Division of
Information Technology

Texas A&M University

Electronic Protected Health Information SYSTEM ACTIVITY REVIEW Control

Table of Contents

Purpose

The purpose is to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Scope

This policy applies to TAMU in its entirety, including all systems that process sensitive information.
HIPPA Safeguard: 45.CFR.164.308 (a)(1)(ii)(D), Security management Process Information System Activity

Roles and Responsibilities

The TAMU Chief Information Security Officer will clearly identify:

- The system(s) with Electronic Protected Health Information (ePHI) that require review
- The types of access reports that are to be generated
- The security incident tracking reports that are to be generated to analyze security violations
- The individual(s) responsible for reviewing all logs and reports

When determining the responsibility for information review, a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

Security Control

TAMU will identify all critical systems that process ePHI. TAMU will implement security procedures to regularly review the records of information system activity on all such critical systems.
HIPPA Safeguard: 45.CFR.164.308 (a)(1)(ii)(D), Security management Process Information System Activity

Procedure(s)

A regular review of information system activity on critical systems containing and/or related to ePHI requires utilization of the information that will be maintained in audit logs, access reports and must be included in security incident tracking reports as reasonable and appropriate:

- Dates and times of ePHI information resource application log-on and log-off as noted in TAMU Security Control AU-8 (http://cio.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=AU-8).
- Associated session activities, exceptions, and security events as defined in TAMU Security Control AU-3 (http://cio.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=AU-3).

TAMU will attempt wherever reasonable, appropriate, and technically feasible to record:

- Who (Unique User ID), did
- What action (Read, write, edit, delete, print, etc.), to
- What data (Server, DB, instance, table, row, field),
- When (Enterprise wide timestamp), and from
- Where (Hostname or Fully Qualified Domain Name, IP address, local or remote access)

Safeguards must be deployed to protect against unauthorized changes and operational problems including:

- The logging facility being deactivated
- Alterations to the message types that are recorded
- Log files being edited or deleted
- Log file media becoming exhausted, and either failing to record events or overwriting itself as noted in TAMU Security Control AU-4, http://cio.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=AU-4 .

TAMU information resource custodians protecting ePHI will develop a process to periodically review information system activity, log-in attempts, access reports, and

security incident tracking reports to ensure that implemented security controls are effective and that ePHI has not been potentially compromised. The process will include the following:

- Maintain logs as stated in the "Electronic Personal Health Information Audit Log Requirements" HIPAA Security Control.
- Maintain documentation that prove periodic log reviews were conducted for six years.
- Define responsibility for information system activity review, including log-in monitoring, access reports, and security incident tracking reports.
- All ePHI access reports must be maintained for six years to meet the accounting of disclosures that may be requested. (§164.528(a))
- All documentation regarding security incidents related to ePHI must be maintained for six years to meet the requirements of Health and Human Services Office of Civil Rights audit compliance requirements.
- Review of whether the information systems functions are adequately used and monitored.

Logging must be enabled at the operating system, application/database, and system/workstation level.

Logs must be reviewed in response to suspected or reported security problems on systems containing restricted data or as requested by TAMU Division of IT Cybersecurity.

Information Resource Custodians are responsible for determining which systems require scheduled log review.

Log review shall include investigation of suspicious activity, including escalation to TAMU Division of IT Cybersecurity as appropriate.

Individuals shall <u>not</u> be assigned to be the sole reviewers of their own ePHI activity.

Logs must be accessed, secured and protected according to the nature of the information they may contain.

Contact and Questions

Please send all inquiries to: *ra@tamu.edu*