TN Department of
Mental Health &
Substance Abuse Services

Policies and Procedures

Subject:	Data Backup and Contingency Planning
Policy Number:	HIPAA 5.7
Effective Date:	10/13/05
Entity Responsible:	Division of General Counsel
Revision Date:	1/18/2023

1. Purpose:

This policy provides standards to ensure that the Tennessee Department of Mental Health and Substance Abuse Services (TDMHSAS) and the Regional Mental Health Institutes (RMHIs) function effectively in the event of a severe disruption of computer services. Severe disruptions can arise from various sources including, but not limited to natural disasters (tornadoes, fire, flood, etc.), equipment failures, process failures, mistakes or errors in judgement, or malicious acts (such as denial of service attacks, hacking, viruses, and arson).

2. Policy:

2.1: TDMHSAS must develop procedures for implementation in the event of an emergency, disaster, or occurrence (i.e., fire, vandalism, system failure, and natural disaster) where any system that contains electronic protected health information (PHI) is affected. Such procedures must minimize data loss, protect data from unauthorized access or manipulation, ensure continuity of critical business functions, and provide for restoration of services. Procedures must include the following:

2.1.1: Applications and data criticality analysis known as a Business Impact Analysis, reviewed annually;

2.1.2: Data backup plan;

2.1.3: Disaster recovery plan;

2.1.4: Emergency mode operation plan (Business Continuity Plan).

2.1.5: Information System Continuity Plans for each system that is agency owned; and

2.1.6: A Cyber Incident Response Plan, reviewed annually

3. Procedure/ Responsibility:

3.1: Each RMHI CEO must designate a person responsible for development and maintenance of the plans required by this policy. The designations must be reported to the TDMHSAS Director of IT and the TDMHSAS Security Officer.

3.2: Applications and Data Criticality Analysis

3.2.1: Each RMHI and the TDMHSAS must assess the relative criticality of specific applications and data to develop their Data backup plan, Disaster recovery plan, and Emergency Mode Operation (Business Continuity) Plan.

3.2.2: The assessment of data and application criticality must be done at least annually to ensure that appropriate procedures are in place.

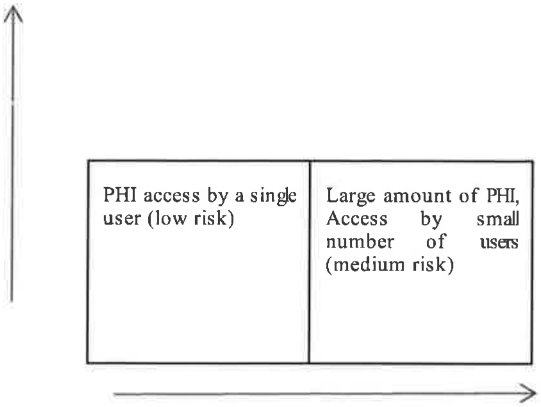
3.2.3: Each identified PHI information system must be analyzed for potential vulnerability to the integrity, confidentiality, and availability of its PHI. The following two-dimensional model can be used to assign a risk level to each PHI repository.

High Risk—Repositories with a large number of records accessed by a large number of users or any repository of PHI necessary for critical business operations;

Medium Risk—Repositories with either a large number of records and a small number of users or a small number of records and a large number of users;

Low Risk—Repositories with a small number of records accessed by a small number of users (i.e. personal patient lists and notes, etc.).

# of users that access PHI	Small amount of PHI, Access by large number of users (medium risk)	Large amount of PHI, Access by large numbers of users OR PHI necessary for critical business operations (high risk)



PHI access by a single user (low risk)	Large amount of PHI, Access by small number of users (medium risk)

# of patient records (amount of Phi)

PHI repositories that fall in the low or medium risk categories may be classified as high risk if the sensitivity or criticality of that information makes it appropriate to do so in the reasonable judgement of the entity charged with determining the level of risk.

