VERMONT
AGENCY OF HUMAN SERVICES

AHS Policy Title: 5.13 Information Security Audit and Logging Policy

Policy Information

Revision Date:

02/21/2023

Revision Number:

1.3

Attachments/Related Documents:

none

Effective Date:

05/01/2020

☒ Trauma Informed Review

☒ Racial Equity Review

Authorizing Signature:

Jenney Samuelson,
Agency of Human Services Secretary

Policy Statement:

To establish high-level requirements, organizational responsibilities, and managerial commitment for an Information Security Audit and Logging Policy that ensures the confidentiality, integrity, and availability of information and systems within the Agency of Human Services (AHS) in compliance with all applicable State and Federal Law, regulations, or policies.

Background:

The HIPAA administrative safeguards (45 C.F.R. §§164.308(a)(1)(ii)(D)) require AHS to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. AHS also is required under HIPAA (45 C.F.R. §§164.308(a)(8)) to perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under that HIPAA rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which the AHS security policies and procedures meet the requirements of HIPAA.

The HIPAA technical safeguards for audit controls (45 C.F.R. §§164.312(b)) require AHS to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

This policy assures compliance with HIPAA, as well as other state and federal laws relating to

information security audit and logging, such as those established by CMS, Internal Revenue Service, Social Security Administration, Criminal Justice Information Services, and Vermont law.

This policy follows the National Institute of Standard and Technology (NIST) SP 800-53 Rev.5 framework. The purpose of this policy is to establish Information Security Audit and Logging protocols.

The policy details how AHS complies with Federal information security standards for implementing and maintaining an Information Security Audit and Logging Policy.

Scope:

This policy governs AHS Information Security Audit and Logging protocols and associated standards and procedures.

Roles and Responsibilities:

AHS Secretary – Responsible for making a final review and approval of this policy.

AHS Policy Committee - Responsible for making a final review of this policy.

Chief Information Security Officer – Responsible for reviewing and approving this policy prior to AHS Policy Committee. The CISO will report all compliance-related activities pertaining to this policy to AHS Secretary.

Authorizing Official - responsible for operating an information system authorized pursuant to AHS Policy 5.08 at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individual's data.

AHS Information Security Director – responsible for:

- creating procedures and standards to meet the requirements established in this policy.
- reporting all matters pertaining to the AHS's compliance with this policy to the CISO and the Authorizing Official; and
- ensuring that this policy is reviewed and updated (if necessary) at least annually.

Protocols:

General

The AHS Information Security Director will ensure that information systems are capable of auditing all events defined in this policy. If an AHS information system cannot be configured to log the minimum required event types, the AHS Information Security Director will document an exception, receive approval from the Authorizing Official, and add the exception to the AHS risk register.

The AHS Information Security Director will employ methods for coordinating audit information among external organizations when audit information is transmitted across organizational boundaries.

If an AHS information system cannot be configured to meet the minimum information security audit and logging standards and procedures, the AHS Information Security Director will document an exception, receive approval from the Authorizing Official, and add the exception to the AHS risk register.

Event Types

At minimum, all AHS information systems will be capable of auditing the following events:

- User Logon/Logoff
- Remote access activity
- Invalid authentication attempts
- Escalation of Privileges
- Use of privileged commands or functions
- Access to sensitive data
- Modification or deletion of sensitive data
- Account/user management activities
- Indicators of potential attacks or compromises
- Inbound and outbound communications traffic

Other event types as required by law or regulation.

Security technologies, capable of generating logs or alerts, will also be enabled and be monitored on a continuous basis. Such alerts include:

- Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) events
- Firewall alerts
- Anti-virus or anti-malware alerts
- Configuration or compliance scan alerts

Log Contents

Logs will be detailed enough so that the following may be determined based on review of log contents:

- The source and destination of a transaction or event.
- The time the event occurred which will be synchronized to an authoritative time source.
- The information systems involved in the event.

- The identifier or account that performed the actions.
- The event action and description.

Confidentiality and Integrity of Log Data

Audit information and audit tools will be protected from unauthorized access, modification, and deletion. Access to log data or platforms designed to review logs will be restricted only to authorized individuals who perform audit review, analysis, and reporting. These individuals will also not have access to production systems to ensure effective separation of duties.

Audit data generated from information systems will be stored securely separate from the information system that generated the logs, with access granted only to authorized personnel with a legitimate business need to access, view, or manipulate log data. Separation of duties will be considered when authorizing access to log data; Administrators of systems should not be able to delete or purge log data independently. Delete and/or write privileges to any servers storing log files will be restricted and follow the principle of least privilege with an approved business purpose for any user with this access.

