CONE HEALTH	**Guideline:** ITS Information Access Management Procedure	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 06/07/2024
	Effective Date: 06/07/2024	**Next Review Date:** 06/07/2025

INTENDED AUDIENCE:
Managers who are responsible for managing access to ITS

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, and sensitive data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.

This purpose of this procedure is to define how Cone Health manages access to covered information and supporting information systems.

Scope and Goals:
The goals of information access management are to ensure:

- Access to covered information and system resources is granted under the minimum necessary needed to perform assigned job responsibilities.
- Access is promptly granted, adjusted, suspended, or terminated by the proper authority (e.g., system owner, supervisor, etc.)
- Users are being positively identified before granting access to covered information and system resources.
- Access is adjusted when appropriate (i.e., promotion/demotion, job change, etc.).
- Access is promptly removed when an individual's employment/contract is terminated.
- System/application owners perform periodic audits to detect or prevent instances of excessive access.
- Requirements for privileged user access are defined.
- Requirements for segregation of responsibilities are defined.
- Define different types of remote access that fall under the scope of this procedure.
- Establish procedure for authorizing remote access.
- Define security controls that will be utilized to manage remote access connections.

Responsibilities:
Chief Information Security Officer:
Cone Health's information security officer (CISO), in partnership with the organization's chief privacy officer, are responsible for maintenance, interpretation, and enforcement of this procedure.

Chief Privacy Officer:
Cone Health's chief privacy officer in partnership with the organization's CISO, are responsible for maintenance, interpretation, and enforcement of this procedure.

Management:

Management will ensure that all users under their supervision, regardless of their employment relationship (e.g., contractors, interns, part-time, etc.), are:

- Briefed on their security roles/responsibilities and terms and conditions of access to the organization's information systems and are provided guidelines regarding the security expectations of their role.
- Motivated to comply with security policies and procedures.
- Continue to maintain appropriate skills and qualifications related to the protection of covered information.
- System administrators
- Responsibilities include, but are not limited to the following:
  - Add, remove, change, or suspend access as defined by this procedure and Workforce Member Access Request/Change/Termination Forms submitted by authorizing officials.
  - Perform account maintenance as defined by this procedure.

System/Application Owners:

Responsibilities include, but are not limited to, the following:

- Approving all requests for access to their respective systems/applications.
- Ensuring access rights to the system/application are based on minimum necessary.
- Maintaining a list of all workforce members (individuals, contractors, and business associates) with access to PHI, PII, and/or other covered information. This list will be updated whenever there are changes in access.
- Ensure that redundant user IDs are not issued to other users and that all users are uniquely identified and authenticated for both local and remote access to information systems.
- Ensure user IDs that were previously used and removed must not be reused for a completely different person.
- Ensuring access rights to their respective systems/applications are accurate through the practice of periodic revalidation as described by this procedure.
- Ensuring that remote access and other types of remote connections (both by workforce members and third parties) to the organization's network are encrypted and otherwise secured using the organizational defined process (see Security Configuration Management procedure).

User Registration and Management:

Access to Cone Health systems will not be allowed without proper verification of identity. Proper verification of identity is the completion of:

- In person verification by a designated organizational official (e.g., the department supervisor)
- Single or Multi-User Access Request form
- Applicable Acceptable Use Agreements
- Background check (outlined in the Employee policy and Personnel Security Management policy/process)

Access to covered information will be granted based on the user's role and responsibilities, with an emphasis on "need-to-know/need-to-use" or what is commonly referred to as "minimum necessary."

Access will never be granted for the purpose of convenience or solely based on position authority (e.g., CEO, manager, etc.).

To enforce minimum necessary requirements, Cone Health will implement role-based security in addition to limiting access to application functions through the use of application security that controls access to menus/screens based on the role (e.g., read, write, delete, and execute).

Application access control will be managed individually by the application and not as a group or system. This is especially crucial for applications that communicate with each other. It will not be assumed that if a user has access rights to one application, that they also have rights to the other application.

Account types shall be identified (individual, system, department, emergency, etc.). The use of group, shared or generic accounts and passwords is prohibited.

Employment/Contract Termination:

Voluntary Termination:

Upon notification of a workforce member terminating their employment or contract (as in end of contract), supervisors will be required to complete the Workforce Member Termination Checklist and notify People and Culture and the security officer as soon as possible, but no later than 24 hours prior to termination of employment. For positions that have access to critical systems or have system administration responsibilities, terminate access immediately once they no longer need access.

Involuntary Termination:

Managers will immediately notify People and Culture and the security officer of all involuntary terminations. Notification responsibility of involuntary business associate terminations is the responsibility of the Cone Health employee overseeing the contract. Access will be disabled just prior to the individual being told they have been terminated.

