Department of Mental Health & Substance Abuse Services

Policies and Procedures

Subject:	Notification in Case of Breach
Policy Number:	HIPAA 3.5
Effective Date:	1/11/18
Entity Responsible:	Division of General Counsel
Revision Date	1/18/2023

1. Purpose:

To provide procedures to the Tennessee Department of Mental Health and Substance Abuse Services (TDMHSAS or Department) and the Regional Mental Health Institutes (RMHIs) on how to notify each individual whose unsecured protected health information (PHI) has been or is reasonably believed by TDMHSAS or the RMHIs to have been accessed, acquired, used, or disclosed as a result of a breach in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and other state and federal laws.

2. Policy:

2.1: The TDMHSAS and/or the applicable RMHI shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the TDMHSAS and/or applicable RHMI to have been accessed, acquired, used, or disclosed as a result of a breach.

2.2: A breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA privacy rule which compromises the security or privacy of the PHI.

2.3: A breach excludes the following:

2.3.1: Any unintentional acquisition, access, or use of PHI by a member of the TDMHSAS or the RMHI workforce or person acting under the authority of TDMHSAS or the RMHI or a Business Associate of TDMHSAS or the RMHI, if such acquisition, access, or use of PHI was made in good faith and within the scope of authority and does not result in a further use or disclosure in a manner not permitted under the HIPAA privacy rules and regulations; or

2.3.2: Any inadvertent disclosure by a person who is authorized to access PHI at TDMHSAS or the RMHI or a Business Associate of TDMHSAS or the RMHI to another person who is also authorized to access the PHI at TDMHSAS or the RMHI or a Business Associate, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA privacy rules and regulations; or

2.3.3: A disclosure of PHI where TDMHSAS, the RMHI, or a Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2.4: Except as provided in paragraph 2.3 of this policy, an acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA privacy rules and regulations is presumed to be a breach unless TDMHSAS, the RMHI, or a Business Associate of TDMHSAS or the RMHI, as applicable, demonstrates that there is a low probability that the PHI has been compromised based upon a risk assessment, which includes the following factors:

2.4.1: The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2.4.2: The unauthorized person who used the PHI or to whom the disclosure was made;

2.4.3: Whether the PHI was actually acquired or viewed; and

2.4.4: The extent to which the risk to the PHI has been mitigated.

2.5: A breach is deemed to have been discovered by TDMHSAS or the RMHI as of the first day on which such breach is known to TDMHSAS or the RMHI, or, by exercising reasonable diligence would have been known to TDMHSAS or the RMHI.

2.6: TDMHSAS or the RMHI will be deemed to have knowledge of the breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member of TDMHSAS or the RMHI or is an agent of TDMHSAS or the RMHI.

3. Procedures/ Responsibilities:

3.1: Any member of the applicable RMHI workforce who discovers an access, use, or disclosure of PHI which is not permitted under the HIPAA privacy rules must immediately, upon discovery of such information, notify their supervisor, RMHI Privacy Officer, and the RMHI Security Officer if such breach relates to the RMHI. If the RMHI Privacy Officer and the RMHI Security Officer receives notification of a breach, they must immediately notify the TDMHSAS Privacy Officer and the

TDMHSAS Security Officer. The TDMHSAS Privacy Officer and TDMHSAS Security Officer will then notify appropriate individuals within Central Office.

3.2: Any member of the TDMHSAS workforce who discovers an access, use, or disclosure of PHI which is not permitted under the HIPAA privacy rules must immediately, upon discovery of the breach, notify their supervisor, the TDMHSAS Privacy Officer, and the TDMHSAS Security Officer. The TDMHSAS Privacy Officer and the TDMHSAS Security Officer will then notify appropriate individuals within Central Office.

3.3: Upon notification, the TDMHSAS Privacy Officer will make the determination of whether a breach in fact occurred. If the TDMHSAS Privacy Officer determines that a breach occurred, the TDMHSAS Privacy Officer, or their designee, will ensure that TDMHSAS and/or the RMHI provide adequate notice to the individuals impacted as described in paragraphs 3.4 through 3.9 of this policy.

3.4: If the breach of unsecured PHI involves less than 500 residents of a State, the TDMHSAS Privacy Officer, or their designee, will provide notification to the individuals regarding the breach. Such notification will be provided without unreasonable delay and must be provided within sixty (60) calendar days of the discovery of the breach. The notification will be written in plain language and include:

3.4.1: A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

3.4.2: A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3.4.3: Any steps individuals should take to protect themselves from potential harm resulting from the breach;

3.4.4: A brief description of what TDMHSAS and/or the RMHI is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and

3.4.5: Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Website, or postal address.

