POLICY AND PROCEDURE MANUAL

SUBJECT Acceptable Use of Artificial Intelligence	ACCOUNTABILITY All Employees, Interns, Contractors, and Volunteers	Effective Date: September 1, 2026	Pages: 3
REQUIRED BY HIPAA | 42 CFR Part 2 | CARF Standards	Managed Care Rules: PIHP Contract Section: Other:	Last Review Date: 5/20/26	Past Review Date:
Policy: ☒ Procedure: ☐	Review Cycle: Annual Author: CIO	Responsible Department: Information Technology & Compliance	Reviewers: NMRE CEO

Definitions

42 CFR Part 2: Federal regulations governing the confidentiality of substance use disorder patient records. These regulations impose restrictions beyond standard HIPAA requirements and apply to records relating to substance use disorder treatment.

AI-Powered Tools: Include but are not limited to: generative AI (e.g., ChatGPT, Microsoft Copilot, Google Gemini), predictive analytics platforms, Natural Language Processing (NLP) systems, and any software using machine learning to generate, analyze, or process text, audio, or video.

Approved AI Tools: AI platforms reviewed and authorized by NMRE's IT and Compliance departments for specific, defined use cases.

Artificial intelligence (AI): A branch of computer science focused on building systems capable of performing tasks that typically require human intelligence. This includes learning from data, recognizing patterns, understanding language, solving problems, and making decisions.

Commission on Accreditation of Rehabilitation Facilities (CARF): An independent, non-profit organization that evaluates and accredits health and human service providers globally. A CARF accreditation signifies that a facility meets rigorous, internationally recognized standards of quality, safety, and personalized care.

De-identified Data: Health information from which all 18 HIPAA-specified identifiers have been removed, such that the remaining information cannot reasonably be used to identify an individual.

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

Individually Identifiable Health Information (IIHI): Information that is a subset of health information, including demographic information collected from an individual, and:

1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse, and
2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual, or the past present or future payment for the provision of health care to an individual; and
   a) That identifies the individual; or
   b) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

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.

Northern Michigan Regional Entity (NMRE): Region 2 PIHP covering Alcona, Alpena, Antrim, Benzie, Charlevoix, Cheboygan, Crawford, Emmet, Grand Traverse, Iosco, Kalkaska, Leelanau, Manistee, Missaukee, Montmorency, Ogemaw, Oscoda, Otsego, Presque Isle Roscommon, and Wexford counties in northern Lower Michigan.

Northern Michigan Regional Entity (NMRE) Internal Operations Committee: A committee comprised of key, senior NMRE staff and/or heads of departments.

Prepaid Inpatient Health Plan (PIHP): A regional organization that manages publicly funded Medicaid specialty mental health, intellectual/developmental disability, and substance use disorder (SUD) services within a designated geographic area under contract with the state

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity—such as name, social security number, biometric data records—either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

Protected Heath Information (PHI): Individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 USC. 1232g; (ii) Records described at 20 USC. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer.

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

Applicability

This policy applies to all employees, interns, contractors, and volunteers who access or use AI-powered tools and platforms in the course of their work at NMRE, regardless of whether the work is performed

on-site or remotely, and regardless of whether personal or agency-owned devices are used. This policy further applies to all data, files, etc. in the NMRE's system or any data that NMRE shares with partner organizations.

Purpose

The purpose of this policy is to establish clear guidelines for the safe, ethical, and responsible use of Artificial Intelligence (AI) tools by staff of Northern Michigan Regional Entity (NMRE). This policy ensures alignment with HIPAA, 42 CFR Part 2, CARF standards, and the agency's core values of client dignity, privacy, and service quality.

Policy

Northern Michigan Regional Entity (NMRE) is committed to the responsible, ethical, and secure use of Artificial Intelligence (AI) technologies in support of its mission and operations. AI tools may be utilized only in accordance with applicable federal and state laws, including HIPAA and 42 CFR Part 2, and only for approved business purposes that protect the confidentiality, privacy, and dignity of the individuals served. The use of AI must not compromise clinical judgment, regulatory compliance, information security, or the integrity of agency operations. All workforce members are expected to use approved AI technologies responsibly and in accordance with NMRE policies and procedures.

Approval Signature

NMRE Chief Executive Officer

August 20, 2026

Date

SUBJECT Acceptable Use of Artificial Intelligence	ACCOUNTABILITY All Employees, Interns, Contractors, and Volunteers	Effective Date:	Pages: 4
REQUIRED BY HIPAA | 42 CFR Part 2 | CARF Standards	Managed Care Rules: PIHP Contract Section: Other:	Last Review Date: 5/20/26	Past Review Date:
Policy: ☐ Procedure: ☒	Review Cycle: Annual Author:	Responsible Department: Information Technology & Compliance	Reviewers: NMRE CEO

Procedure

A. Approved AI Tools

NMRE has authorized the use of the following AI platform(s) for agency-related work:

Currently Approved AI Tool(s)
Microsoft Copilot — integrated within the Microsoft 365 suite, accessed through organizational accounts only.
Microsoft Teams Premium and Auto-Transcription – activates when joining meetings automatically and only displays real-time conversation without retaining after meeting end. Premium license allows chat and audio transcription and summarization.
All AI integrated into internet searches - must remain limited to search. Subsequent interactions that take users into an AI chat style environment are not considered compliant for work purposes.
Canva AI tools — used in the Canva software to generate forms, slides, pamphlets, etc. (for details on acquiring a license, reach out to the IT department)

Use of any other AI tool — including but not limited to ChatGPT, Google Gemini, Meta AI, or Perplexity— is strictly prohibited.

