Department of
Mental Health &
Substance Abuse Services

Policies and Procedures

Subject:	Uses and disclosures: Organizational requirements for Business Associates
Policy Number:	HIPAA 4.2
Effective Date:	5/15/04
Entity Responsible:	Division of General Counsel
Revision Date:	1/18/2023

1. Purpose:

To provide instructions and guidance to Tennessee Department of Mental Health and Substance Abuse Services (TDMHSAS) and the Regional Mental Health Institutes (RMHIs) regarding how to use, disclose, and request protected health information (PHI) consistent with the organizational requirements for business associates under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and other relevant federal and state laws.

2. Policy:

2.1: Business associate contracts or other arrangements must comply with the requirements of HIPAA.

2.2: The Tennessee Department of Mental Health and Substance Abuse Services (TDMHSAS) and the Regional Mental Health Institutes (RMHIs) are not in compliance with HIPAA standards if, TDMHSAS or applicable RMHI knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associates obligation under the contract or other arrangement, unless TDMHSAS or RMHI took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

2.3: A business associate is not in compliance with HIPAA standards, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure

the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

2.4: A contract between the TDMHSAS or the RMHIs and a business associate must:

2.4.1: Establish the permitted and required uses and disclosures of PHI by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of HIPAA, if done by the TDMHSAS or the RMHIs, except that:

(a): The contract may permit the business associate to use and disclose PHI for the proper management and administration of the business associate, as provided under HIPAA; and

(b): The contract may permit the business associate to provide data aggregation services relating to the health care operations of the TDMHSAS or RMHI.

2.4.2: A business associate will:

(1): Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(2): Use appropriate safeguards and comply with HIPAA with respect to electronic PHI, to prevent use or a disclosure of information other than as provided for by its contract;

(3): Report to the TDMHSAS or RHMI any use or disclosure of information not provided for by its contract of which it becomes aware, including breaches of unsecured PHI;

(4): Ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

(5): Make available PHI in accordance with HIPAA standards;

(6): Make available PHI for amendment and incorporate any amendments to PHI in accordance with HIPAA standards;

(7): Make available the information required to provide an accounting of disclosures in accordance with HIPAA standards;

(8): To the extent the business associate is to carry out TDMHSAS or RMHI obligations under HIPAA, comply

with the requirements of HIPAA that apply to TDMHSAS or RMHI in the performance of such obligation;

(9): Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of the TDMHSAS or applicable RMHI available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining the TDMHSAS or applicable RMHIs compliance with HIPAA;

(10): At the termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the business associate on behalf of the TDMHSAS or RHMI that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protection of the contract to the information and limit further uses and disclosures to those purposes that make the return of the information infeasible.

2.4.3: Authorize termination of the contract by the TDMHSAS or applicable RMHI, if TDMHSAS or RMHI determines that the business associate violated a material term of the contract.

2.5: If the TDMHSAS or RMHI and its business associate are both governmental entities:

2.5.1: Both governmental entities may enter into a memorandum of understanding that contains terms that accomplish the objectives of this policy and HIPAA standards.

2.5.2: The TDMHSAS or RMHI may comply with HIPAA, if other law (including regulations adopted by TDMHSAS or RHMI or its business associate) contains requirements applicable to the business associate that accomplish the objectives of this policy.

2.6: If the business associate is required by law to perform a function or activity on behalf of the TDMHSAS or RMHI, the TDMHSAS or RMHI may disclose PHI to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of HIPAA, provided that the TDMHSAS or RMHI attempts in good faith to obtain satisfactory assurances as required by HIPAA. If such attempt fails, the TDMHSAS or RMHI shall document the attempt and the reasons that such assurances cannot be obtained.

2.7: The TDMHSAS or RMHI may omit from its other arrangements the termination authorization required by paragraph 2.4.3 of this policy, if such authorization is inconsistent with the statutory obligations of TDMHSAS or its business

associate.

2.8: The TDMHSAS or RMHI may comply with HIPAAs organizational requirements if the TDMHSAS or RMHI discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the TDMHSAS or RMHI has a data use agreement with the business associate that complies with HIPAA.

2.9: The contract or other arrangement between the TDMHSAS or RMHI and the business associate may permit the business associate to use the PHI received by the business associate in its capacity as a business associate to the TDMHSAS or RMHI, if necessary:

2.9.1: For the proper management and administration of the business associate; and/or

2.9.2: To carry out the legal responsibilities of the business associate;

2.10: The contract or other arrangement between the TDMHSAS or RMHI and the business associate may permit the business associate to disclose the PHI received by the business associate in its capacity as a business associate, if:

2.10.1: The disclosure is required by law; or

2.10.2:

a. The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and

b. The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

2.11: The requirements of this policy apply to the contract or other arrangement between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between the TDMHSAS or RMHI and business associate.

3. Procedure/ Responsibility:

3.1: The TDMSAS Privacy Officer must ensure that every service contract contains a HIPAA compliance clause that provides for the execution of a BAA.

3.2: The TDMHSAS Privacy Officer must ensure that BAAs are developed as required by HIPAA regulations and this policy for any business associates of the TDMHSAS and the RMHI. The TDMHSAS Privacy Officer must ensure that the

terms of the BAAs conform to the requirements above.

3.3: When a member of the TDMHSAS or the RMHI workforce receives a request for use or disclosure of PHI from a business associate for purposes other than treatment, payment, or healthcare operations, he or she must check with the TDMHSAS Privacy Officer or the RMHI Privacy Officer to ensure that a BAA is on file. The RMHI Privacy Officer must confirm with the TDMHSAS Privacy Officer that a BAA is on file. If no BAA is on file, PHI should not be shared.

3.4: The TDMHSAS Privacy Officer must ensure that a BAA file is maintained at the Central Office, which must contain originals of all BAAs executed between the TDMHSAS or RMHIs and their business associates. All BAAs must be kept for six (6) years after the BAA is no longer in effect.

4. Other Considerations

4.1: Authority

45 C.F.R. §§164.502(e), 504, 514(b), and 45 C.F.R. §164.314.

Approved:

Commissioner

1-18-2023

Date