3.3: Data Backup Plan

3.3.1: Some data stores may reside on equipment owned and/ or managed by the Division of Strategic Technological Solutions (STS) in the Department of Finance and Administration, some on equipment owned and managed by the TDMHSAS, and others on equipment under a joint arrangement between STS and TDMHSAS. Regardless of ownership and management responsibility, each TDMHSAS and RMHI (in concert where appropriate) must establish and implement a Data Backup Plan by which retrievable exact copies of all PHI determined to be medium and high risk are created and maintained. Data Backup Plans must be reviewed at least annually and modified as needed.

3.3.2: The Data Backup Plan must apply to all medium and high-risk files, records, images, voice, or video files that may contain PHI.

3.3.3: Minimally, PHI backups must be performed once each day of operation (excluding holidays and weekdays).

3.3.4: All media used for backing up PHI must be stored in secure location with controlled access, such as a secure, off-site storage facility. If backup media remains on site, it must be stored in a physically secure location, separate from the physical location of the computer systems it backed up (i.e. separate physical building).

3.3.5: STS maintains and/or stores all information systems. If an off-site storage facility or backup service is used, a written contract or business associate agreement (BAA) must be used to ensure that the business associate will safeguard PHI appropriately.

3.3.6: The data backup plan must define exactly what (?) information is needed to be retrievable to allow the entity to continue business "as usual" in the face of damage or destruction of data, hardware, or software.

3.3.7: Data backup procedures outlined in the Data backup plan must be tested periodically to ensure that exact copies of PHI can be retrieved and made available.

3.4: Disaster Recovery Plan

3.4.1: Some data stores may reside on equipment owned and/or managed by STS in the Department of Finance and Administration, some on equipment owned and/or managed by the TDMHSAS, and others on equipment under a joint arrangement between STS and TDMHSAS. Regardless of ownership and management responsibility, each RMHI and the TDMHSAS Central Office (in concert with STS where appropriate) must establish and implement a Disaster Recovery Plan to ensure their availability to recover from loss of data or access to data due to an emergency or disaster including, but not limited to, fire, vandalism, terrorism, system failure, or natural disaster affecting systems containing electronic PHI.

3.4.2: The Disaster Recovery Plan must assure restoration of electronic PHI and the systems needed to make the electronic PHI available in a timely manner.

3.4.3: Plans must be updated whenever computing or telecommunications environments undergo significant changes. Such changes may include, but are not limited to physical facility, computer hardware/software, telecommunications hardware/software, telecommunications networks, application systems, organization, or budget.

3.4.4: The Disaster Recovery Plan must:

(1): Be documented and easily available at all times to the personnel who are trained to implement the Disaster Recovery Plan;

(2): Include a "chain of communication" (call tree) as the basis for notifying appropriate personnel of the disaster with instructions for reporting to the designated recovery site;

(3): Apply to medium and high-risk electronic PHI information systems;

(4): Include procedures to log system outrages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the Disaster Recovery Plan;

(5): Include procedures to restore electronic PHI from data backups;

(6): Be tested periodically to ensure that electronic PHI and the systems needed to make it available can be restored or recovered;

(7): Be reviewed, updated, and tested annually, or more frequently, if appropriate.

3.5: Emergency Mode Operation Plan

3.5.1: Each RMHI and the TDMHSAS must establish an Emergency Mode Operation Plan and implement procedures, as needed, to enable continuation of critical business processes in the event of the electronic PHI data loss or system failure. Emergency Mode Operation Plans must be reviewed at least annually and modified as needed.

3.5.2: The Emergency Mode Operation Plan must include a "chain of communication" (call tree) as the basis for notifying appropriate personnel of the emergency with instructions for reporting to the designated emergency operations site.

3.5.3: Emergency mode operation procedures outlined in the Emergency Mode Operation Plan must be tested periodically to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.

4. Other Considerations

4.1: Authority: 45 CFR §§164.308, and 164.310.

Approved:

Marie Williams

Commissioner

1-18-2023

Date