Policies and Procedures

Policy Title: Security of Data and Electronic Information Systems			
Department Responsible: Compliance & Integrity	**Policy Code:** THN-CP-0417-4.0	**Effective Date:** April 10, 2017	**Next Review/Revision Date:** September 30, 2019
Title of Person Responsible: Data Security Officer	**Approval Council:** Cone Health Leadership Council		Adopted by THN C&I Committee: April 10, 2017

POLICY:
The safe keeping 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 Triad HealthCare Network. 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.

PURPOSE:
To define how THN will protect confidential information from accidental or intentional unauthorized access, disclosure, duplication, diversion, modification or destruction.

DEFINITIONS:
- **Availability**: Data is accessible and usable upon demand by an authorized person.
- **Confidentiality**: Data is not made available or disclosed to unauthorized persons or processes.
- **Electronic Information Systems**: All computer equipment and network systems including operating systems, computers (desktops, mobile devices, servers, mainframes, etc.) and all applications and data (whether developed in-house or licensed from third parties) contained on those systems wherever they physically reside.
- **ePHI**: Protected Health Information in electronic format.
- **Integrity**: Data or information has not been altered or destroyed in an unauthorized manner.
- **HIPAA and HITECH**: The Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009 are federal laws that contain regulations affecting how certain healthcare and insurance plans protect the privacy and confidentiality of PHI and ePHI by setting and enforcing standards. HIPAA and HITECH address both Privacy and Security of PHI. The Privacy Rule contains provisions about what PHI is protected and how PHI can be used and disclosed. The Security Rule contains provisions about what PHI is protected and what safeguards must be in place to ensure appropriate protection of ePHI. Other state and federal laws also govern how healthcare and insurance plans protect PHI.

- **Protected Health Information (PHI)**: PHI is individually identifiable health information, including demographic information, created or received by healthcare and insurance entities which relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual and that identifies or can be used to identify the individual. This includes information contained in medical records, automated computer systems, clinical departments, patient financial systems and employee/affiliate files.
- **Risk**: The probability of a loss of confidentiality, integrity, or availability of information resources.
- **Threat**: The potential for possible action that could cause unauthorized access, disrupt operations or inflict other harm.
- **Vulnerability**: A flaw or weakness in system security procedures, design, implementation, operation or internal controls that could be exploited (accidently or intentionally) to gain unauthorized access or disrupt critical processing.
- **Workforce**: Physicians, residents, students, employees, contractors, consultants, temporaries, volunteers, interns, etc.

PROCEDURE:

Administrative Safeguards

1. Triad HealthCare Network 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
2. Triad HealthCare Network 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
3. 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
4. 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
5. Information technology crucial to business operations, care of patients and other essential functions of the organization is located throughout Triad HealthCare Network. 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.
6. 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 of inappropriate login attempts, and for effective password management. HIPAA Administrative Security Standard 5

7. 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
8. 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
9. Periodic technical and nontechnical evaluations will be performed to establish the extent to which policies and procedures meet 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
10. Business Associates, who create, receive, maintain or transmit electronic PHI data for Triad HealthCare Network will be required to provide satisfactory assurance that the BA meets applicable federal and state guidelines. HIPAA Administrative Security Standard 9
11. All policies and procedures will to 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 six (6) 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 Triad HealthCare Network that is responsible for the documentation.
12. 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.

Physical Safeguards

1. Cone Health and Triad HealthCare Network 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. Link security policy HIPAA Physical Security Standard 1
2. 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
3. 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 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

Technical Safeguards

1. 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
2. Access to all confidential information will 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
3. 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
4. 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
5. Procedures will be developed and put in place to protect confidential information from improper alteration or destruction. HIPAA Technical Safeguards Standard 3
6. 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
7. When required, confidential information will be electronically transmitted with safeguards in place to prohibit unauthorized access. HIPAA Technical Safeguards Standard 5

Computer and Information Control

1. Ownership: 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.
2. 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.
3. Virus Protection: Users are not authorized to configure, and may not turn off or disable, virus checking software deployed and approved by Management Systems.
4. Controls: Physical and electronic access to PHI, confidential and internal information is controlled.

REFERENCE DOCUMENTS/LINKS:

- CONE HEALTH POLICY OP-MIS-2012-124

PREVIOUS REVISION/REVIEW DATES:

Date	*Reviewed*	*Revised*	*Notes*
October 2012			Original effective date.
October 2, 2015			Updated formatting to match current policy template; no content changes.
April 10, 2017			Adopted by THN C&I Committee