CONE HEALTH	**Guideline:** ITS Audit Logging and Monitoring Procedure	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 02/14/2024
	Effective Date: 02/14/2024	**Next Review Date:** 02/14/2025

INTENDED AUDIENCE:

- System administrators
- Operations/business owners

PROCEDURE:

In accordance with the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), Cone Health is committed to ensuring the confidentiality, integrity, and availability of all protected health information (PHI/ePHI), confidential data, and sensitive data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.

The purpose of this procedure is to define roles, responsibilities, and processes associated with auditing and monitoring user and system activity on production, test, and development systems.

Scope and Goals:

This procedure applies to all Cone Health information systems and the users who utilize the systems. The goals for auditing and monitoring systems and users are as follows:

- Compliance with federal regulatory requirements
- Identify, respond, and mitigate:
    - Insider threat deterrence
    - Fraudulent activity
    - External intrusions
    - Security risks
    - System performance problems and flaws
- Capture evidence for taking disciplinary action, forensic analysis and potential civil and criminal litigation

Responsibilities:

Chief Information Security Officer (CISO):

The CISO is responsible for, but not limited to, the following activities:

- Revisions, implementation, workforce education, interpretation, and enforcement of this procedure.
- Assisting system/application administrators with implementation of log-on banners.
- Ensuring all users are subject to audit and monitoring, to include system/application administrators, privileged users, etc.
- Ensuring all systems that store, process, or transmit covered information are subject to audit and monitoring.
- Ensuring that all audit systems used are able to provide filtering capabilities (able to find specific logging events based on selectable criteria) and reporting functionality.

- Ensuring the ability to manipulate, disable, and delete audit logs is restricted or monitored to detect these activities and positively identify anyone who executes these functions.
- Ensuring the access to audit logs is restricted to the least number of people (e.g., administrators) as possible.
- Ensuring that the workforce members who are responsible for the management and review of the audit logging and monitoring systems are qualified to perform the duties. For any systems that require a certification, ensure these are obtained by the applicable workforce members.

Management:

Management will ensure that business units identify operations/business owners for their respective systems (i.e., People and Culture system = VP of People and Culture, Financial system = CFO, etc.) and that they comply with this procedure.

Management will work with general counsel to ensure all applicable legal requirements related to monitoring workforce system use and activity are met.

System/Application Administrators:

System/application administrators are responsible for, but not limited to, the following activities

- Ensuring all users, to include administrators and privileged users, are being monitored and their activities are captured in the system audit logs.
- Restricting all users, to include administrators and privileged users, the ability to manipulate, disable, and delete audit logs, and monitoring to detect these activities and positively identify anyone who executes these functions.
- Configuring audit log capability to capture all activity required by this procedure.
- Reviewing audit logs daily for unusual or suspicious activity and taking appropriate action, to include informing the CISO.
- Reviewing any unauthorized remote access connections to the organization's network and information systems upon alert receipt and taking appropriate action when unauthorized connections are discovered. In addition, review with management on a quarterly basis.
- Periodically checking to make sure the audit logging and monitoring systems are functioning and collecting data as expected and fixing any issues that are discovered.

Operations/Business Owners:

Operations/business owners are responsible for, but not limited to, the following activities

- Restricting user access to audit logs to the minimum necessary based on job responsibilities.
- Ensuring all user activity is being monitored and reviewed, to include system/application administrator and privileged user activity.
- Ensuring the ability to manipulate, disable, and delete audit logs is restricted or monitored to detect these activities and positively identify anyone who executes these functions.

Types of Audit Logs:

All systems have one audit log. Described below are several types of audit activity that are captured in logs:

- User: User level audit trails generally monitor and log all commands directly initiated by the user, all identification and authentication attempts, and files and resources accessed.
- Application/Database: Application/database level audit trails generally monitor and log user activities, including data files opened and closed, specific actions defined in this procedure, and printing reports.
- System: System level audit trails generally monitor and log user activities, applications accessed, and other system defined specific actions.
- Network: Network level audit trails generally monitor what is operating, unauthorized access attempts, and vulnerabilities.

