POLICY AND PROCEDURE MANUAL

SUBJECT Breach Notification	ACCOUNTABILITY: NMRE, NMRE Network Providers	Effective Date: March 2, 2020	Pages: 3
REQUIRED BY	BBA Section: PIHP Contract Section: 18.1.7 Other: 45 CFR 160 – 164	Last Review Date:	Past Review Date:
Policy: ☒ Procedure: ☐	Review Cycle: Annual Author: NMRE Compliance Coordinator	Responsible Department: Compliance	Reviewers:

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 Electronic Health Records (EHR). For the purposes of this policy, a "Business Associate" is a "Network Provider."

Breach: The acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of the protected health information.

The definition of a breach that requires notification includes:

(1) Unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity or business associate, if it was made in good faith, within the course and scope of employment or professional relationship and does not result in further use or disclosure;
(2) Certain limited unintentional or inadvertent disclosures made by employees or authorized individuals within the same facility; or
(3) Where the PHI was disclosed to a person who would not reasonably be able to retain the disclosed information.

Compromises the Security or Privacy or the Protected Health Information: Poses a significant risk of financial, reputational, or other harm to an individual.

Covered Entity: A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in an electronic form in connection with a HIPAA transaction.

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of information outside the covered entity or business associate holding the information.

Discovery of a Breach: A breach of PHI will be treated as "discovered" as of the day on which the beach is known to the covered entity, by exercising reasonable diligence, would have been known to the covered entity (including breaches by business associates).

EHR: Electronic Health Record.

Health Insurance Portability and Accountability Act (HIPAA): United States legislation that provides data privacy and security provisions for safeguarding medical information.

HIPAA Privacy Rules: National standards to protect individuals' medical records and other personal health information that apply to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

MDHHS: Michigan Department of Health and Human Services.

Network Provider: Any provider that receives Medicaid funding directly or indirectly to order, refer, or render covered services as a result of the state's contract with the NMRE, its member CMHSPs, and the Substance Use Disorder provider panel. For the purposes of this policy, a "Network Provider" is a "Business Associate."

PIHP: Prepaid Inpatient Health Plan.

Protected Health Information (PHI): Individually identifiable information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

Risk Assessment: A analysis performed by the covered entity or business associate after a breach to determine:

(1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
(2) The unauthorized person who used to PHI or to whom the disclosure was made;
(3) Whether the PHI was actually acquired or viewed; and
(4) The extent to which the risk to the PHI has been mitigated.

If, as a result of the risk assessment, the covered entity or business associate cannot demonstrate that there is a low probability of compromise of the PHI, it must begin to follow the breach notification process by notifying the affected individuals, the Secretary of HHS, and, when necessary, the media in accordance with the HIPAA Privacy Rules. The covered entity or business associate must document the results of the risk assessment and retain the documentation for six (6) years.

Unsecured PHI: PHI in electronic or paper form that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by MDHHS guidance.

Purpose

The purpose of the policy is to maintain compliance with HIPAA Privacy Rules and notification guidelines in the case of a breach of unsecured protected health information.

Policy

The NMRE shall maintain the confidentiality, security and integrity of member information that is used in connection with the performance of its contract with MDHHS to the extent and under the conditions specified in HIPAA, the Michigan Mental Health Code (PA 258 of 1974, as amended), the Michigan Public Health Code (PA 368 of 1978 as amended), and 42 C.F.R. Part 2.

References

1. 42 CFR § 438.224 Confidentiality
2. 45 CFR § 164 .404 Notification to Individuals
3. MDHHS Contract
4. American Recovery and Reinvestment Act (ARRA) Title XIII Section 13402, "Notification in the Case of Breach"
5. Federal Trade Commission (FTC) Breach Notification Rules – 16 CFR Part 318
6. Public Act 258 of 1974, "Michigan Mental Health Code," as amended
7. Public Law 115-5, "Health Information Technology for Economic and Clinical Health (HITECH) Act"
8. NMRE Regulatory Compliance Plan

Approval Signature

NMRE Chief Executive Officer

3/2/20

Date

SUBJECT Breach Notification	ACCOUNTABILITY NMRE, NMRE Network Providers	Effective Date: March 2, 2020	Pages: 4
REQUIRED BY	BBA Section: PIHP Contract Section: 17.0-18.1.7 Other: 42 CFR 438.224 45 CFR 164.404	Last Review Date:	Past Review Date:
Policy ☐ Procedure ☒	Review Cycle: Annual Author: NMRE Compliance Coordinator	Responsible Department: Compliance	Reviewers:

Procedure

A. Discovery of a Breach

A breach is determined to be "discovered" the day on which NMRE is made aware that a breach has occurred, or by exercising reasonable diligence, would have been known to occur.

