



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: March 2, 2026	Past Review Date: November 1, 2025
Policy: <input checked="" type="checkbox"/> Procedure: <input type="checkbox"/>	Review Cycle: Annual Author: NMRE Compliance Coordinator	Responsible Department: Compliance	Reviewers:

Definitions

Beneficiary: A person served by the publicly funded behavioral health and substance use disorder system or their representative (also “consumer” or “member”).

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.

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.”

Community Mental Health Services Program (CMHSP): For the purposes of this document, a CMHSP member is one or more of the following: Centra Wellness Network, North Country Community Mental Health, Northeast Michigan Community Mental Health Authority, and Northern Lakes Community Mental Health Authority, and Wellvance.

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 breach is known to the covered entity, by exercising reasonable diligence, would have been known to the covered entity (including breaches by business associates).

Electronic Health Record (EHR): A digital record of a patient's health record, including but not limited to, medical history, demographics, medications, and diagnoses.

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.

Michigan Department of Health and Human Services (MDHHS): The principal department of the state of Michigan, headquartered in Lansing, which provides public assistance, child and family welfare services, and oversees health policy and management.

Network Provider: Any provider, group of providers, or entity that has a provider agreement with the NMRE or its CMHSPs, and receives Medicaid funding directly or indirectly to order, refer, or render covered services as a result of the NMRE's Specialty Supports and Services Contract with the State.

Prepaid Inpatient Health Plan (PIHP): A term contained in federal regulations from the Centers for Medicare & Medicaid Services. It means an entity that 1) provides medical services to enrollees under contract with the state Medicaid agency based on prepaid capitation payments, 2) includes responsibility for arranging inpatient hospital care, and 3) does not have a comprehensive risk contract.

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: An 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 Protected Health Information (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 this policy is to maintain compliance with the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule and to outline the processes for identifying, reporting, documenting, and notifying affected individuals, the Secretary of Health and Human Services (HHS), and other entities following a breach of unsecured Protected Health Information (PHI).

Policy

The NMRE will maintain the confidentiality, integrity, and security of member information in accordance with HIPAA, the Michigan Mental Health Code, The Michigan Public Health Code, and 42 CFR, Part 2. When a breach of unsecured PIHP occurs, the NMRE and its Network Providers will comply with the notification, documentation, and oversight requirements outlined in this policy and 45 CFR §§164.400-414.

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

March 5, 2026

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: November 1, 2025	Past Review Date:
Policy <input type="checkbox"/>	Review Cycle: Annual	Responsible Department: Compliance	Reviewers:
Procedure <input checked="" type="checkbox"/>	Author: NMRE Compliance Coordinator		

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 without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. The notice will include all elements required under 45 CFR §164.404(c), including a description of the incident, the types of PHI involved, steps individuals may take to protect themselves, a description of what NMRE and/or its Network Providers are doing to investigate and mitigate harm, and contact information for further assistance.

The NMRE and its Network Providers will use the NMRE-approved Breach Notification Letter Template to ensure all required notification content elements are included and that the letter is written in plain language at or below a 6.9 grade reading level.

E. Notification: HHS Secretary

For breaches affecting 500 or more individuals, the NMRE will notify the Secretary of Health and Human Services at the same time individual notifications are made, as specified on the HHS website. For breaches affecting fewer than 500 individuals, the NMRE will maintain a log of such breaches and submit the log annually to the Secretary no later than 60 days after the end of each calendar year.

Each Network Provider will be responsible for submitting required notifications to the Secretary of Health and Human Services for any breaches of unsecured PHI occurring within its organization. The NMRE will require Network Providers to submit confirmation of such notifications, including the date of submission and confirmation number or screenshot, for inclusion in the NMRE's centralized Breach Tracking Log. The NMRE's Compliance Department will review these confirmations annually to verify that all reported breaches have been submitted to HHS as required under 45 CFR §164.408.

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 unsecured 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 its Network Providers will receive training on HIPAA Privacy Rules and the identification and reporting of unsecured breaches of Protected Health Information (PHI). Training will occur upon hire or contract execution and at least annually thereafter. The NMRE Compliance Department will maintain training materials and attendance records and monitor completion to ensure ongoing compliance with federal regulations and the MDHHS–PIHP Contract.

J. Complaints

Individuals who wish to make complaints to the NMRE regarding its policies 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 fail to comply with the NMRE 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 and Policy Review

The NMRE holds the burden of proof for demonstrating that all breach notifications were

administered as required by federal regulations, the MDHHS-PIHP Contract, and this policy, unless a determination has been made that the acquisition, access, use, or disclosure of PHI did not constitute a breach. The NMRE's Compliance Department will review this policy annually to ensure continued alignment with HIPAA breach notification requirements and MDHHS contract provisions, including oversight of Network Providers' reporting and documentation processes.

N. Network Provider Oversight and Reporting

To ensure consistent breach notification practices across the NMRE region, the NMRE will oversee and monitor its Network Providers for compliance with the HIPAA Breach Notification Rule (45 CFR §§164.400-414) and Section 18.1.7 of the MDHHS-PIHP Contract.

