Use of Choctaw Volunteer Fire Department IT infrastructure is not a right but a privilege granted to those with an official affiliation with the department. Access to specific services on the IT infrastructure is based on a business need or in order to provide services. Unauthorized use of IT infrastructure is prohibited.

All Users (authorized or unauthorized) are advised that they should have no expectation whatsoever of privacy in any materials they place or view on this system.

By continuing to use this system, a user acknowledges that they are subject to the terms of the department's acceptable use policy and give their unrestricted consent to the monitoring, copying, and distribution of any transmission/communication or image generated, received by, sent by, or stored on this system.

Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and/or criminal penalties.

Technical Safeguards- Access Control Policy

Scope: Choctaw Volunteer Fire Department organization and workforce.

Purpose: The purpose of the Information Access Control Policy is to ensure that all members of the workforce have access to the systems and information appropriate to their job functions, and to ensure that inappropriate access is prevented under the HIPAA Security Policy- Security Standards for the Protection of Electronic Protected Health Information (ePHI).

Choctaw Volunteer Fire Department is committed to following all applicable laws, regulations and policies. This Policy pertains to the unique user identification and password, emergency access, automatic logoff, encryption and decryption, firewall, and remote and wireless access procedures that will apply to electronic information systems that maintain ePHI.

Authoritative Reference: The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191) HIPAA Security Rule [HIPAA Technical Safeguards] [see §164.312(a)(1) & (2)]

Policy:

1) Unique User Identification and Password

- a. Any user that requires access to any network, system, or application that accesses, transmits, receives, or stores ePHI, must be provided with a unique username.
- b. When requesting access to any network, system, or application that accesses, transmits, receives, or stores ePHI, a user must supply his or her previously assigned unique username in conjunction with a secure password to gain access.
- c. Each user's password should meet the minimum requirements as outlined below:
    - i. Must be a minimum of eight characters in length.
    - ii. Must contain a unique character.
    - iii. Must contain a number.
    - iv. May not contain your user-name or any part of your full name
    - v. Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc.
    - vi. If a system does not support the minimum structure and complexity as detailed in the previous guidelines, one of the following procedures must be implemented
        - 1. The password assigned must be adequately complex to ensure that it is not easily guessed and the complexity of the chosen alternative must be defined and documented.

        - 2. The legacy system must be upgraded to support the requirements as soon as administratively possible.
        - 3. All ePHI must be removed and relocated to a system that supports the foregoing security password structure.
    - vii. Users must not allow another user to use their unique username or password.
- d. Users must ensure that their username and password are not documented, written, or otherwise exposed in an insecure manner.
- e. Each user must ensure that their assigned username is appropriately protected and only used for legitimate access to networks, systems, or applications.
- f. If a user believes their username or password has been compromised, they must report that security incident to the fire chief, who will take appropriate action.

2) Emergency Access

- a. The HIPAA Security Rule requires Covered Entities to establish procedures to allow access to ePHI during an emergency. During an emergency or disaster, covered entities must remember that protecting ePHI is of utmost importance. Emergency procedures may be very different from standard operating procedures, but they are necessary because the normal methods for obtaining access may fail. Emergencies include, but are not limited to, the following:
    - i. Natural disasters – Floods, earthquakes, tornadoes, tsunamis, hurricanes, etc.
    - ii. Man-made disasters – Hacking attacks, thefts, vandalism, terrorist attacks, etc.
    - iii. Unforeseen disasters – Power outages, internal failures, etc.
- b. To ensure that access to critical ePHI is maintained during an emergency situation, each Department must establish and implement procedures to ensure that access to a system that contains ePHI and is used to provide treatment to an individual is made available to any caregiver, if the denial or strict access to that ePHI could inhibit or negatively affect an individual's care.
- c. ePHI repositories that do not affect an individual's care are not subject to the foregoing emergency access requirement.
- d. When developing this policy and procedure, a covered entity should:
    - i. Determine the type of situation that may require emergency access to ePHI.
    - ii. Determine who will need access to ePHI in case of an emergency
- e. In the case of emergency, a computer account may be temporarily shared with another individual. The requirements for emergency access sharing are:
    - i. There must be a true emergency.
    - ii. The sharing must be temporary.
    - iii. The emergency incident must be reported to the managing authority of the computer account being shared.
    - iv. In no case should this emergency access sharing exceed 30 days.
    - v. The Emergency access procedure must be used in case a terminated employee's computer account must be maintained for business reasons. Unless the Emergency Access procedure is implemented, all terminated employee computer accounts will be deleted immediately upon notification of the termination to all relevant parties.
- f. Emergency accounts have been created for accessing ePHI for continuing care. These are unique usernames and passwords that can be tracked easily. They should not be used unless there is a true emergency.
- g. Servers with ePHI are maintained off-site in order to reduce potential damage during a disaster at the facility.
- h. Critical personnel have been issued emergency response cards for access to the facilities in the event of an emergency or disaster.
- i. In the event of a power outage, a backup generator will be utilized.
- j. In the event the backup generator doesn't work, remote access will be utilized by the designated personnel. Information will be printed or transmitted via phone (cell, sat) for patient care.
- k. If a facility is under a pre-evacuation, print only necessary documents to maintain proper care for patients.