At the time NMRE staff discovers that a breach has occurred, or suspects that a breach might have occurred, he/she will immediately notify the NMRE Compliance Officer, who acts as the NMRE Privacy and the NMRE CIO, who acts as the NMRE Security Officer.

If a breach of unsecured protected health information occurs at or by a Network Provider, Network Provider staff will notify the NMRE following the discovery of the breach.

B. Breach Investigation

For breach response and notification purposes, a breach is presumed to have occurred unless the NMRE or its Network Providers can demonstrate that there is a low probability that the PHI has been compromised based on, at minimum, the following risk factors:

1. Whether the nature and extent of the PHI involved includes the following types of identifiers:
   a. Social security numbers, credit card numbers, financial data;
   b. Clinical detail, diagnosis, treatment, medications;
   c. Mental health, substance use, sexually transmitted disease, pregnancy information.
2. Whether the unauthorized person who used the PHI or to whom the disclosure was made:
   a. Has an obligation to protect the privacy and security of the PHI;
   b. Can re-identify the PHI;
   c. Positively acquired or viewed the PHI.
3. Whether an analysis of a stolen and recovered device shows that PHI on the device was never accessed.
4. Whether the NMRE can obtain the unauthorized person's satisfactory assurances that the PHI will not be further used or disclosed or will be destroyed.

The investigation should consider these factors, or more, in combination to determine the overall probability that PHI has been compromised.

C. Risk Assessment

To determine whether an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals, the HHS Secretary, or the media under breach notification requirements, a risk assessment will be performed. The risk assessment will be thorough and completed in good faith. The NMRE will document the finding of the risk assessment and draw reasonable conclusions; supporting documentation will be fact-specific and address:

1. Consideration of who impermissibly used or to whom the information was impermissibly disclosed;
2. The type and amount of PHI involved;
3. The potential for significant risk of harm to affected individuals (financial, reputational, etc.)

All documentation related to the breach investigation, including the risk assessment, will be retained for a minimum of six (6) years. Based on the outcome of the risk assessment, the NMRE will determine the need to move forward with breach notification.

D. Notification: Affected Individuals

If it is determined that breach notification must be sent to affected individuals, the NMRE's Breach Notification Letter will be sent. The NMRE may notify affected individual following an impermissible acquisition, access, use or disclosure of PHI without performing a risk assessment at its discretion. Notice to affected individuals will be written in plain language and must contain the following information (included in the NMRE's Breach Notification Letter template):

1. A brief description of what happened, including the date of the breach and the date of the discovery of breach, if known;
2. A description of the type of unsecured PHI involved in the breach (social security numbers, dates of birth, addresses, bank account or credit card numbers, diagnoses, disability codes, etc.);
3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
4. A brief description of what the NMRE and/or its Network Providers are doing to investigate the breach, mitigate harm to individuals, and protect against further breaches;
5. Contact information to enable affected individuals to contact the NMRE including a toll-free telephone number, email address, website, and mailing address.

The notice will be sent by first-class mail to affected individuals at their last known addresses. Notifications may be provided in more than one mailing, as information is made available. If NMRE has determined that any affected individuals are deceased and has the addresses of their next of kin or personal representatives, notification will be sent to the next of kin or personal representative.

If there is insufficient or outdated contact information that precludes direct written or electronic notification, a substitute form of notice reasonably believed to reach the individual will be sent. If there is insufficient or outdated contact information for fewer than 10 individuals, the substitute notice may be provided by an alternative form of written notice, by telephone, or by other means. If there is insufficient or outdated contact information for more than 10 individuals, the substitute notice will be in the form of either a conspicuous posting for a period of 90 days on the homepage of the nmre.org website, or a conspicuous notice in major print or broadcast media in the NMRE geographic area where affected individuals are likely to reside. The notice will include a toll-free telephone number that individuals can access to learn whether their PHI was included in the breach that will remain active for at least 90 days.

Notice to affected individuals will be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. If the NMRE determines that notification requires urgency because of imminent misuse of unsecure PHI, notification will be provided by telephone or other means, as appropriate. It is the responsibility of the NMRE to demonstrate that all notifications were administered as required, including evidence demonstrating the necessity of any delay.

