Department of
Mental Health &
Substance Abuse Services

Policies and Procedures

Subject:	Workforce Security
Policy Number:	HIPAA 5.2
Effective Date:	5/11/05
Entity Responsible:	Division of General Counsel
Revision Date:	1/18/2023

1. Purpose:

This policy outlines the information access rules and permissions in the Tennessee Department of Mental Health and Substance Abuse Services (TDMHSAS) and Regional Mental Health Institutes (RMHIs) to ensure that (1) information resources containing protected health information (PHI) is accessed only by persons (or software programs) who are appropriately authorized and granted access rights, (2) reasonable grounds are taken to limit such access to PHI to the minimum necessary for the person to fulfill his or her assigned duties, (3) access to PHI is modified when assigned duties change, (4) access to PHI is revoked upon termination of employment or when access is no longer appropriate.

2. Policy:

To ensure that all members of the TDMHSAS and the RMHI workforce have appropriate access to PHI and to prevent unauthorized persons from obtaining access to PHI.

3. Procedure/ Responsibility:

3.1: Each RMHI CEO (in conjunction with the RMHI Security Officers and RMHI Information Technology Support Staff) and the TDMHSAS Security Officer (in conjunction with the Strategic Technology Solutions (STS) employees assigned to TDMHSAS) shall implement procedures to ensure that only workforce members with a need to access PHI, to perform an essential element of their job, are granted access and to determine and authorize the appropriate level of PHI for the workforce member. Such procedures shall include:

3.1.1: Reasonable and appropriate security measures and safeguards for each PHI Information Systems and/or repository sufficient to reduce risks and vulnerabilities;

3.1.2: Measures to limit a workforce member's access to PHI to the minimum necessary to perform his or her specific job function;

3.1.3: Measures to ensure that PHI access of an individual is appropriate when granted and continues to be appropriate on an on-going basis;

3.1.4: Documentation that an individual's access to PHI has been authorized;

3.1.5: Documentation that an individual with PHI access has received HIPAA privacy and security training;

3.1.6: Incorporation of the State of Tennessee's Acceptable Use Policy and Network Rights and Obligations User Agreement Acknowledgement;

3.1.7: Execution of a confidentiality agreement;

3.1.8: Processes to remove any temporary access rights when the need ends;

3.1.9: Processes to terminate an individual's access to PHI when his or her employment ends or when access is no longer appropriate;

3.1.10: Processes to grant access to contractors or non-state agencies that are based on the same principles used to determine and terminate access levels for state employees;

3.1.11: Processes to grant electronic access by a computer software program based upon the same principles used to determine and terminate access levels for state employees.

3.2: Each user of PHI must know and follow established privacy and security policies. Individuals seeking to access the state's network, any system, database, or repositories containing PHI (1) must do so using only the unique identification assigned, (2) must not allow any other persons or entities to use their unique user identification and password, (3) are responsible for all transactions performed under their assigned user identification, and (4) must report immediately any known improper use or disclosure of PHI or suspected breach of security or risk of the integrity of PHI to their supervisor and their RMHI Privacy Officer or the TDMHSAS Privacy Officer and the RMHI Security Officer or TDMHSAS Security Officer, as applicable.

4. Other Considerations

4.1: Authority:

45 C.F.R. §§164.306, 164.308, 164.310, 164.312, 614.316; and 42 C.F.R. §2.16.

Approved:

Commissioner

1-18-2023

Date