Privileged User Access Logs

The use of privileged accounts will be audited (recorded in security event logs, on SIEM platforms) and the corresponding audit logs stored in a location the privileged users do not have access to (e.g., separate/dedicated logging server)

Data Normalization and Aggregation

To adequately capture and efficiently analyze event activity on AHS information systems, automated mechanisms, such as Security Information Event Management (SIEM) tools, will be employed to aggregate and normalize event data across the entire environment. Aggregation enables the collection and cross-referencing of event sources – in the event of a cyber security incident, this practice will aid the investigation by providing a trail of evidence to follow.

Monitoring and Alerting

SIEM tools will be configured to monitor for specific activities on information systems (such as indicators of potential attacks, inbound and outbound traffic, anomalies, etc.) and will alert the appropriate response personnel when event indicators are triggered.

Information systems must be configured to alert designated personnel in the event of audit production or processing failures. If audit production mechanisms fail, these information systems must also be configured to continue logging until administrator intervention.

Log Review and Analysis

Authorized individuals will review and analyze audit logs daily for indications of inappropriate or unusual activity, and report findings to designated personnel. The review and analysis of audit logs will not alter the original content of audit records Updates to review methods and reporting of audit information will correspond to changes to risk against operations, assets, individuals, or other organizations in response to credible sources.

Retention

Audit logs will be retained based on retention periods required by applicable requirements (be it from NIST, MARS-E, HIPAA, etc.), and local, state, or federal regulations, superseding AHS policy, or contractual obligations for which AHS is a party. Audit logs will be securely deleted following the required retention periods.

Storage Capacity

AHS will ensure that sufficient storage is available for all logs in accordance with any applicable retention periods. Storage capacity thresholds will be established and monitored. Alerts will be sent to the AHS security team to request an increase in capacity as needed.

Time Stamps

The information system uses internal clocks to generate time stamps for audit records. Time stamps will be configured in either Coordinated Universal Time or Greenwich Mean Time.

Protection of Audit Records

The information system will protect audit information and audit tools from unauthorized access, modification, and deletion.

Non-Repudiation

The information system will protect against an individual from falsely denying having performed a particular action.

System Correlated Audit Trail

AHS will develop standards and procedures for information systems that compile audit records from defined information system components into a system-wide/time correlated audit trail.

Log Review and Analysis Standards

AHS will develop standards for reviewing audit logs and event types that include the frequency that reviews occur.

Enforcement:

The AHS Secretary may initiate reviews, assessments or other means to ensure that policies, guidelines or standards are being followed.

Authorities:

- Health Insurance Portability and Accountability Act (HIPAA) Security Rule: 45 CFR Part 160 and Subparts A and C of Part 164
- National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5
- Centers for Medicare and Medicaid Services (CMS), Minimum Acceptable Risk Standards

for Exchanges (MARS-E), Version 2.2, September 16, 2021

- IRS Publication 1075 (Rev. 11-2021)
- Social Security Administration (SSA), *Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information With The Social Security Administration* based on: Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347, the Privacy Act of 1974 and SSA's own policies, procedures, and directives
- Criminal Justice Information Services (CJIS), Security Policy, Version 5.9.1, 10/01/2022, CJSD-ITS-DOC-08140-5.9.1

References:

MARS-E	IRS Pub 1075	SSA	HIPAA	CJIS
AU-1	9.3.3.1	5.4	§164.308(a)(1)(ii)(D)	5.4
AU-2			§164.308(a)(8)	5.4.1
AU-2 (3)	AU-1		§164.312(b)	5.4.1.1
AU-3	AU-2			5.4.2
AU-3 (1)	AU-3			5.4.3
AU-4	AU-4			5.4.4
AU-5	AU-5			5.4.5
AU-6	AU-6			5.4.6
AU-6 (1)	AU-7			5.4.7
AU-6 (3)	AU-8			
AU-7	AU-9			
AU-7 (1)	AU-11			
AU-8	AU-12			
AU-8 (1)	AU-16			
AU-9AU-9 (2)				
AU-9 (4)				
AU-11				
AU-12				

Document Review and Revision Control

Version	Review Date	Author/Reviewer	Description
1.0	4/1/2020	Emily Wivell	New AHS policy replacing VHC and DCF policies.
1.1	7/6/2021	Emily Wivell	Annual Renewal and Conforming Changes
1.2	9/8/2022	Emily Wivell	Annual Review
1.3	02/21/2023	Emily Wivell	Annual Review

Appendix:

None.