E. Notification: HHS Secretary

In the even a breach of unsecured PHI affects 500 or more individuals, the HHS Secretary will be notified at the same time notice is made to the affected individuals, in the matter specified by the Office of the Secretary. If fewer than 500 individuals are affected, NMRE will maintain a secure log of breaches to be submitted annually to the Secretary of HHS no later than 60 days after the end of each calendar year, in the matter specified by the Office of the Secretary. The submission will include all breaches discovered the preceding calendar year.

F. Notification: Media

In the event a breach affects more than 500 residents of a state, prominent media outlets serving the state and regional area will be notified without reasonable delay and in no case greater than 60 calendar days after the discovery of the breach. The notice will be provided in the form of a press release.

G. Notification: Delay Authorized for Law Enforcement Purposes

If a law enforcement official contacts the NMRE any of its Network Providers with information that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the NMRE will:

1. Delay the notification, notice, or posting for the time period specified by the law enforcement official if the request is made in writing and specifies the timeframe of the delay;
2. Delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the statement, if the request is made orally and documented by NMRE, including the identity of the law enforcement official making the statement.

H. Maintenance of Breach Information

The NMRE will maintain a log of all breaches of unsecure PHI, regardless of the number of individuals affected. The following information will be collected for each breach:

1. A brief description of what happened, including the date of the breach and the date of the discovery of breach, and the number of individuals affected, if known;
2. A description of the type of unsecured PHI involved in the breach (social security numbers, dates of birth, addresses, bank account or credit card numbers, diagnoses, disability codes, etc.);
3. A description of the actions taken by the NMRE regarding notification to affected individuals;
4. Steps taken to mitigate the breach and prevent future occurrences.

I. Staff Training

NMRE and Network Provider staff will be trained with respect to HIPPA Privacy Rules and the identification and reporting of unsecured breaches of PHI as determined by the Chief Executive Officer to ensure compliance with federal regulations and the MDHHS-PIHP Contract. The NMRE will monitor to ensure that Network

J. Complaints

Individuals who wish to make complaints to the NMRE regarding its privacies or procedures, compliance with its privacy policies or procedures, or breach notification processes may contact the Compliance Hotline at 1.866.789.5774.

K. Sanctions

NMRE staff who fails to comply with the NNRE Breach Notification Policy and Procedure will be subject to disciplinary action, up to and including termination of employment.

L. Retaliation/Waiver

NMRE staff will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising his/her rights. Individuals will not be required to waive their privacy rights as a condition or provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

M. Burden of Proof

The NMRE holds the burden of proof for demonstrating that all breach notifications were administered as required by federal regulations, the MHDDS-PIHP contract and the NMRE Breach Notification Policy and Procedure, unless a determination has been made that the use acquisition, access, use, or disclosure of PHI did not constitute a breach.