General Event Logging:
The following general attributes are mandatory audit requirements:

- Audit log entries must include:
  - The user ID or service name that initiated an event
  - The unique data subject ID or function that was performed
  - Date and time the event was performed (timestamp)
- Any privileged operations (root, admin, security, supervisory, etc.) performed by the endpoint
- System storage capacity issues
- Packet denials (network perimeter devices)
- System startup, reboot, or shutdown
- Covered information will never be captured in audit logs. Approval is needed for any exceptions to this rule.

NOTE: Cone Health will at times require a unique and elevated level of system auditing and monitoring for the purpose of:

- Business continuity
- Complying with federal regulations and statutory requirements

Security Event Logging:
At a minimum, the following security related events will be captured in audit logs:

- Successful and unsuccessful access attempts to access the system
- User accounts that have been inactive for longer than 30 days
- Changes to access rights and privileges
- Unsuccessful attempts to use or access privileged operations
- Inbound and outbound communications from external entities
- File integrity monitoring
- System configuration and security policy (i.e., function/control) changes
- Date and time password changes are made
- Access to and changes to covered information, critical resources, and processes involved
- Attempts to reactivate or access disabled accounts
- Changes to access rights/privileges and security attributes, specifically those that increase authority
- System alerts or failures
- Access to and attempts to modify audit log attributes

- Authorized and unauthorized remote access connections to the organization's network

Data Repositories (e.g., databases, directories, folders, etc.):
Data repositories containing covered information will record the following activity by name, date, and time of event:

- Creation, viewing, modification, copying, moving, or deletion of covered information
- Creation, viewing, modification, copying, moving, or deletion of objects, tables, cells, folders, directories, etc.
- Authorized access and unsuccessful attempts to access databases or network folders and directories
- Every 90 days, Cone Health will review each extract of covered information on these repositories and determine if the data can be erased or its use is still required

Security Event Notification:
Systems will be configured to alert administrators of malicious or suspicious activity (system capabilities permitting). All alerts related to suspicious activity or suspected violations will be analyzed and investigated. This type of activity is defined as, but not limited to:

- Numerous failed attempts (in a short period of time) to access critical files, objects, directories, process, administrative/privileged operations, etc.
- Suspicious activity or inappropriate use of system privileges, with extra attention to administrative/privileged accounts.
- Unannounced changes to critical files, objects, directories, processes, etc.
- Attempts to modify audit log attributes, change or delete audit logs.

Data Exchange:
An audit log will be maintained for all forms of data exchange (i.e., email, instant messaging, texting, etc.). Logs will capture the date, time, origin, and destination of messages received and transmitted, but not the contents of the message.

All disclosures of covered information within or outside of the organization will be captured in the audit log and identified by type of disclosure, date/time of the event, recipient, and sender.

Audit Log Security Controls:
Audit logs shall be protected against unauthorized access or modification by ensuring that they are set to "read-only." System administrators, privileged users, or anyone who has the rights to access system audit logs shall be restricted to "read-only." This is done to protect audit logs from unauthorized access and manipulation. At Cone Health, no single person should be able to access, modify, or use information systems without authorization or detection at some point in the audit logging systems.

Whenever possible, audit trail information shall be stored on a separate system to minimize the impact auditing may have on production resources. Where applicable, system administrators will synchronize their system clocks on a weekly basis (or sooner if needed, e.g., daylight savings time, system reset, etc.) to avoid time drift and to detect tampering. Accurate clock time is needed to protect the integrity of the information being recorded in audit logs. Time data must be controlled and protected to prevent any unauthorized access or altering.

Audit logs for all devices, especially those that are for external facing technologies (e.g., wireless, firewalls, webservers, portals, DNS, etc.) are maintained on a server within the internal network.

