MSHN
Mid-State Health Network

POLICIES AND PROCEDURE MANUAL

Chapter:	Information Technology		
Title:	Breach Notification Procedure		
Policy: ☐ Procedure: ☒ Page: 1 of 4	Review Cycle: Biennial Author: Chief Information Officer	Adopted Date: 11.2017 Review Date: 09.12.23	Related Policies: Information Management Breach Notification Policy

Purpose

To ensure that Mid-State Health Network (MSHN) maintains HIPAA security breach notification procedures that meet legal and regulatory standards under the Medicaid Specialty Supports and Services contract and federal and state privacy guidelines and to ensure compliance with notification requirements.

Procedure

Reporting and Documentation Requirements

Mid-State Health Network personnel, who believe there has been a breach of protected health information shall notify Mid-State Health Network's Privacy and Security Officers immediately.

A. Upon receipt of a breach or suspected breach of PHI, the Mid-State Health Network Privacy Officer will:
    1. Record the date that the suspected breach was known, or should have reasonably been known, to the organization;
    2. Determine if an actual breach occurred; and
    3. If a breach occurred:
        a. Record the date the breach occurred
        b. To the extent that is practical, mitigate the cause of the breach;
        c. If the organization is acting as a business associate, notify the covered entity as soon as possible, but no later than the time frame stipulated in the applicable business associate agreement, which cannot be more than 60 calendar days from the date of knowledge as required by federal law;
        d. Provide notice, as required by federal law, to the individual affected by the breach outlined below;
        e. Provide notice, as required by federal law to the Department of Health and Human Services, as outlined below; and
        f. Conduct post-breach evaluation and remediation.
    4. Ensure all required notifications have been provided, or that a use or disclosure of unsecured PHI did not constitute a breach.
    5. With respect to an impermissible use or disclosure, Mid-State Health Network will maintain documentation that all required notifications were made, or alternatively, documentation to demonstrate that notification was not required, such as: (1) the risk assessment demonstrating a low probability that the PHI has been compromised by theimpermissible use or disclosure; or (2) the application of any other exceptions to the definition of "breach."

Breach Notification Requirements

A breach shall be treated as discovered as of the first day on which such breach is known by the Covered Entity/Business Associate, or, by exercising reasonable diligence would have been known to either. Covered Entity/Business Associate shall be deemed to have knowledge of a 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 or agent.

Following the discovery of a breach of unsecured protected health information, the Covered Entity shall notify each individual whose unsecured protected health information has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach.

A. Individual Notice

Covered Entity shall notify affected individuals in written form by first class mail to their last known address. Notice must be provided without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. The notification may be provided in one or more mailings as information is available. If the individual is deceased written notification by first class mail will be sent to the personal representative of the individual, if known.

1. The notice shall include:
    a. A brief description, in plain language, of what happened, including the date of the breach and the date of the discovery of the breach, if known;
    b. A description of the types of unsecured protected health information 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);
    c. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
    d. A brief description of what the Covered Entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
    e. Contact information for individuals to ask questions or learn additional information, including a toll-free number and email address.

B. Substitute Notice – Insufficient or Out-of-Date Contact Information

1. If Covered Entity has insufficient or out-of-date contact information for fewer than 10 individuals, Covered Entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.
2. If Covered Entity has insufficient or out-of-date information for 10 or more individuals, Covered Entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individual likely resides. A toll-free phone number that remains active for at least 90 days must be included.
3. These notices must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach.

C. Additional Notice in Urgent Situations

If Covered Entity deems a breach to be a potential for imminent misuse of unsecured PHI, Covered Entity may provide information to individuals by telephone or other means, as appropriate, in addition to the written notice.

D. Notification to the Media

For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, Covered Entity shall notify prominent media outlets serving the State or jurisdiction. Media notification shall be provided without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. Media notification shall include the same information required for the individual notice.

E. Notification to the Secretary of Health and Human Services

In addition to notifying affected individuals and the media (where appropriate), Covered Entity must notify the Secretary of breaches of unsecured PHI. Notification is made electronically at the HHS web site on the breach report form provided. If a breach affects 500 or more individuals, Covered Entity must notify the Secretary without reasonable delay and in no case later than 60 days following the discovery of a breach. If, however, a breach affects fewer than 500 individuals, Covered Entity may notify the Secretary of such breaches on an annual basis, no later than 60 days after the end of the calendar year in which the breaches are discovered.

F. Notification to a Covered Entity

If Mid-State Health Network is a Business Associate of another Covered Entity, Mid-State Health Network will notify the covered entity immediately following the discovery of a potential breach of the covered entity's protected health information. The Covered Entity will file necessary notification to individuals, Secretary of HHS and the media, as applicable, unless stated otherwise in the Business Associate Agreement.

G. Law Enforcement Delay

If a law enforcement official states that a notification, notice, or posting required under this procedure would impede a criminal investigation or cause damage to national security, Covered Entity or Business Associate shall:

a. delay such notification, notice, or posting for the time period specified by the official, if the statement is in writing and specifies the time for which a delay is required, or
b. document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, if the statement is made orally; or unless a written statement as described in paragraph (a) of this section is submitted during that time.

Applies to

☒All Mid-State Health Network Staff
☐ Selected MSHN Staff, as follows:
☒MSHN's CMHSP Participants: ☐Policy Only ☒Policy and Procedure
☒Other: Sub-contract Providers

Definitions

Business Associate: A HIPAA business associate is any organization or person working in association with or providing services to a covered entity who handles or discloses Personal Health Information (PHI) or Personal Health Records (PHR).
Covered Entity: A HIPAA covered entity is any organization or corporation that directly handles Personal Health Information (PHI) or Personal Health Records (PHR). The most common examples of covered entities include hospitals, doctors' offices and health insurance providers.
Breach: An impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information.
Unsecured protected health information: protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section13402(h)(2) of Public Law 111–5 (HITECH Act) on the HHS Web site.
Workforce: employees, volunteers, trainees, and other persons whose conduct, in the performance of work for Mid-State Health Network or a business associate, is under the direct control of Mid-State Health Network or a business associate, whether or not they are paid by Mid-State Health Network or a business associate.

Other Related Materials
MSHN Compliance Plan

References/Legal Authority
45 CFR § 164 Privacy of Individually Identifiable Health Information
45 CFR § 164.400-414 Breach Notification Rule
Public Law 111-5 Health Information Technology for Economic and Clinical Health Act (HITECH Act)

Change Log:

Date of Change	Description of Change	Responsible Party
06.21.2017	New Procedure	Chief Information Officer
06.2018	Annual Review	Chief Information Officer
06.2019	Annual Review	Chief Information Officer
06.2021	Biennial Review	Chief Information Officer
05.2023	Biennial Review	Chief Information Officer