1. Reporting Requirement: Each Network Provider must notify the NMRE of any suspected or confirmed breach of unsecured PIH within one (1) business day of discovery (ten [10] days for Business Associates per NMRE's BAA). Reports must be submitted using the NMRE's Breach Report Form and include all known facts regarding the incident.
2. Documentation Submission: Network Providers must submit to the NMRE a completed HIPAA Risk Assessment form, a copy of the Member Notification Letter, and evidence of any required notifications to HHS and/or media, as applicable.
3. Tracking and Verification: The NMRE will maintain a centralized Breach Tracking Log documenting all reported breaches. The log will include the date of discovery, the date the NMRE was notified, the date members were notified, and the date HHS and/or media were notified. The log will indicate whether each report originated from a Network Provider.
4. Oversight Review: The NMRE's Compliance Department will review the Breach Tracking Log on a quarterly basis to verify that each reported breach was properly addressed, documented, and resolved within the required timeframes. Results of these reviews will be maintained as part of the NMRE's compliance oversight records.
5. Corrective Action: Network Providers that fail to report or document breaches in accordance with these requirements may be subject to corrective action consistent with the NMRE's contractual oversight and compliance monitoring processes.

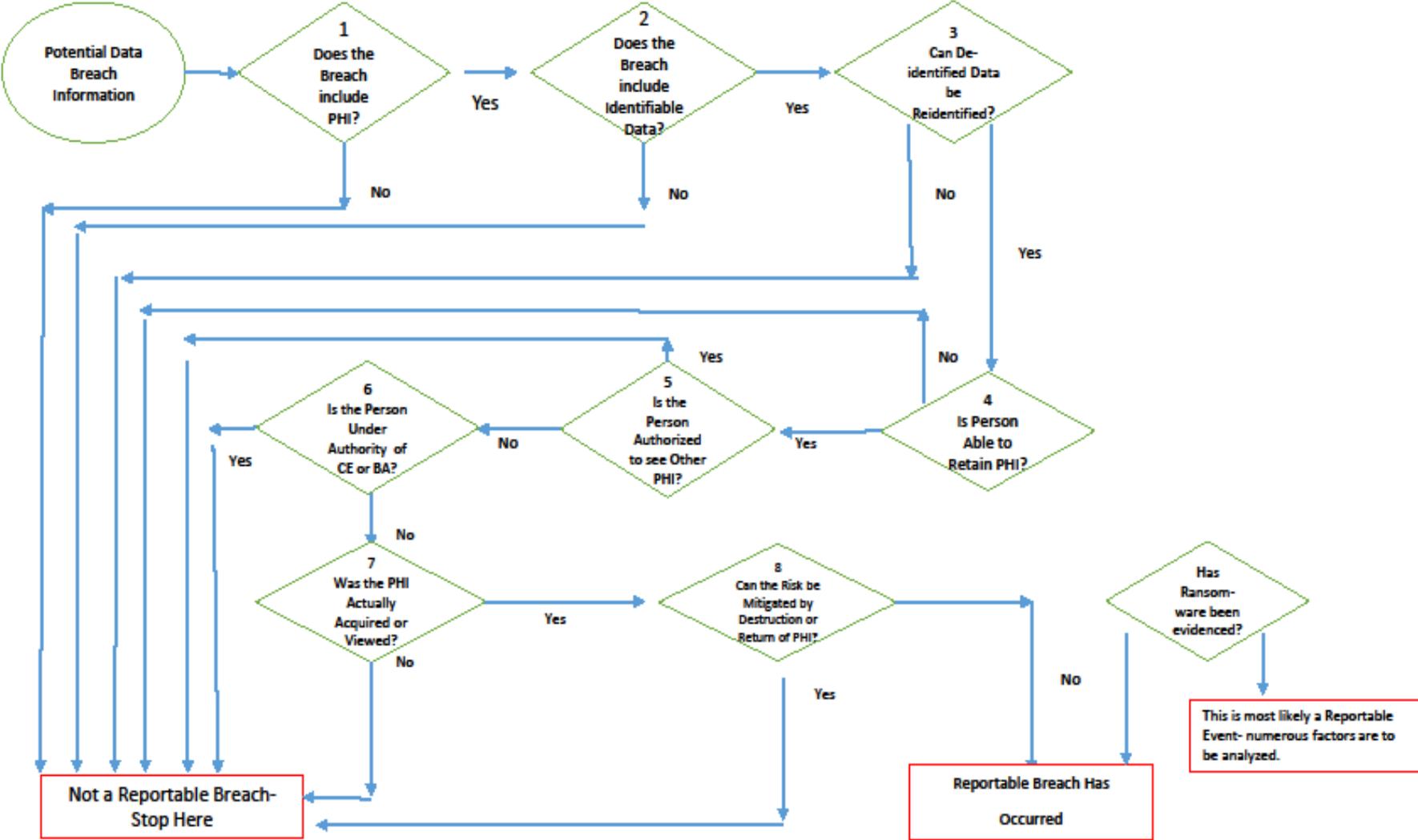
Approval Signature



NMRE Chief Executive Officer

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 was 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.

Northern Michigan Regional Entity
HIPAA Risk Analysis

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.