B. Requesting Usage of Additional AI Tools

Requests to evaluate additional AI tools must be submitted to the Chief Information Officer or Compliance Officer for security, privacy, and compliance review before any use occurs. Approval of requests will be handled by the NMRE Internal Operations Committee.

C. Acceptable Uses of AI

Staff may use approved AI tools for the following purposes, provided no IIHI, PII, or confidential agency data is entered:

- Drafting non-client-specific emails, memos, reports, or training materials
- Summarizing policies or documentation (using de-identified or non-client text only)
- Generating ideas for internal projects or communications
- Translating technical information for broader understanding
- Assisting with internal data analysis using anonymized datasets

- Creating general administrative templates or workflow documentation

When in doubt regarding whether a specific use is permissible, staff must consult with the Chief Information Officer or Compliance Officer before proceeding.

D. Prohibited Uses of AI

The following uses of AI are strictly prohibited when using any approved AI tool:

Prohibited —Confidential Data
Entering IIHI or PII into any AI tool (including names, diagnoses, addresses, visit notes, dates of birth, insurance information, etc.)
Uploading internal documents containing sensitive, confidential, or client-related data to any AI tool
Inputting a document that contains IIHI or PII into an AI service to de-identify the data therein is prohibited as AI services keep their own copy of whatever is submitted to them.
Using any AI tool to transcribe or otherwise record any digital meeting over Zoom, Teams, or similar platforms, except where automatic transcription is enabled through Microsoft Teams in accordance with Subsection E of the NMRE Acceptable Use of AI Policy and Procedure. Should any external users join an NMRE meeting with an AI transcription tool enabled outside of approved platforms, they must be asked to disable it for the duration of the meeting. Meeting minutes will be provided upon request if not generally made available.
Any usage of AI to replicate into new audio or video the sound, appearance, credentials, or any other personal or identifying information of NMRE staff member(s), clinical patient(s), contracted provider(s), and their associated organizational branding is prohibited.

Prohibited — Clinical Use
Using AI tools to document, summarize, or generate clinical session notes or assessments
Using AI to make, inform, support, or influence any clinical decision, care determination, risk assessment, or treatment recommendation
Using AI-generated content as a basis for any clinical or diagnostic judgment

Prohibited — Regulatory Compliance
Using non-approved AI platforms for any agency-related work or decision-making
Using AI in any way that may compromise compliance with HIPAA, 42 CFR Part 2, CARF standards, or other applicable regulatory requirements
Sharing AI-generated content externally without appropriate review and approval

E. Automatic Transcription

Meeting Transcription/Recording using AI-powered transcription tools, bots, or services is prohibited unless those tools are approved in the NMRE Acceptable Use of AI Policy and Procedure. If attendees bring their own tools to a meeting, those tools should be removed before the meeting continues.

F. Data Privacy & Security Procedures

- All AI tools used for agency work must comply with all NMRE's data security policies.
- Only AI tools approved by the NMRE Internal Operations Committee may be used for agency-related activities.
- Staff must not use personal AI accounts or consumer-facing AI services for any work-related task.
- If staff are unsure about the appropriateness of a tool or a specific use, they must consult the Chief Information Officer or Compliance Officer before proceeding.
- Staff must complete annual training on safe AI use as a condition of continued access to approved AI tools.

Any actual or suspected unauthorized disclosure of IIHI or PII— including accidental submission to an AI tool — must be reported immediately to the HIPAA Privacy Officer and HIPAA Security Officer. The organization is legally required to investigate all potential HIPAA and 42 CFR Part 2 breaches and to notify affected individuals and the Michigan Department of Health and Human Services as required.

G. Oversight & Reporting

- All AI-related activity on NMRE systems and accounts is subject to monitoring and audit.
- Any suspected misuse of AI tools must be reported to a supervisor, the Chief Information Officer or the Compliance Officer immediately.
- Violations of this policy may result in referral to HR where disciplinary action may occur, up to and including termination of employment, and may result in further referral to regulatory or law enforcement authorities where applicable.
- The IT Department will conduct periodic reviews of AI tool usage to assess compliance with this policy.

H. Exceptions

No exceptions to the confidential data prohibition (Subsection D of the NMRE Acceptable Use of AI Policy and Procedure) or the clinical use prohibition (Subsection D of the NMRE Acceptable Use of AI Policy and Procedure) will be granted under any circumstances.

Any request for an exception to other provisions of this policy must be:

- Submitted in writing to the Chief Information Officer and Compliance Officer
- Reviewed and approved by both the Chief Information Officer and Compliance Officer
- Documented in writing prior to implementation
- Retained on file by the Compliance department

Review

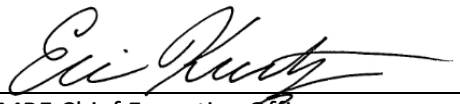
This policy and procedure will be reviewed annually and updated as needed to reflect changes in technology, regulatory requirements, and organizational practices. Workforce members will be notified

of any material updates. Continued use of AI tools following notification of an update constitutes acceptance of the revised policy.
Questions regarding this policy should be directed to the Chief Information Officer or Compliance Officer.

References

- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- HIPAA Privacy Rule — 45 CFR Part 164, Subpart E
- HIPAA Security Rule — 45 CFR Part 164, Subpart C
- HIPAA Breach Notification Rule — 45 CFR Part 164, Subpart D
- 42 CFR Part 2 — Confidentiality of Substance Use Disorder Patient Records
- CARF Standards (applicable accreditation standards)
- HITECH Act of 2009
- NMRE Information Security Policy
- NMRE Acceptable Use Policy
- NMRE HIPAA Privacy and Security Policies

Approval Signature



NMRE Chief Executive Officer

August 20, 2026

Date