CONE HEALTH	**Guideline:** ITS Identification and Authentication Procedure	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 06/07/2024
	Effective Date: 06/07/2024	**Next Review Date:** 06/07/2025

INTENDED AUDIENCE:
Entire workforce

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. 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 endpoint/entity identification and authentication requirements when accessing Cone Health systems, applications, services, and technology resources.

Scope and Goals:
This procedure applies to all Cone Health users who access the organization's systems, applications, services, and technology resources. The goals of this procedure are to:

- Define identification requirements
- Define authentication requirements
- Establish password management requirements

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.
- Ensuring system passwords are changed whenever there is a security incident that indicates a password compromise.

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

- Configuring systems or implementing technical controls that comply with the requirements of this procedure.
- Maintain a list of commonly used and compromised (or expected of) passwords, and review and updates the list at least every 180 days. Implement a system that checks for and rejects the use of these passwords by users.
- Configuring the password management system to allow for long passwords and passphrases, including spaces and all printable characters.

- Configuring the password management system to assist workforce members in selecting strong passwords and authenticators.
- Ensuring default passwords across all organizational systems are changed.

Identification Requirements:
Access to covered information will be traceable to an individual using a unique user identification (userID) code. The use of generic, shared, or group userIDs, and passwords, or any other type of access that could lead to actions being performed that would not require individual authentication or identification is prohibited. These requirements apply to ANY user with access to Cone Health's information systems including non-organizational user such as customers, clients, and/or contractors.

Certain types of user support transactions, like resetting passwords, whether by the Help Desk, system administrator, or self-provisioning tool, will require positive verification of the requestor's identity. Positive verification can be accomplished through one of the following:

- In person, face-to-face verification.
- Responding correctly to "secret" questions that the requestor previously provided the answers to. The questions are used by the Help Desk or a self-provisioning tool to verify the requestor's identity if face-to-face verification is not possible or feasible. At least three points of verification will be confirmed by the Help Desk or the self-provisioning tool before providing the requestor with a temporary password.
- Cell phone verification: Technology used to send a one-time temporary code to a predefined cell phone number. The code is used to gain access to a screen where the requester is prompted to create a new password. used to send a one-time temporary code to a predefined cell phone number. The code is used to gain access to a screen where the requester is prompted to create a new password.

Workforce members are required to send acknowledgement whenever a password is successfully received or reset to confirm the information was sent to the correct user and the account has not been compromised.

Authentication Requirements:
Authentication requirements defined by this procedure will be required in all information technology (e.g., workstations, laptops, mobile devices, servers, routers, etc.) configuration standards. If application specific identification and authentication controls are needed those will be defined in a separate standard. Information technology password configuration requirements are as follows:

- Passwords will be at least (14) fourteen characters in length.
- Passwords must contain each of the following: uppercase alpha character; lowercase alpha character; numeric character; and special character (i.e., !, @, #, $, %, &, *, ?).
- Passwords will not be the same as a user's ID/logon.
- Passwords cannot be the same as the previous 3 passwords.
- Passwords will not be included in automated log-on processes.
- For all initial, first-time, log-on's or under any circumstance that requires a user to change their password (e.g., account recovery), users will be provided a secure (i.e., not guessable) temporary password to use to login. Upon login, the user will be immediately prompted (i.e., forced) to

change the temporary password to something only they know that meets the previously mentioned composition requirements. Temporary/default passwords will:

- Be one time use only
- Follow same composition rules as regular passwords

Electronic Signatures:
Electronic signatures used in conjunction with passwords for the purposes of authentication and system access will be protected by ensuring the following:

- The organization requires that electronic signatures are unique to one individual and cannot be reused by, or reassigned to, anyone else. Workforce members will be held accountable to all actions initiated under their electronic signatures.
- Identity verification of the individual is required prior to establishing, assigning, or certifying an individual's electronic signature or any element of such signature.
- Electronic signatures based upon biometrics are designed to ensure that they cannot be used by any individual other than their genuine owners.
- Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records.
- Signed electronic records shall contain information associated with the signing in human-readable format.
- If relevant, ensure that all legal considerations related to the use of electronic signatures are addressed.
- For any electronic signatures that are not based upon biometrics, these instances shall employ at least two distinct identification components that can be administered and evaluated for authorized authentication.

Documentation Retention:
Documentation of compliance assessments will be retained for a period of no less than 6 years from the date of the assessment.

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.