Regardless of the type of termination, People and Culture, the CISO, and the direct supervisor will ensure physical and logical access rights are disabled, removed, or downgraded to prevent access and materials that are the property of the organization (e.g., phones, computers, passwords, keycards, keys, documentation that identifies them as current members of the organization) within 24 hours. For high risk terminations, which may result in an incident, immediate escorting of the former employee offsite may also be necessary.

User accounts will be immediately disabled (password changed, and privileges reduced to the lowest levels of access) and deleted 90 days later if it is determined that there is no legitimate business reason to maintain the account. Retaining disabled accounts provides management the opportunity to have the account reactivated in order to clean up uncompleted projects, respond to email, etc. In the event of a criminal investigation this gives investigators a chance to collect evidence they may need for prosecution.

Account Management:

Account Maintenance:

System administrators will be responsible for performing monthly maintenance associated with the clean-up of unnecessary and dormant accounts. System administrators will:

- Disable default and unnecessary system accounts. If an account must be maintained, the password to the account will be changed and privileges reduced to the lowest level of access.
- Disable inactive/dormant/orphan accounts (accounts that have had no activity for more than 30 days).
- Configure automated mechanisms to assist in system account management including provisioning and de-provisioning user accounts, notifying appropriate account managers of changes in access, disabling emergency accounts within 24 hours, and temporary accounts within a fixed duration not to exceed 365 days.

Leaves of Absence:

Managers will inform the security officer of any workforce member who takes a leave of absence in excess of 30 days. Badges and user accounts will be disabled until instruction to reactivate them, typically upon return of the workforce member from leave of absence.

Change of Responsibilities:

Managers of workforce members who have a change in job responsibilities that impacts their access to Cone Health systems will be required to submit a Workforce Member Access Request form, noting the changes in their access that need to occur. Changes are usually the result of promotion, demotion, transfer, changes in responsibilities, etc. If a workforce member is changing departments, it may be necessary for the losing and gaining managers to both submit a Workforce Member Access Request form. Access changes will be submitted to system administrators and action taken as soon as possible, not to exceed 30 days.

Periodic Revalidation of Access:

Every 90 days, system administrators will work with application owners to revalidate user access (including a user accounts assigned to vendors). The system administrator will send application owners a list of all the users who have access to their systems, along with the rights and privileges they have. Application owners will confirm that the user still needs access at the level granted with the same rights and privileges. If there are changes that need to be made, the application owner will inform the system administrator or the changes. System administrators will implement these changes within 24 hours of notification.

Privileged User Access:

Privileged user access is a level of access that allows an individual to perform system administration or security relevant functions (e.g., configuring/modifying access authorizations and setting/modifying audit logs and auditing behavior, boundary protection system rules, authentication parameters, and system configurations and parameters) that ordinary users are not authorized to do. The following rules apply to privileged user access:

- Formally authorized and strictly controlled.
- Granted on a need-to-use and event-by-event basis for their function or role.
- Documented for each system.

- Will use separate system accounts when performing privileged functions (i.e., user must use two different accounts, one for privileged access duties and another for normal business usage). Accounts used for privileged functions will only be used on the system they are assigned to and not shared/used for other systems.
- Limited to the smallest number of users possible.
- Will be reviewed every 60 days to see if privileged access is still necessary.
- Access to management functions or administrative consoles for virtualized environments is also consider privileged access and is subject to the same minimum necessary rules and controls.

Wherever possible and feasible, the organization will promote the development and use of programs that avoid the need to run with elevated privileges and system routines to avoid the need to grant privileges to users.

Segregation of Responsibility:
Access authorization requests (e.g., adding, removing, changing or suspending access) will be segregated to avoid conflict of interest, collusion, fraudulent or other malicious activity. The following rules apply to segregation of responsibility:

- A single individual will never be able to perform a process from the beginning to the end without the involvement of another individual or group with appropriate authority.
- Users, regardless of their level of authority, will not be allowed to add or change their access to covered information without approval from an appropriate authority (e.g., user's manager, system owner, CISO, chief privacy officer, etc.).
- System administrators or security personnel are not allowed to change system security or audit functions without proper approval from an appropriate level of management.
- If a separation of duties cannot be achieved, then additional auditing and monitoring will be put in place to maintain system integrity.
- Access for individuals responsible for administering access controls is limited to the minimum necessary based upon each user's role and responsibilities and these individuals cannot access audit functions related to these controls.
- Development, testing, quality assurance, and production functions are separated among multiple individuals/groups.
- For any other relevant mission critical and/or information system support functions, Cone Health will ensure these tasks are divided among separate individuals.

