Department of Mental Health & Substance Abuse Services

Policies and Procedures

Subject:	HIPAA Security: Communicating PHI via Electronic Mail or Other Electronic Resources
Policy Number:	HIPAA 5.5
Effective Date:	5/24/05
Entity Responsible:	Division of General Counsel
Revision Date:	1/18/2023

1. Purpose:

This policy describes procedures that govern use of communicating protected health information (PHI) for the Tennessee Department of Mental Health and Substance (TDMHSAS) and the Regional Mental Health Institutes (RMHIs) workforce members who read, create, store, respond to, or transmit PHI via the State E-Mail System or other approved Electronic Resources.

2. Policy:

2.1: The TDMHSAS and the RMHIs permit e-mail or transmission by approved electronic resources of PHI when appropriate safeguards as described below are utilized.

2.2: TDMHSAS and Strategic Technology Solutions (STS) have approved some Electronic Resources as appropriate mechanisms to communicate PHI in accordance with the Health Insurance Portability and Accountability Act (HIPAA). These approved Electronic Resources are subject to change over time. Therefore, each user shall consult with the TDMHSAS Privacy Officer and TDMHSAS Security Officer for TDMHSAS Central Office users or the RMHI Privacy Officer or RMHI Security Officer for RMHI users prior to disseminating PHI through Electronic Resources other than State E-Mail System.

3. Procedure/ Responsibility:

3.1: All TDMHSAS and RMHI workforce members when communicating PHI, in or attached to an e-mail message or other approved Electronic Resources or devices, must:

3.1.1: Set state e-mail accounts and/or approved Electronic Resources or devices to require a unique password.

3.1.2: Limit e-mail communications containing PHI about service recipients to transmission within the State E-mail System, if possible. Both e-mail messages and attachments are automatically encrypted when sent within the state e-mail system, i.e., from a state e-mail user to another state e-mail user. 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 outside parties to ensure encryption.

3.1.3: Never place any PHI (including Name, SSN, ID, Chart Number, etc.) in the subject line of any e-mail, title of any document, or in another place where it may be visually viewed, whether within or outside of a State e-mail message or other transmittal medium. If PHI is already in the subject line of an incoming e-mail or other transmittal medium, it must be removed before a reply is sent.

3.1.4: Attach the PHI in a password protected attachment instead of within the e-mail message itself or other transmittal medium and communicate the password to the recipient(s) in a phone call or other non-written, non-persistent- format after taking measures to ensure they are speaking to the correct person.

3.1.5: Double-check the recipient information to ensure proper routing. Verify that the proper document is attached and that the message and any attachments include no unintended information.

3.2: The following privacy law complaint disclaimer shall be included in all work-related electronic communications (e.g., e-mail, fax, etc.) by all TDMHSAS workforce members (RMHI, Central Office, etc.). All TDMHSAS workforce members shall apply this disclaimer in their electronic signature boxes for all state issued devices or must added it separately in any other communications where this disclaimer is not automatically added along with the signature box regardless of whether PHI is being communicated:

The information transmitted in this communication is intended solely for the specific individual(s) or entity(ies) to whom it is addressed and may contain PRIVILEGED and/or CONFIDENTIAL information. Any unauthorized use,

retransmission, dissemination, or copying of this communication, or the information contained in it or attached to it is prohibited. If you have received this communication in error, please delete it and any information sent with it from any computer or electronic device, destroy any hard copies, and immediately notify the sender. Thank you.

3.2.1: In the event a TDMHSAS and/or RMHI workforce member receives notification from an individual or entity that privileged and/or confidential information was received in error, the TDMHSAS and/or RMHI workforce member shall immediately notify their supervisor, the TDMHSAS Privacy Officer and the applicable RMHI Privacy Officer. The matter shall be handled in accordance with the TDMHSAS HIPAA policy 3.5.

3.3: When a workforce member terminates his or her employment, the TDMHSAS Security Officer and STS employees supporting TDMHSAS or the RMHI Security Officer and RMHI IT support staff must ensure that there are proper off-boarding procedures are in place to prevent the continued access by the individual to the individual's state e-mail address or other state electronic resources or devices. These procedures must ensure that:

3.3.1: A terminating member of the workforce is no longer able to access their e-mail address or other state electronic resources or devices by terminating the account on the last day of the individual's employment or at the earliest opportunity, or if the e-mail, other state electronic resources or device must still be accessed, that account password must be changed to a new password unknown by the individual.

3.3.2: If the account must still be accessed, the individual's supervisor must request that the e-mail address, other state electronic resources or device remain active for a specific period of time, and only individuals who requires access to the account(s) to perform an essential element of his or her job are granted access.

[SIGNATURE APPEARS ON FOLLOWING PAGE]

4. Other Considerations

4.1: Authority:

45 CFR §§164.308, 164.310, and 164.312.

Approved:

Commissioner

1-18-2023

Date