Department of Mental Health & Substance Abuse Services

Policies and Procedures

Subject:	Workstation Use
Policy Number:	HIPAA 5.4
Effective Date:	5/24/05
Entity Responsible:	Division of General Counsel
Revision Date:	1/18/2023

1. Purpose:

This policy specifies appropriate workforce behavior for the secure use of technology resources that are used to access, store, transmit, or create protected health information (PHI) in the Tennessee Department of Mental Health and Substance Abuse Services (TDMHSAS) and the Regional Mental Health Institutes (RMHIs) as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and other federal and state laws.

2. Policy:

To protect the confidentiality of PHI, the TDMHSAS and RMHIs must ensure that technology resources used to access, store, transmit, or create PHI are used securely. All members of the TDMHSAS or the RMHI workforce must be trained on the guidelines on this policy and must follow the guidelines outlined in this policy.

3. Procedure/ Responsibility:

Each RMHI and the TDMHSAS shall implement procedures to ensure that workforce members with a need to access, store, transmit, or create PHI understand how to securely use the associated technology resources. Such procedures must comply with the following guidelines:

3.1: Application Access/ Passwords

3.1.1: Users must sign on to any application which contains electronic PHI using only the unique user identification assigned to them. Users are accountable for all transactions performed under their assigned user identification;

(1): Passwords should not be written down or stored online. If passwords must be written down or stored online, they must be stored in a secured place.

(A): Users may not share or allow other persons or entities to use their unique user identification and password;

(B): Users must not give their unique user identification or password to anyone at any time;

3.1.2: Users must ensure others cannot access the state network using their account. Users should log off the state network before leaving their office/work area, use power-on, keyboard lock, and screensaver passwords.;

3.1.3: If a workforce member terminates his or her employment, the TDMHSAS Security Officer and the STS employees supporting the TDMHSAS or the RMHI Security Officer and the RMHI IT support staff must ensure that the person no longer has access to any databases, including those which contain PHI, by terminating the individual's account on the last day of their employment, or changing the password to a new password unknown by the individual.

3.2: Desktop Storage of PHI

3.2.1: Users must never store PHI on their computer's local hard drive (C drive);

3.2.2: Users must only store PHI on the appropriate, secure assigned network drive. This drive should have restricted access and only be accessible to other members of the TDMHSAS or the RMHI workforce whose job duties require access to this PHI;

3.2.3: Users must not access, store, transmit, or create PHI on a home personal computer or personal portable device including laptop, tablet, or cell phone. Only devices owned and issued by the State of Tennessee may be used to access, store, transmit, or create PHI.

3.3: Portable Device Storage of PHI

3.3.1: Users must limit storage of PHI on the hard-drive of portable devices such as laptops, tablets, or cellphones, and should only store PHI on these devices when absolutely necessary, such as when there is no connectivity to the user's assigned, secure network drive. As soon as connectivity to the user's assigned, secure network drive is established, the user must transfer any PHI stored on the hard-drive of portable devices to the appropriate, secure network drive and delete it from the originating device.

3.3.2: If any PHI is stored on a portable device such as a laptop, tablet, or cellphone pursuant to paragraph 3.3.1 of this policy, the device user must follow the below steps:

(A): protect the portable device with a password;

(B): configure the device to shut down or lock after a period of inactivity;

(C): encrypt any PHI data that is stored on the portable device.

(D): not use the portable device on public wireless networks while PHI is present

(E): use a State of Tennessee approved VPN solution while on a network not owned by the State of Tennessee

3.4: Removable Media Storage of PHI

3.4.1: Users must limit storage of PHI on removable media and should only store PHI on removable media temporarily and when absolutely necessary, such as when there is no connectivity to the user's assigned, secure network drive. As soon as connectivity to the user's assigned, secure network drive is established, the user must transfer any PHI stored on the removable media to the appropriate, secure network drive.

3.4.2: Users must use approved encryption technology when using removable media to temporarily store PHI.

3.4.3: Users must protect the removable media with a password when using removable media to temporarily store PHI.

