Policy Title: Data Backup, Security, Privacy, and Removal of User Access			
Department Responsible: THN Compliance & Integrity	**Policy Number:** SEC-104	**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.** SEC-104 describes Triad HealthCare Network's (THN's) process for backing up data, and how this information is protected against potential threats.

II. **Policy.** THN will back up data and software on the server on a monthly basis. The safekeeping and confidentiality of data and the provision of access to that data by authorized individuals are essential to patient care and to the business operations of THN. It is the intent of THN to protect the integrity and confidentiality of information while providing appropriate access to that information and complying with federal and state regulations regarding such data. This policy applies to all members of the workforce and to all who have access to THN information. To gain access to THN information systems, authorized users, as a means of authentication, must apply employee user passwords. Additionally, THN will follow Cone Health procedures for removal of user access to its network and/or information systems based upon the type of user account.

III. **Procedure.**

A. Password Policy.

1. To gain access to THN 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. 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. 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. Passwords will not be stored in readable form without access control or in other locations where unauthorized person might discover them. All such

passwords are to be strictly controlled using physical security or computer security controls.

d. All programs, including third-party produced software and applications developed by THN must be password protected.
e. 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 is 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. 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:
    i. Suspended until reset by a system administrator;
    ii. Temporarily disabled for no less than three (3) minutes; or
    iii. If other external network connections are involved, disconnected.

B. **Security of Data and Electronic Information Systems**

1. ***Administrative Safeguards:***

a. THN will conduct initial and periodic assessments to document the threats and vulnerabilities to stored and transmitted information. The analysis will address all applicable federal and state requirements. Measures will be implemented that reduce the impact of risks associated with threats and vulnerabilities to a reasonable and appropriate level. **HIPAA Administrative Security Standard 1**
b. THN will develop and maintain procedures for periodic system activity reviews. Those procedures will reside in specific areas as appropriate. Documentation will be maintained as appropriate. **HIPAA Administrative Security Standard 1**

c. Violations of this security policy and other policies addressing confidentiality of data are addressed up to and including termination of access and/or employment. See Policies HRD-2005-109 and ER-HRD-2005-54. **HIPAA Administrative Security Standard 1**
d. Corporate Security Official - The Corporate Security Official (Data Security Officer) is responsible for working with the workforce to develop and implement policies, procedures, and controls to protect electronic information subject to the approval of the Chief Information Officer (CIO) and/or the appropriate governing body. **HIPAA Administrative Security Standard 2**
e. Information technology crucial to business operations, care of patients and other essential functions of the organization is located throughout THN. Management responsible for departmental systems shall develop procedures that define who can access, what access is appropriate, how timely termination of access will be accomplished, and processes followed in granting or changing access, along with their documentation. Departmental system management is responsible for updating procedures as required by changes in information technology. **HIPAA Administrative Security Standard 3 and 4**
f. Training that includes security awareness will be conducted at orientation, yearly and on an as needed basis. Departmental management is responsible for further training and procedures in their area. Measures will be taken to protect systems from malicious software, monitor improper login attempts, and manage passwords. Management responsible for departmental systems shall develop procedures for monitoring inappropriate login attempts, and for effective password management. **HIPAA Administrative Security Standard 5**
g. Anyone aware of a perceived or actual incident involving risk to security of electronic information (theft/loss of media or device, stolen password, virus attack, etc.) shall immediately notify the Cone Health Vice President-Chief Information Officer, the Cone Health Privacy Officer, THN's Data Security Officer, or other designated staff. **HIPAA Administrative Security Standard 6**
h. Management responsible for essential systems shall address reasonably anticipated situations that could put electronic information at risk, including but not limited to backup, restoration, recovery from a disaster and

continuation of operations in an emergency mode. **HIPAA Administrative Security Standard 7**

i. Periodic technical and nontechnical evaluations will be performed to establish the extent to which policies and procedures meet the requirements of the HIPAA Security Rule and other applicable federal and state guidelines. Criteria for an out-of-cycle evaluation will be developed. **HIPAA Administrative Security Standard 8**

j. Business Associates, who create, receive, maintain or transmit electronic PHI data for THN will be required to provide satisfactory assurance that the BA meets applicable federal and state guidelines. **HIPAA Administrative Security Standard 9**

k. All policies and procedures will be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures will also be documented. All documentation will be retained for at least ten (10) years after initial creation or change. All documentation will be periodically reviewed to verify that it is appropriate and up to date, the period to be determined by each entity within THN that is responsible for the documentation.

l. At each entity and/or department level, additional policies, standards, and procedures may be developed detailing the implementation of this policy and set of standards and addressing any additional information systems functionality in that entity and/or department. All such departmental policies must be consistent with this policy. All systems implemented after the effective date of this policy are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as is practical.

