Department of Mental Health & Substance Abuse Services

Policies and Procedures

Subject:	Device and Media Controls
Policy Number:	HIPAA 5.3
Effective Date:	5/24/05
Entity Responsible:	Division of General Counsel
Revision Date:	1/18/2023

1. Purpose:

This policy outlines measures for proper receipt and removal of hardware or electronic media that contains protected health information (PHI). The Health Insurance Portability and Accountability Act (HIPAA), as amended, and other federal and state laws require covered entities to develop policies and procedures to address PHI movement into, from, and within the facilities of the Tennessee Department of Mental Health and Substance Abuse Services (TDMHSAS) and Regional Mental Health Institutes (RMHIs).

2. Policy:

To protect the confidentiality of PHI contained in electronic media, the TDMHSAS and the RMHIs must ensure that PHI is irretrievably removed from the electronic media before the media is re-assigned to another user, disposed of, stored, or retired.

3. Procedure/ Responsibility:

3.1: The TDMHSAS Security Officer, in conjunction with the Strategic Technology Solutions (STS) employees assigned to TDMHSAS, and the RMHI CEOs, in conjunction with the RMHI Information Technology support staff and the RMHI Security Officers, shall institute processes to ensure that all PHI stored on electronic media is irretrievably removed and destroyed before the media is re-assigned to another user, marked for surplus for future use, or retired.

3.2: A data destruction tool that meets U.S. Department of Defense standards must be used to destroy the data on the device or media before it is re-assigned to another user, disposed of, stored, or retired. Simple data deletion or a typical reformat or reimage is not sufficient as it does not overwrite the data. This process must be

documented for each device. If using removable media for the purpose of system backups and disaster recovery and the removable media is stored and transported in a secured environment, the use of a data destruction tool between uses is not necessary.

3.3: If the media contains PHI that is required or needed by the TDMHSAS or the RMHI, a retrievable, exact copy of the PHI must be made before data destruction.

3.4: A record must be created by the parties listed in paragraph 3.1 of this policy to keep track of the computer hardware and electronic storage media from one location to another, or re-assignment from one user to another.

3.5: When an electronic storage device containing PHI requires vendor technical support, efforts must be made to ensure the protection of PHI before the vendor has access to the electronic storage device. Appropriate documentation, including, but not limited to, a business associate agreement must be in place before providing access to electronic storage devices with PHI.

4. Other Considerations:

4.1: Authority:

45 C.F.R. § 164.310(d); and 42 C.F.R. §2.16.

Approved:

Commissioner

1-18-2023

Date