Protection of Audit Tools:
Access to audit tools (i.e., services and hardware) must be strictly controlled against misuse or compromise. Use of these tools by unauthorized or ill-trained people can result in unnecessary downtime, disruption of business, and privacy issues. The CISO and operations/business owners will approve the use of audit tools. These tools will include, but are not limited to:

- Scanning tools and devices
- War dialing software
- Password cracking utilities
- Network "sniffers"
- Passive and active intrusion detection systems

Audit Requests for Specific Cause:
Requests to monitor user activity or to access a workforce member's account without their knowledge and with the intent to investigate fraud or inappropriate activity, to discipline or terminate the member, or to dismiss a contractor/consultant requires approval from People and Culture (HR). Requests will be sent by People and Culture to the CISO, who will work with Information and Technology Services (ITS) and management and if appropriate, coordinate and setup monitoring. These requests must include the time frame, frequency, and nature of the request.

Situations that do not require approval are:

- Request to review telephone logs as long as they are not directed at a specific employee.
- Request to access terminated employee's email or voice mail accounts.
- Request from an individual to allow someone else to access their email, voice mail, or telephone calls (e.g., manager giving access to their administrative support person).

Evaluation and Reporting of Audit Findings:
Audit log information must be reviewed daily for suspicious or malicious activity. Audit findings shall be reported to appropriate operations/business owners in a timely manner. Significant findings that could indicate a security breach has or is likely to occur shall be immediately reported to the CISO.

Routine findings shall be documented and reported to operations/business owners and the CISO on a monthly basis.

False positives must also be addressed and for significant events, potential impact analysis must be conducted for critical information systems.

Reports of audit results shall be limited to internal use on a minimum necessary/need-to-know basis. Audit results shall not be disclosed externally without the chief privacy officer's and/or legal counsel approval.

Security audits could constitute an internal, confidential monitoring practice that will be used to evaluate a workforce member's performance. Care shall be taken to ensure that the results of these types of audits are only provided to the appropriate supervisor and People and Culture. Audit information that could disclose organizational risks will be shared with extreme caution.

Automated Audit Systems:
Cone Health will use automated systems and tools (e.g., a Security Information and Event Management or SIEM) to collect audit log information from the all key systems throughout the organization. The tool is used to consolidate, analyze in real-time, send alerts, and report on key events identified in this procedure. To ensure the tools are current on the threats they should be looking for, the logs and other types of data collected will be correlated with several non-technical inputs (i.e., security newsfeeds/newsletters).

Auditing Business Associate and/or Vendor Access and Activity:
Periodic monitoring of business associate and vendor information system activity shall be carried out to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between Cone Health and the external entity.

If it is determined that the business associate or vendor has exceeded the scope of access privileges Cone Health leadership will reassess the business relationship.

If it is determined that a business associate has violated the terms of their contract, Cone Health must take immediate action to remediate the situation. Continued violations will result in the termination of the business relationship.

Audit Log Retention:
Audit logs shall be maintained based on organizational needs. For the purpose of HIPAA compliance, reports summarizing audit activities shall be retained for a period of six years. Retention requirements for the actual audit logs are as follows:

- Active logging must be available for at least 90 days.
- Once logging data has gone beyond 90 days, the data must be archived for 1 year, unless otherwise instructed by People and Culture, legal counsel, or other entity (i.e., evidence, investigation, etc.).
- Logging data must be backed-up as part of the system's regular backup process.
- The data itself must also be periodically audited by the security officer for availability and integrity purposes.
- Management has given consideration to extending retention of audit logs associate with online activities involving pending incidents/breaches, investigations, litigation, and disciplinary action. All incidents that are logged are reviewed by management at a minimum annually.

Systems will shut down and stop generating audit logs or overwrite the oldest records first, should storage media (i.e., hard drive) become unavailable. An alert will be sent to designated personnel for any audit processing failure.

Guideline: ITS Audit Logging and Monitoring Procedure

Exception Management:
Exceptions to this procedure will be evaluated in accordance with Cone Health's Information Security Exception Management procedure.

Applicability:
All employees, volunteers, trainees, consultants, contractors, and other persons (i.e., workforce) whose conduct, in the performance of work for Cone Health, is under the direct control of Cone Health, whether or not they are compensated by Cone Health.

Compliance:
Workforce members are required to comply with all information security policies/procedures as a condition of employment/contract with Cone Health. Workforce members who fail to abide by requirements outlined in information security policies/procedures are subject to disciplinary action up to and including termination of employment/contract.