2. ***Physical Safeguards:***

a. Cone Health and THN will limit physical access to its buildings and identified parking areas, confidential data and electronic information systems and the facility or facilities in which they are housed, while ensuring that proper authorized access is allowed. Controlled access will include keyed entries, keypads, proximity cards such as employee ID badges and other means. **HIPAA Physical Security Standard 1**

b. Workstations intended to access PHI will be utilized for healthcare-related purposes only. Workstations that can access confidential data will be placed so that only authorized individuals will be able to view data. Users

accessing PHI from remote locations will be aware of risks and their responsibility to maintain privacy and security of all PHI. Cone Health will implement physical safeguards as appropriate for workstations that access ePHI to restrict access to authorized users. **HIPAA Physical Security Standard 2 and 3**

c. Receipt and removal of hardware and electronic media that contain confidential information, into and out of a facility, and the movement of these items within the facility will be controlled by Management Systems. Management Systems will designate types of hardware and electronic media to be tracked and maintain an accounting of the location of all hardware and electronic media and be responsible for the final disposition of all tracked hardware and electronic media, including the appropriate removal of all PHI. See Policy OP-CAD-1998-85. **HIPAA Physical Security Standard 4**

3. ***Technical Safeguards:***
   a. Access to electronic information systems that maintain ePHI shall be allowed only to persons or software programs that have been granted access rights as specified in Administrative Safeguards E of this policy. **HIPAA Technical Safeguards Standard 1**
   b. Access to all confidential information will be limited while ensuring that access meets the minimal requirements for its workforce and others to maintain continuity of care and other business functions. Management for each system will develop procedures for assigning a unique name and/or number credential for identifying and tracking user identity. **HIPAA Technical Safeguards Standard 1**
   c. Management for each system will develop procedures for obtaining access to confidential information as necessary during an emergency situation, downtime procedures and identify who may need access in such situations. **HIPAA Technical Safeguards Standard 1**
   d. Mechanisms will be developed and employed to record and examine activity in systems that contain confidential information as required by Administrative Safeguards B of this policy. **HIPAA Technical Safeguards Standard 2**
   e. Procedures will be developed and put in place to protect confidential information from improper alteration or destruction. **HIPAA Technical Safeguards Standard 3**
   f. Procedures are in place and will be developed and put in place as appropriate, to verify that the identity of a person or

entity seeking access to confidential information is valid and authentic. **HIPAA Technical Safeguards Standard 4**

g. When required, confidential information will be electronically transmitted with safeguards in place to prohibit unauthorized access. **HIPAA Technical Safeguards Standard 5**

4. ***Computer and Information Control:***
   a. Computer software developed by Cone Health or THN employees or contract personnel on behalf of or licensed for either Cone Health or THN's use is the property of Cone Health or THN and must not be copied unless otherwise specified by the license agreement.
   b. All hardware and software that resides on computers and networks within Cone Health or THN will comply with application licensing agreements and restrictions and comply with Management System's guidelines and policies.
   c. Virus Protection: Users are not authorized to configure, and may not turn off or disable, virus checking software deployed and approved by Management Systems.
   d. Controls: Physical and electronic access to PHI, confidential and internal information is controlled.

C. **Data Backup**
1. THN will be backed up onsite and offsite per VPN. The backup will be encrypted with the key to a special administrative account known to the Privacy & Security Officer.
2. THN will keep offsite installable copies of all software that is used by THN in its original form.
3. These policies and procedures enable THN to respond to the following failures:
   a. If THN loses the hard drive that contains the database in the server, the system's data can be restored to the moment of the failure.
   b. If THN loses the server in a way that destroys the main hard drive and the database, THN can restore all but the last day's data.
   c. If any other failure (i.e., software) affects THN data, THN can restore to any given day up to the previous week.

D. **Removal of User Access**
1. Removal of authorization due to normal processes.
   a. **Employees:** Terminations should be entered into Lawson. This will automatically disable the user's network logon.
   b. **All others:** All other terminations should be entered as an IT Service Desk ticket or called into the IT Service Desk at 832-7242. This will ensure a moderate ticket for the Security and Access Management team is opened.
1. Removal of authorization immediately, or high priority.

a. **Any type of user:** If a termination is deemed high priority, or needs to be accomplished immediately, please contact the IT Service Desk at 832-7242. This will ensure a critical ticket for the Security and Access Management team is opened and paged out to the On Call team member.

1. Removal of authorization due to inactivity (They can easily be reactivated by having the user's manager, supervisor, or Cone Health sponsor contact the IT Service Desk at 832-7242).
    a. **Employees:** Employee accounts will be disabled after 30 days of inactivity. Once the employee is terminated in Lawson, the account will be disabled, and all security groups will be removed. After 60 days of termination, the account will be deleted.
    b. **Contractors:** Contractor accounts will be disabled after 30 days of inactivity. After 60 days of being disabled, the account will be deleted.
    c. **Non-Employees:** Non-employee accounts will be disabled after 60 days of inactivity. After 90 days of being disabled, the account will be deleted.
    d. **Providers:** Provider accounts will be disabled after 90 days of inactivity. After 270 days of being disabled, the account will be deleted.
    e. **Community Connect:** Community Connect accounts will be disabled after 60 days of inactivity. After 90 days of being disabled, the account will be deleted.
    f. **Students:** Student accounts will be disabled after 30 days of inactivity. After 540 days of being disabled, the account will be deleted.
    g. **Vendor:** Vendor accounts will be disabled after 180 days of inactivity. After 180 days of being disabled, the account will be deleted.
    h. **Generics:** Generic accounts will be deleted after 90 days of inactivity.

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