Department of Mental Health & Substance Abuse Services

# Policies and Procedures

| | |
|---|---|
| Subject: | Other requirements relating to uses and disclosures of protected health information |
| Policy Number: | HIPAA 4.7 |
| Effective Date: | 7/1/04 |
| Entity Responsible: | Division of General Counsel |
| Revision Date: | 1/18/2023 |

## 1. Purpose:

To provide instruction and guidance on other requirements relating to uses and disclosures of protected health information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and other state and federal laws.

## 2. Policy:

2.1: It is the policy of the TDMHSAS and the RMHIs not to use or disclose PHI except as permitted or required by HIPAA regulations, and other relevant federal and state laws.

2.2: The following guidance applies to other requirements relating to uses and disclosures of PHI under HIPAA and which may apply to other relevant federal and state laws.

2.3: Prior to using or disclosing PHI, all members of the TDMHSAS or RMHIs workforce shall ensure that that the use or disclosure is consistent with both federal and state law. If the member of the workforce is unsure whether the use or disclosure is consistent with both federal and state law, the member of the workforce shall consult with the TDMHSAS Division of General Counsel and the applicable Privacy Officer.

2.4: De-identification of PHI.

2.4.1: Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be

used to identify an individual is not individually identifiable health information.

2.5: Requirements for de-identification of PHI.

2.5.1: The TDMHSAS or RMHI, in consultation with the TDMHSAS Privacy Officer or RMHI Privacy Officer, as applicable, may determine that health information is not individually identifiable health information only if:

2.5.2: A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(a): Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(b): Documents the methods and results of the analysis that justify such determination; or

2.5.3 (i): The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A): Names;

(B): All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1): The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2): The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C): All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D): Telephone numbers;

(E): Fax numbers;

(F): Electronic mail addresses;

(G): Social security numbers;

(H): Medical record numbers;

(I): Health plan beneficiary numbers;

(J): Account numbers;

(K): Certificate/license numbers;

(L): Vehicle identifiers and serial numbers, including license plate numbers;

(M): Device identifiers and serial numbers;

(N): Web Universal Resource Locators (URLs);

(O): Internet Protocol (IP) address numbers;

(P): Biometric identifiers, including finger and voice prints;

(Q): Full face photographic images and any comparable images; and

(R): Any other unique identifying number, characteristic, or code, except as permitted under HIPAA; and

(ii): The TDMHSAS or the RMHI does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

2.6: Re-identification.

2.6.1: The TDMHSAS or the RMHI, in consultation with the TDMHSAS Privacy Officer or RMHI Privacy Officer, as applicable, may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the TDMHSAS or the RMHI, provided that:

2.6.2: The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

2.6.3: The covered entity does not use or disclose the code or other means of record identification for any other purpose and does not disclose the mechanism for re-identification.

2.7: Minimum necessary requirements.

2.7.1: In order to comply with HIPAA and this policy, the TDMHSAS or the RMHI must meet the requirements of paragraphs 2.7.2 through 2.7.4 of this policy with respect to a request for, or the use and disclosure of, PHI.

2.7.2: Minimum necessary disclosures of PHI.

(i): For any type of disclosure that the TDMHSAS or the RMHI makes on a routine and recurring basis, the TDMHSAS or the RMHI must implement policies and procedures (which may be standard protocols) that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii): For all other disclosures, the TDMHSAS or the RMHI must:

(A): Develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(B): Review requests for disclosure on an individual basis in accordance with such criteria.

(iii): The TDMHSAS or the RMHI may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(A): Making disclosures to public officials that are permitted under HIPAA, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(B): The information is requested by another covered entity;

(C): The information is requested by a professional who is a member of its workforce or is a business associate of TDMHSAS or RMHI for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(D): Documentation or representations that comply with the applicable requirements of a HIPAA authorization have been provided by a person requesting the information for research purposes.

2.7.3: Minimum necessary requests for PHI.

(i): The TDMHSAS or the RMHI must limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(ii): For a request that is made on a routine and recurring basis, the TDMHSAS or the RMHI must implement policies and procedures (which may be standard protocols) that limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii): For all other requests, TDMHSAS or RMHI must:

(A): Develop criteria designed to limit the request for PHI to the information reasonably necessary to accomplish the purpose for which the request is made; and

(B): Review requests for disclosure on an individual basis in accordance with such criteria.

2.7.4: Implementation specification: Other content requirement. For all uses, disclosures, or requests to which the requirements in paragraph 2.7 of this policy apply, TDMHSAS or RMHI may not use, disclose, or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

2.8: Limited data set.

2.8.1: The TDMHSAS or the RMHI may use or disclose a limited data set that meets the requirements of paragraphs 2.8.2 and 2.8.3 of this policy, if the TDMHSAS or the RMHI enters into a data use agreement with the limited data set recipient, in accordance with paragraph 2.9 of this policy.

2.8.2: Implementation specification: Limited data set: A limited data set is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(i): Names;

(ii): Postal address information, other than town or city, State, and zip code;

(iii): Telephone numbers;

(iv): Fax numbers;

(v): Electronic mail addresses;

(vi): Social security numbers;

(vii): Medical record numbers;

(viii): Health plan beneficiary numbers;

(ix): Account numbers;

(x): Certificate/license numbers;

(xi): Vehicle identifiers and serial numbers, including license plate numbers;

(xii): Device identifiers and serial numbers;

(xiii): Web Universal Resource Locators (URLs);

(xiv): Internet Protocol (IP) address numbers;

(xv): Biometric identifiers, including finger and voice prints; and

(xvi): Full face photographic images and any comparable images.

