Department of Mental Health & Substance Abuse Services

Policies and Procedures

Subject:	Reviewal and Registration of Protected Health Information (PHI) Information systems & Maintenance of the PHI Information Systems Registry
Policy Number:	HIPAA 5.1
Effective Date:	4/11/05
Entity Responsible:	Division of General Counsel
Revision Date:	1/18/2023

1. Purpose:

This policy outlines the basic safeguards implemented by the Tennessee Department of Mental Health and Substance Abuse Services (TDMHSAS) and the Regional Mental Health Institutes (RMHIs) to prevent electronic sources of protected health information (PHI) from unauthorized access, alteration, deletion, and transmission in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and other federal and state laws.

2. Policy:

All information systems must be registered with STS and carefully evaluated by TDMHSAS Security Officer and IT Director. All such information systems must comply with all laws, rules, and security policies and procedures related to PHI.

3. Procedure/ Responsibility:

3.1: Each RMHI and the TDMHSAS Central Office must have a process to receive and review requests for PHI information systems. At the RMHI, the RMHI Security Officer will review and approve requests for PHI information systems in consultation with the TDMHSAS Security Officer. At the TDMHSAS Central Office, the TDMHSAS Security Officer will review and approve requests for PHI information systems. The process to receive and review requests for PHI information systems should be as follows:

3.1.1: Requests for approval of PHI information systems are submitted to the RMHI Security Officer;

3.1.2: Requests are evaluated and approved at the local level;

3.1.3: The RMHI Security Officer will evaluate each request to discern whether or not the information system conforms to the applicable HIPAA security regulations and will work with the information system owner to rectify any associated issues. If there are unresolved security issues, the request will be forwarded to the TDMHSAS Security Officer for further action;

3.1.4: The RMHI Security Officer is responsible for submitting locally approved requests to the TDMHSAS Security Officer for cataloguing;

3.1.5: If a Business Associate Agreement (BAA) is needed, the RMHI Security Officer is responsible for notifying the TDMHSAS Privacy Officer. *See* TDMHSAS HIPAA Policy 4.3.

3.2: Each PHI information system must have a designated information system owner. The information system owner should be a person that uses the information system on a regular basis and fully understands the operational functions that the information system provides. This person serves as the operational contact and is responsible for assuring that the information system complies with HIPAA regulations.

3.3: The information system owner must designate an individual to be the information system access authorizer who authorizes access to the data. Any process for automatic authorization (such as by job category) must be approved by the information system owner and be documented in written procedure.

3.4: The information system owner must designate an individual to be the information system access administrator. Each information system containing PHI must have a designated person to administer access. The information system access administrator will set up access for new users and remove access when a user's employment is terminated or when access is no longer appropriate. For application, this person would add users to the application system. For PHI residing outside an application this person would be responsible for requesting the appropriate network security rights from STS.

3.5: Upon the execution of a Business Associate Agreement (BAA), the TDMHSAS may permit a business associate to create, receive, maintain, or transmit PHI contained in a PHI information system on TDMHSAS' behalf. See TDMHSAS HIPAA Policy 4.2. It is the responsibility of the TDMHSAS Division of General Counsel, Office of Contracts to ensure that the appropriate BAA's and any other applicable agreement(s) are in place.

3.6: Before creating or implementing a PHI information system, the system owner or their designee must submit a PHI Information System Registration Form to the TDMHSAS Security Officer for review and approval. Each information system must receive approval prior to implementation. The system owner or designee must provide the following information when submitting the PHI Information System Registration Form:

3.6.1: Name of system or information system;

3.6.2: Description of purpose of system or information system;

3.6.3: Location of information system;

3.6.4: Developer of system or information system;

3.6.5: Number of anticipated users;

3.6.6: Primary contact person or owner for system or information system;

3.6.7: Source of PHI;

3.6.8: Use of PHI;

3.6.9: Specific functions performed with PHI;

3.6.10: External uses of PHI (if applicable);

3.6.11: Business Associates related to this PHI information system.

3.7: The information provided in paragraph 3.6 of this policy will be maintained by the TDMHSAS Security Officer in a PHI Information System Registry (PHI Registry). Registration should be done for all PHI information systems prior to their purchase or development.

3.8: The TDMHSAS Security Officer shall review the PHI Registry, at least annually, to ensure that each information system is maintained in the PHI Registry. If the TDMHSAS Security Officer becomes aware of an information system not maintained in the PHI Registry, the TDMHSAS Security Officer shall communicate with the responsible information system owner, who shall submit to the TDMHSAS Security Officer the information required under paragraph 3.6 of this policy within a reasonable period of time not to exceed 30 business days.

4. Other Considerations:

4.1: Authority:

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

Approved:

Commissioner

1-18-2023

Date