Emergency Access Management:
The security officer will work with application owners to establish emergency access procedures, sometimes referred to as "break-the-glass" for all critical applications. These procedures are documented instructions and operational practices for obtaining access to covered information during emergency situations. The security officer and application owners must determine the types of situations that would require emergency access to an information system or application that contains covered information. Situations that warrant emergency access could be, but are not limited to, the following:

- Account problems
- Authentication problems

- Authorization problems
- Physical equipment failures
- Life-threatening situations

Access associated with emergency situations will be disabled as soon as possible after it is determined that access is no longer needed.

Remote Access Management:
Remote access at Cone Health is categorized as one of the following:

- Workforce members who telework (e.g., at home or when traveling).
- Third parties who are providing services on behalf of Cone Health that requires access to internal resources and/or covered information.
- Vendors who provide support and/or ongoing maintenance activities for internal systems (e.g., environmental, ITS, medical/patient care, etc. systems).

Authorization for Remote Access:
To ensure remote access by workforce members is limited to minimum necessary, those who need remote access will be required to submit an access request through their appropriate manager, who in turn will submit to ITS for final approval and implementation. All remote access must adhere to the security requirements outlined in the Security Configuration Management procedure. For any remote access sessions involving administrative functions, these will need to be specifically authorized per instance by the CISO.

Third party entities to include service/maintenance vendors will be approved by the CISO. Only those third parties that have signed a business associate agreement (BAA) and have completed a current (within the last year) risk assessment/analysis will be authorized remote access to the minimum necessary internal resources and/or covered information. Third party entities require the approval of the appropriate business leader that oversees their contract. Remote access will be limited to the terms of their contract with Cone Health (see Third Party Assurance procedure for additional requirements). Access to all sessions and network connections is terminated when remote (nonlocal) maintenance is completed.

Device Authorization for Remote Access:
Workforce members will:

- Use approved devices owned or leased by Cone Health for remote access.
- Use approved personal devices in accordance with Cone Health's Personal Device Use procedure.
- All devices must comply with Cone Health's Security Configuration Management procedure.

Remote Access Security Requirements:
Remote connectivity to internal resources and data will comply by the following security requirements:

- Remote access connections that are used to transmit covered information will only use approved 256 bit or greater, encryption services (e.g., SSL, TLS 1.1 or later, VPN, SSH, etc.).
- Multi-factor authentication will be required for all instances of remote access. Prior to its use, multi-factor authentication technology will be approved by the CISO. For one of the factors, a device that is separate from the system gaining access must be used. If hardware or software

tokens are going to be distributed for use in the process, the user identification requirements stated above must be completed.

- Remote access to covered information across public networks will only take place after successful identification and authentication. (See Identification and Authentication procedure.)
- Support/maintenance vendors are required to coordinate all remote access activity with ITS and the appropriate business unit in advance. Vendors will be required to notify ITS and the business unit at least 5 business days in advance of any planned remote activity. Records for remote (nonlocal) maintenance and diagnostic activities is maintained. Access to all sessions and network connections is terminated when remote (nonlocal) maintenance is completed.
- Remote access accounts used by vendors or other business partners will be deactivated/disabled when not in use.
- The use of collaborative computing devices that create remote connections (e.g., networked white boards, camera, and microphones) are restricted. In the event one of these connections is required, the use of these devices will be limited to approved individuals only. Also, while the connection is active, the user must be presented with a physical indication to signal a session is active (e.g., signals, screen/light indicators).
- All remote users, regardless of who they are, will be instructed to immediately logout when access is no longer needed.
- Auto-termination of remote connections will be implemented wherever possible. Auto-termination will be set to occur after 30 minutes of inactivity.
- ITS will actively audit and monitor all remote access connections in accordance with Cone Health's Audit Logging and Monitoring procedure.
- Remote access rights and privileges will be restricted to the minimum necessary required to perform assigned/contracted responsibilities. Rights and privileges are defined as the ability to remotely read/view, write/change, copy, delete, print (to include print screen), etc., and store covered information. Remote access requests will specifically address what rights and privileges are needed when remotely accessing internal resources and data and be in accordance with a defined business need.
- When Public Key Infrastructure (PKI)-based authentication is used, the information system will validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information. Access rights will be enforced to the corresponding private key and map to the account of the individual or group. Also, a local cache of revocation data will be maintained to support path discovery and validation if the ability to receive this information via the network becomes unavailable.

Remote access accounts that have shown no activity for a period of 30 days will be disabled by ITS, unless a valid reason has been communicated to and approved by ITS and the CISO.

Documentation Retention:
All related documentation will be retained for a minimum of 6 years from date of completion.

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

Guideline: ITS Information Access 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 directly compensated for services/work 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.