including termination. In cases in which PHI is involved, the CISO will collaborate with the Office of General Counsel to recommend appropriate sanctions.

Exceptions
The process to request exceptions to Information Security policies is available. Requests are documented, then evaluated based on the potential risks to business, as well as, HIPAA Security Rule. The CISO, or designee, can approve exceptions necessary to meet a business or patient care need. Alternatively, the CISO, or designee, may request compensating controls and processes to ensure UM adherence to the HIPAA Security Rule. All approved policy exceptions will be reviewed annually for appropriateness by the CISO, or designee, and may be revoked at any time.