3) Automatic Logoff

- a. Servers, workstations, or other computer systems located in open, common, or otherwise unsecured areas, that access, transmit, receive, or store ePHI, or that have been classified as high risk must employ inactivity timers or automatic logoff mechanisms. These systems must terminate a user session after a maximum of 15 minutes of inactivity.
- b. Applications and databases using ePHI, such as electronic claims records, must employ inactivity timers or automatic session logoff mechanisms. These application sessions must automatically terminate after a maximum of 30 minutes of inactivity.
- c. Servers, workstations, or other computer systems that access, transmit, receive, or store ePHI, and are located in locked or secure environments need not implement inactivity timers or automatic logoff mechanisms.
- d. If a system that otherwise would require the use of an inactivity timer or automatic logoff mechanism does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented:
    - i. The system must be upgraded or moved to support the required inactivity timer or automatic logoff mechanism.
    - ii. The system must be moved into a secure environment.
    - iii. All ePHI must be removed and relocated to a system that supports the required inactivity timer or automatic logoff mechanism.
- e. When leaving a server, workstation, or other computer system unattended, users must lock or activate the system's automatic logoff mechanism (CTRL+ALT+DELETE and Lock Computer) or logout of all applications and database systems containing ePHI.

4) Encryption and Decryption

- a. Encryption of ePHI as an access control mechanism is not required unless the custodian of said ePHI deems the data to be highly critical or sensitive. Encryption of ePHI is required in some instances as a transmission control and integrity mechanism.

5) Firewall Use

- a. All networks housing ePHI repositories must be appropriately secured. To ensure that all networks that contain ePHI-based systems and applications are appropriately secured, each connection to outside the network must follow the steps outlined below. Networks containing ePHI-based systems and applications must implement perimeter security and access control with a firewall.
- b. Firewalls must be configured to support the following minimum requirements:
    - i. Limit network access to only authorized Choctaw Volunteer Fire Department users and entities.
    - ii. Limit network access to only legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the secure network.
    - iii. Console and other management ports must be appropriately secured or disabled.
    - iv. Implement mechanism to log failed access attempts.
    - v. Must be located in a physically secure environment.
- c. Choctaw Volunteer Fire Department shall document its configuration of firewalls used to protect networks containing ePHI-based systems and applications. This documentation should include a configuration plan that outlines and explains the firewall rules.
- d. The configuration of firewalls used to protect networks containing ePHI-based systems and applications must be submitted to and approved by the Information Security Officer.

6) Remote Access

- a. Dial-up connections (if allowed), directly into secure networks are considered to be secure connections and do not require a VPN connection. This implementation of secure remote access extends the secure network to the remote user using a secure PSTN (Public Switched Telephone Network) connection.
- b. Authentication and encryption mechanisms are required for all remote access sessions to networks containing ePHI via an ISP (Internet Service Provider) or dial-up connection. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, and secured Citrix client access.
- c. The following security measures must be implemented for any remote access connection into a secure network containing ePHI:
    - i. Mechanisms to bypass authorized remote access mechanisms are strictly prohibited. For example, remote control software and applications, such as GoToMyPC.com, are not permitted.
    - ii. Remote access workstations must employ a virus detection and protection mechanism.
- d. Users of remote workstations must comply with HIPAA Security Policy – Workstation Acceptable Use Policy.
- e. All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.
- f. Any user requesting remote access to a secure network containing ePHI-based systems and applications must be approved by the Security Officer to ensure that the remote workstation device being used by said user meets the security measures detailed in HIPAA Security Policy -- Server, Desktop, and Wireless Computer System Security. The administrator of the secure network must ensure that the previous requirement has been satisfied before access is granted.
- g. Choctaw Volunteer Fire Department shall establish a formal, documented procedure to ensure that remote workstations and mobile devices used by their users to remotely access secure networks containing ePHI-based systems and applications continue to meet the security measures detailed in HIPAA Security Policy -- Server, Desktop, and Wireless Computer System Security.

7) Wireless Access

- a. To ensure that all networks that contain ePHI based systems and applications are appropriately secured, Choctaw Volunteer Fire Department shall follow the wireless access policies and procedures outlined below.
- b. Wireless access to networks containing ePHI-based systems and applications is permitted so long as the following security measures have been implemented:
    - i. Encryption must be enabled.
    - ii. MAC-based or User ID/Password authentication must be enabled. MAC-based (Media Access Control) authentication is based on a permitted list of hardware addresses that can access the wireless network. MAC addresses are hard coded on each network interface card and typically cannot be changed.
    - iii. All console and other management interfaces have been appropriately secured or disabled.
    - iv. Unmanaged, ad-hoc, or rogue wireless access points ARE NOT PERMITTED on any secure network containing ePHI-based systems and applications.
    - v. All wireless LANs do not utilize standard 2.4GHz, 5.0GHz or microwave radio frequencies. Wireless LANs and devices may utilize infrared frequencies and may not support the typical wireless LAN encryption and security mechanisms. For instance, the use of infrared ports on PDAs, laptops, and printers to transmit ePHI may not allow encryption of that data stream. It has been determined that this is low risk because this implementation of infrared is very short distance and low power.
    - vi. All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.

- c. Any user requesting access to a secure wireless network containing ePHI-based systems and applications must ensure that the wireless device being used by said user meets the security measures detailed in HIPAA Security Policy -- Server, Desktop, and Wireless Computer System Security. The administrator of the secure wireless network must ensure that the previous requirement has been satisfied before access is granted.
- d. Choctaw Volunteer Fire Department shall establish a formal, documented procedure to ensure that wireless devices used by their users to access secure networks containing EPHI-based systems and applications continue to meet the security measures detailed in HIPAA Security Policy -- Server, Desktop, and Wireless Computer System Security.