3.5: If the breach of unsecured PHI involves less than 500 residents of a State, TDMHSAS will provide the notification described in paragraph 3.4 of this policy in the following form:

3.5.1: Written notification by first-class mail to the impacted service recipient at the last known address of the service recipient, or, if the service recipient

agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

3.5.1.1: If TDMHSAS or the RMHI knows that the impacted service recipient is deceased and has the address of the next of kin or personal representative of the individual, written notification provided by first-class mail may be provided to either of those parties. If TDMHSAS or the RMHI is unable to provide notification to next of kin or personal representative due to insufficient or out-of-date contact information, substitute notification (as described below) is not necessary.

3.5.2: If there is insufficient or out-of-date information that precludes the written notice described in paragraph 3.5.1 of this policy, the TDMHSAS or the RMHI may provide a substitute form of notice reasonably calculated to reach the service recipient shall be provided, as described below:

3.5.2.1: If a substitute form of notice is needed for fewer than ten (10) service recipients, such substitute notice may be provided in alternative form of written notice, telephone, or other means; or

3.5.2.2. If substitute form notice is needed for more than ten (10) service recipients, such substitute notice shall be provided in either a conspicuous posting for a period of ninety (90) days on the TDMHSAS web homepage, or conspicuous notice in major print or broadcast media in geographic areas where the service recipients affected in the breach are likely to reside; and include a toll-free phone number that remains active for the ninety (90) day period where a service recipient can learn whether their unsecured PHI was included in the breach.

3.5.3: If TDMHSAS and/or the RMHI determines the situation requires urgency because of possible imminent misuse of unsecured PHI, notice may be provided to individuals by telephone, or other means, as appropriate, in addition to the notification methods described above.

3.6: If the breach of unsecured PHI involves more than 500 residents of a State, TDMHSAS shall notify prominent media outlets serving the State. This notification must be provided without unreasonable delay and in no case later than sixty (60) calendar days of the discovery of the breach. The notification will be written in plain language and include:

3.6.1: A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

3.6.2: A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3.6.3: Any steps individuals should take to protect themselves from potential harm resulting from the breach;

3.6.4: A brief description of what TDMHSAS and/ or the RMHI is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and

3.6.5: Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Website, or postal address.

3.7: In the case of any breach of unsecured PHI, the TDMHSAS Privacy Officer shall notify the Department of Health and Human Services (DHHS) in the manner specified on the DHHS website.

3.7.1: For breaches involving less than 500 individuals, the TDMHSAS Privacy Officer shall keep a log or other documentation, and not later than 60 days after the end of the calendar year, provide the notification to DHHS as required.

3.7.2: For breaches involving more than 500 individuals, the TDMHSAS shall contemporaneously provide the notification to DHHS as required.

3.8: Any Business Associate shall, following the discovery of a breach of unsecured PHI, notify the TDMHSAS without unreasonable delay and not later than sixty (60) days after discovery of the breach. If this notification is provided to any member of the TDMHSAS workforce other than the TDMHSAS Privacy Officer, the member of the TDMHSAS workforce shall promptly notify the TDMHSAS Privacy Officer of this notification. The notification by the Business Associate shall include to the extent possible:

3.8.1: The identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been accessed, acquired, used, or disclosed during the breach; and

3.8.2: Any other available information, as it becomes available, that the TDMHSAS and the RMHI is required to provide in their notification to the individuals as described in paragraphs 3.4 through 3.6 of this policy.

3.9: If a law enforcement official states to TDMHSAS or the RMHI or a Business Associate of TDMHSAS or the RMHI, that a notification, notice or posting described above and required under the law would impede a criminal investigation

or cause damage to national security, the TDMHSAS, RMHI, or the Business Associate of the TDMHSAS or RMHI shall:

3.9.1: If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

3.9.2: If the statement is made orally, the TDMHSAS Privacy Officer shall document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than thirty (30) days from the date of the oral statement, unless a written statement as described above is provided during that time.

4. Other Considerations:

4.1: Authority

45 C.F.R. §§164.400, 164.402, 164.404, 164.406, 164.408, 164.410, 164.410, and 164.412.

Approved:

Commissioner

1-18-2023

Date