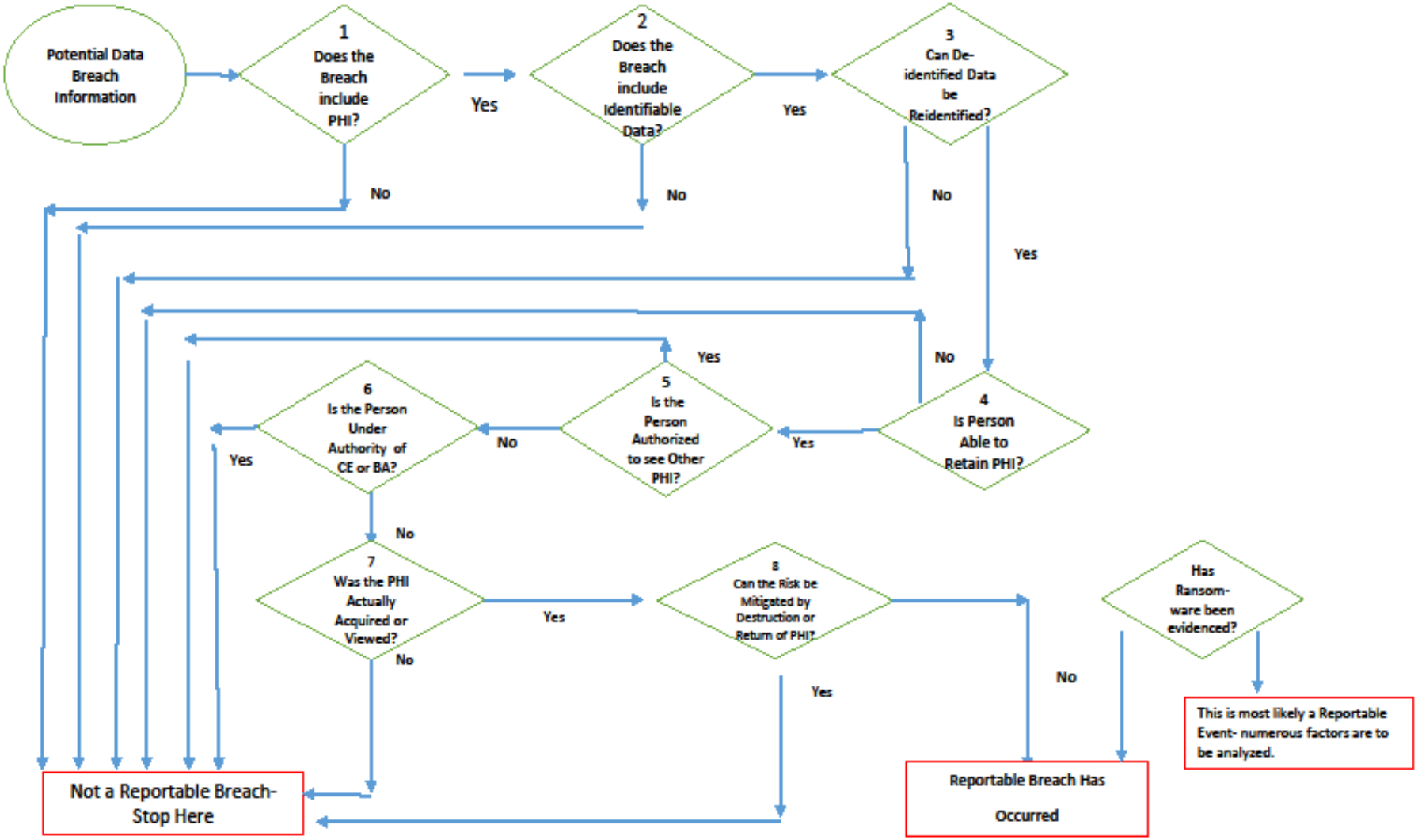
Approval Signature

NMRE Chief Executive Officer

3/2/20

Date

Decision Tree for Assessing a Suspected Breach



Northern Michigan Regional Entity

HIPAA Risk Analysis

The purpose of the HIPAA Breach Risk Analysis process is to determine if a discovered breach of protected health information (PHI) poses a significant risk of financial, reputational, or other harm to the affected individual.

Identifying Information: _____

Breach Report Date: _____ **Breach Reported By:** _____

PHI Incident Date: _____ **Breach Risk Analysis Date:** _____

Number of Individuals Involved in the PHI Breach: _____

Participants Conducting the Breach Risk Analysis: _____

_____

_____

I. Gather Information and report findings within the categories below (attach CQI Report).

1. Specifically state what type or amount of PHI was impermissibly used or disclosed:

2. Who impermissibly used the information or to whom wand the information impermissibly disclosed?

3. Provide substantiation for whether the PHI was actually assessed

4. Fully explain what steps have been taken to mitigate or eliminate the risk of harm.

II. Determine if the alleged breach meets any of the three statutory exemptions to the definition of breach. Include a brief narrative for each item checked below.

Exemption Type #1: ☐ **Yes** ☐ **No**

1. Did the breach involve any unintentional acquisition, access, or use of PHI by a person acting under the authority of a covered entity or business associate?
   ☐ Yes ☐ No
2. Was the acquisition, access, or use made in good faith and within the scope of authority?
   ☐ Yes ☐ No
3. Did it not result in further use or disclosure in a manner not permitted by the HIPAA Privacy Rules?
   ☐ Yes ☐ No

(If "Yes" was checked for all three above, check "Yes" for exemption box #1 above)

Exemption Type #2: ☐ **Yes** ☐ **No**

1. Was the breach an inadvertent disclosure of PHI from a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate, or organized health care arrangement (e.g., integrated care setting) in which the covered entity participates?
   ☐ Yes ☐ No

(If "Yes," check "Yes" for exemption box #2 above)

Exemption Type #3: ☐ **Yes** ☐ **No**

1. Was the disclosure of PHI made by a person within a covered entity or business associate?
   ☐ Yes ☐ No
2. Did the person have a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information?
   ☐ Yes ☐ No

(If "Yes" to both above, then check "Yes" for exemption box #3)

If any of the exemptions have been checked "Yes," no breach notification is required.