Division of
Information Technology

Texas A&M University

Electronic Protected Health Information AUDIT LOG REQUIREMENTS Control

Table of Contents

Purpose

The purpose is to implement hardware, software, and/or procedural mechanisms that record and examine activity in information resource assets that contain or use electronic Protected Health Information (ePHI).

Scope

This policy applies to TAMU in its entirety, including all workforce members. This policy also applies to all systems, networks, and applications, as well as all facilities, which process, store or transmit ePHI.
HIPPA Safeguard: 45.CFR.164.312 (b), Audit Controls Standard.

Roles and Responsibilities

The Chief Information Security Officer (CISO), or delegate will be responsible for ensuring the implementation of this policy.

Security Control

TAMU will identify critical systems with ePHI that require event auditing capabilities and define the events to be audited on all such systems.

TAMU will require procedures to regularly review records of information resources assets ePHI activity, such as audit logs, access reports, and security incident tracking reports.

Procedure(s)

TAMU information resources shall log certain activities that occur on networks, systems, and applications. These logs shall provide sufficient data to support incident investigation and comprehensive audits of compliance with the documented TAMU Information Resource requirements found in Rules, Standard Administrative Procedures (SAPs), Security Controls, including CUI and HIPAA special requirements, and unit IT guidelines. Logging and auditing shall be implemented using the following guidelines:

Activity Logs and Audit Trails – There are certain activities that occur on networks, systems and applications that shall be logged. These include, but are not limited to, activities such as data requests, data transfers, changes to configuration files, and the addition, deletion, or modification of access. Logs of computer security events shall provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with, the TAMU Information Resources requirements including the audit event content requirements of TAMU Security Control AU-3, http://cio.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=AU-3 .

In addition, ePHI requires more granularity for detail related to both user and information accessed or modified. For the use, storage, and transmission of ePHI there are further audit log requirements as follows.

Security Event Logging Detail – Logs shall be created that can be used to monitor activities that can affect network, system or application security. These logs shall record the following:

- Intrusion activity
  - Failed login attempts with an invalid User ID
  - Failed login attempts with a valid User ID (password guessing attempts)
  - Failed password change attempts
  - Attempts to use privileges that have not been authorized

- User ID administration activity
  - Modifications
  - Additions
  - Deletions
  - Disabling
  - Re-enabling
  - Changes to the privileges of users

- System activity
  - Start-up

    - Shut-down

- Hardware
    - Hardware and disk media errors
    - Maintenance activity

- System anomalies
    - Initialization sequences
    - Logons and errors
    - System processes and performance
    - System resources utilization

Perimeter Protection Logging Detail – Logs shall be created that can be used to monitor activities on perimeter devices, including firewalls and routers. These logs shall record the following:

- Device activity
    - Packet screening denials originating from trusted and un-trusted networks
    - User Account Management
    - Modification of packet filters
    - Application errors
    - System errors
    - System shutdown and reboot

ePHI User Activity Logging Detail – Logs shall be created in such a manner that individual events are attributed to individual User IDs. Networks and applications shall log activity using the following guidelines:

- User activity involving ePHI should be logged at the field level, and shall record the following:
    - User IDs
    - Access date/time
    - User Access
    - Record access
    - Field access relating to records
    - User Actions
    - Additions at the record and field level
    - Modifications at the record and field level
    - Deletions at the record and field level

- If user activity involving ePHI cannot be logged at the field level, activity logging should be maintained at the record level, and shall record the following:
    - User IDs
    - Action date/time
    - User Access
    - Record access
    - User Actions

  - Additions at the record level
  - Modifications at the record level
  - Deletions at the record field level

- If user activity involving ePHI cannot be logged at the record level, activity logging should be maintained at the system access level. The ability to only do ePHI system access logging must be documented to tamu-it-ra@tamu.edu. The ePHI system access level logging shall be recorded, including:
  - User IDs
  - Logon date/time
  - Logoff date/time
  - Password change date/time
  - Applications invoked
  - Attempted access to unauthorized data
  - Use of authorized advanced privileges (security bypass, etc.)
  - Changes to critical application system files
  - Modifications

Backup, Archive, And Protection – Log files shall be saved to other media and secured in off-site or other appropriate storage.

- Logs shall be rolled (a new log activated, the old log saved) rather than being overwritten (the same log is used again, losing data).

- Log files are CONFIDENTIAL and shall be protected such that no individual can modify or delete the logs.

- Individuals authorized to view logs as appropriate under the rule of least privilege include the unit IT, unit-designated HIPAA officials, TAMU IT, TAMU Privacy Officer, and University Risk and Compliance.

- If an unauthorized individual needs access to these logs, they shall request access in writing and obtain written permission from the Information Owner. It must be established that they have received HIPAA training.

Backup Retention – Log files shall be retained for a period of time so as to accomplish their purpose, and according to the following guidelines:

- Activity logs shall be retained as specified by local IT Policy, unit record retention standards, TAMUS Records Retention Schedule, or contractual, regulatory, or statutory mandates.

- *Electronic Medical Record log information on user activity should be maintained for six (6) years. (http://rules-saps.tamu.edu/PDFs/16.99.99.M0.25.pdf) It is* recommended that other security event and user activity logs *related to ePHI infrastructure* be retained for a period of one (1) year. If log files cannot be retained for one (1) year, log files shall be maintained for no less than ninety (90) days.

Clock Synchronization – The internal clocks of systems that generate activity on TAMU networks and applications shall reflect the current time accurately as defined in TAMU IT Security Control AU-8, http://cio.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=AU-8 .

Deactivation, Modification, Or Deletion – Mechanisms to detect and record significant computer security events shall be resistant to attacks. These attacks include attempts to deactivate, modify, or delete the logging software and/or the logs themselves.

Auditing Log Reviews – Unit information resources owners, unit information resource custodians, or unit-designated HIPAA officials shall monitor the ePHI security event logs created by the information resource assets containing ePHI to ensure that inappropriate behavior or potential intrusions are recognized and addressed.

- Audit access logs shall be examined for failed logon attempts and other security events on a routine basis. It is recommended that this be conducted weekly, or if the ePHI has limited use monthly. Electronic Medical Records applications event logs should be reviewed monthly for suspicious activities such as extensive single user access or bulk modifications but the access review should not exceed ninety (90) days.

- Automated utilities may be used to assist in audit log reviews. However, manual reviews should be conducted periodically to identify unusual, unexpected or suspicious behavior not identified through automated reviews.

- It is recommended that reviews of user activity also be conducted if such reviews could assist in identifying unusual, unexpected, or suspicious behavior.

- Centralized monitoring of all unit ePHI applications is preferred over individual system monitoring. If centralized monitoring is not available then individual system monitoring still must be conducted.

- Incident Reporting And Notification – Any incidents found in the ePHI log auditing procedure shall be handled according to unit documented incident response procedure required by TAMU Security Control IR-1, http://cio.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=IR-1

Contact and Questions

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