3.4.4: Users must not remove media from the state property without permission from a supervisor and documentation of the reason for doing so.

3.4.5: Users must safeguard removable media containing PHI in a locked desk or filing cabinet when not in use.

3.4.6: Users must clearly label any removable media to indicate what it contains.

3.5: Sharing PHI Utilizing Wireless Networks

3.5.1: Prior to using any wireless devices or sharing PHI utilizing a wireless network, users must ensure that the wireless network is private, password protected, and inaccessible to other unauthorized users. Users may not use

a public wireless network connection even if it is password protected, as other unknown, individuals could also be utilizing this wireless connection.

3.5.2: Prior to using any wireless devices or sharing PHI utilizing a wireless network, all users must use the Juniper Virtual Private Networking (JVPN). This connects users to the State's network and ensures that all files being transmitted through the wireless network are encrypted.

3.5.3: If emailing PHI, emails containing PHI must be encrypted. Emails sent within the State e-mail system are automatically encrypted. Emails sent outside the State e-mail system are *not* automatically encrypted. Each user must type in "[secure email]" in the email subject line when sending emails to parties outside the State e-mail system. *See* TDMHSAS HIPAA Policy 5.5.

3.6: Physical Security Considerations

3.6.1: Physical Documents:

(1): When handling any physical documents that contain PHI, users must ensure that documents are handled in a way that prevents inadvertent disclosure, including securing such documents in a locked desk or file cabinet when not in use, and locking office doors.

(2): When printing any documents that contain PHI, users must ensure documents are retrieved immediately following printing and are not left on a shared printer.

(3): When copying any documents that contain PHI, users must stay with the document that is being copied and may not allow the copies to remain on the machine unattended.

(4): When discarding printouts containing PHI, users must shred printouts or place printouts in designated lock bins for shredding.

(5): Printers handling PHI must have encrypted hard drives and must be behind a locked barrier or otherwise not accessible to the public or those lacking a 'need to know'.

3.6.2: When faxing any documents that contain PHI, users must do the following: (1) double check the fax number to ensure the documents are being sent to the correct location, (2) utilize a coversheet which does not contain PHI and notifies the recipient of the sensitive nature of the transmission, (3) call the recipient where the transmission will be received to notify them that the

transmission is coming and to request that they notify the user when the fax is received, (4) if the recipient does not notify the user when the fax was received, the user shall follow up with the recipient to receive confirmation of the transmission.

3.6.3: When accessing PHI on a computer, users must ensure that computer screens are not easily seen by someone who is not authorized to access PHI such as by using privacy filters on monitors that may contain or display PHI.

3.6.4: When utilizing any portable equipment that contains PHI or other sensitive information, such portable equipment must be handled in a way that mitigates opportunities for equipment to be stolen by placing the portable equipment is a secure, locked location when not in use.

3.6.5: Each member of the workforce should strive to prevent visitors or individuals who are not a member of the TDMHSAS or the RMHI workforce from being exposed inadvertently to PHI while visiting the TDMHSAS Central Office or other TDMHSAS facilities, including the RMHIs. Visitors or individuals who are not a member of the TDMHSAS or the RMHI workforce should not wander through the TDMHSAS central office, work area, or RMHIs alone, but instead should be escorted throughout these areas by the appropriate member of the TDMHSAS or the RMHI workforce.

3.7: Data Integrity

3.7.1: Users must immediately report any known or suspected breach of security or risk to the integrity of the PHI to his or her supervisor, the TDMHSAS Privacy Officer or the RMHI Privacy Officer and the TDMHSAS Security Officer or the RMHI Security Officer, as applicable. Users must notify the RMHI Security Officer and/or TDMHSAS Security Officer as well as STS employees assigned to TDMHSAS if his or her computer exhibits any unusual behavior or, have reasonable suspicion it was accessed by someone not employed by the state.

4. Other Considerations

4.1: Authority: 45 C.F.R. §§164.308, 164.310, 164.312; and 42 C.F.R. §2.16.

Approved:

Commissioner

1-18-2023

Date