Triad HealthCare Network
Physicians Partnering with CONE HEALTH

Policy Title: Password Policy			
Department Responsible: THN Compliance & Integrity	**Policy Number:** SEC-105	**THN's Effective Date:** January 1, 2022	**Next Review/Revision Date:** September 30, 2023
Title of Person Responsible: THN Director of Compliance & Privacy	**THN Approval Council:** THN Board of Managers	**Date Approved:** August 29, 2022	**Date Approved by THN Board of Managers:** August 29, 2022

I. **Purpose.** The purpose of SEC-105 is to provide instruction to all of Triad HealthCare Network's (THN's) workforce members regarding the required use of passwords for access to THN's systems that contain PHI and to maintain an adequate level of security by the use of passwords to protect THN data and information systems from unauthorized access.

II. **Policy.** This policy defines rules necessary to achieve protection and to ensure the secure and reliable operation of THN's information systems. The purpose of this policy is to ensure that passwords are appropriately used on THN's systems so that only authorized users gain access to THN information systems.

III. **Procedure.** To gain access to THN's information systems, authorized users, as a means of authentication, must apply employee user passwords. These passwords must conform to certain rules contained in this policy.

A. **Affected Systems:** This policy applies to all computer and communication systems owned or operated by THN which access PHI. Similarly, this policy applies to all platforms (operating systems) and all application systems used to access PHI.

B. **User Authentication:** All systems will require a valid user ID and password. All unnecessary operating system or application user IDs not assigned to an employee user or for appropriate administrative purposes will be deleted or disabled.

C. **Password Storage:** Passwords will not be stored in readable form without access control or in other locations where unauthorized persons might discover them. All such passwords are to be strictly controlled using either physical security or computer security controls.

D. **Application Passwords Required:** All programs, including third-party produced software and applications developed internally by THN must be password protected.

E. **Choosing Passwords:** All user-chosen passwords must comply with "strong pass phrase construction", be at least eight (8) characters in length, and contain at least five (5) alphabetic and three (3) non-alphabetic characters, one of which must be non-numeric, arranged in any order. The use of control characters and other non-printing characters are prohibited. All users must be automatically forced to change their passwords appropriate to the classification level of information. To obtain a new password, a user must present suitable identification.

F. **Changing Passwords:** All passwords must be promptly changed if they are suspected of being disclosed or known to have been disclosed to unauthorized parties. All users must be forced to change their passwords at least once every sixty (60) days.

G. The display and printing of passwords should be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. After three (3) unsuccessful attempts to enter a password, the involved user-ID must be either:

1. Suspended until reset by a system administrator,
2. Temporarily disabled for no less than three (3) minutes, or
3. If other external network connections are involved, disconnected.

Date	Reviewed	Revised	Notes
January 1, 2022			Originally Published
August 2022	X		No changes