2.8.3: Implementation specification: Permitted purposes for uses and disclosures.

(i): The TDMHSAS or the RMHI may use or disclose a limited data set under paragraph 2.8 of this policy only for the purposes of research, public health, or health care operations.

(ii): The TDMHSAS or the RMHI may use PHI to create a limited data set that meets the requirements of paragraph 2.8.2 of this policy, or disclose PHI only to a business associate for such purpose, whether or not the limited data set is to be used by the TDMHSAS or the RMHI.

2.9: Data use agreement.

2.9.1: The TDMHSAS or the RMHI may use or disclose a limited data set under paragraph 2.8.1 of this policy only if TDMHSAS or the RMHI obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the PHI for limited purposes.

2.9.2: A data use agreement between the TDMHSAS or the RMHI and the limited data set recipient must:

(A): Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph 2.8.3 of this policy. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this policy, if done by the TDMHSAS or the RMHI;

(B): Establish who is permitted to use or receive the limited data set; and

(C): Provide that the limited data set recipient will:

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

(2): Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

(3): Report to the TDMHSAS or the RMHI any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

(4): Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

(5): Not identify the information or contact the individuals whose information is subject to the limited data set.

2.9.3: The TDMHSAS or the RMHI is not in compliance with the standards in paragraphs 2.8 and 2.9 of this policy if the TDMHSAS or the RMHI knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the TDMHSAS or the RMHI took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(1): Discontinued disclosure of PHI to the recipient; and

(2): Reported the problem to the Secretary of the Department of Health and Human Services.

2.9: Standard: Verification requirements.

2.9.1: Prior to any disclosure permitted by this policy, the TDMHSAS or the RMHI must:

(i): Verify the identity of a person requesting PHI and the authority of any such person to have access to PHI under this section, if the identity or any such authority of such person is not known to the TDMHSAS or the RMHI.

(ii): The person requesting PHI must show a valid picture ID, and when required (if requester is someone other than parent), appropriate court or legal documents showing his or her relationship to the service recipient, or former service recipient, and when required (if requester is someone other than parent), appropriate documents to show his or her authority to act on behalf of service recipient or former service recipient; and

(iii): Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when such documentation, statement, or representation is a condition of the disclosure under this subpart. For example, if the disclosure of PHI requires consent of the service recipient, or former service recipient whose records are being requested, the person requesting the disclosure of PHI shall be provided with a copy of TDMHSAS's Form "Authorization to Release Confidential Information" or directed to where one can be obtained online at: https://www.tn.gov/behavioral-health/mhsa-law/legal-forms.html. The TDMHSAS and/or RMHI may disclose PHI upon receipt of a valid, completed authorization to release information in accordance with TDMHSAS HIPAA policy 4.4.

2.9.2: Implementation specifications: Verification.

(i): Conditions on disclosures. If a disclosure is conditioned by this policy on particular documentation, statements, or representations from the person requesting the PHI, TDMHSAS or RMHI may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

(A): The conditions under TDMHSAS HIPAA policy 4.6 regarding disclosures made pursuant to an administrative subpoena may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(B): The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).

(ii): Identity of public officials. The TDMHSAS or the RMHI may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

(A): If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(B): If the request is in writing, the request is on the appropriate government letterhead; or

(C): If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii): Authority of public officials. TDMHSAS or RMHI may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

(A): A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B): If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv): Exercise of good faith. The verification requirements of this paragraph are met if the TDMHSAS or RMHI acts on a good faith belief in making a use or disclosure in accordance with TDMHSAS HIPAA Policy 4.5 or making a disclosure in accordance with TDMHSAS HIPAA Policy 4.6.

(v): Exercise of individual rights. The TDMHSAS or RMHI may not impose unreasonable verification measures on an individual that would impede the individual from exercising a right under this part. An unreasonable measure is one that causes an individual to expend unnecessary effort or resources

when a less burdensome verification measure is practicable for the TDMHSAS or RMHI. Practicability considerations include the TDMHSAS or RMHI technical capabilities, its obligations to protect the privacy of PHI under § 164.530(c), the security of electronic PHI under § 164.306, and the costs of implementing measures that are more convenient for individuals. Examples of unreasonable measures include requiring an individual to provide proof of identity in person when a method for remote verification is practicable for the TDMHSAS or RMHI and more convenient for the individual or requiring an individual to obtain notarization of the individual's signature on a written request to exercise the individual right.

**3. Procedure/ Responsibility:**

3.1: The TDMHSAS Privacy Officer and the RMHI Privacy Officers are responsible for ensuring that the HIPAA and other privacy law requirements under this policy are followed department wide.

3.2: The RMHI Privacy Officers shall consult with the TDMHSAS Privacy Officer with any questions about the HIPAA and other privacy law requirements under this policy and determining when a use, disclosure or request applicable to this policy is necessary.

[SIGNATURE APPEARS ON FOLLOWING PAGE]

**4. Other Considerations:**

4.1: Authority:

45 CFR § 164.514.

Approved:

Commissioner

1-18-2023

Date