



MNSHINE HEALTH INFORMATION EXCHANGE

HIE Services Policies & Procedures Manual

Minnesota Statewide Health Information Network and Exchange
(MNSHINE)

November 2026 Edition · Approved · Effective November 1, 2026

Policy Owners	MNSHINE HIE Advisory Committee
Approval Authority	MNSHINE Board of Directors
Contents	14 policies and 2 forms (55 pages)
Applies To	MNSHINE health information exchange services and its responsibilities as a Minnesota-certified HIO, including the HIE business line acquired from Koble

Printed copies are uncontrolled. Confirm that each policy is the current approved version before use.

HIE SERVICES POLICIES & PROCEDURES MANUAL

Table of Contents

Charter first, then policies by number, then forms. Each document begins on the manual page shown; front matter is numbered i–ii. Page ranges reflect the approved versions effective November 1, 2026.

Number	Title	Category	Version	Manual Pages
GOVERNANCE				
HIE-POL-016	HIE Advisory Committee Charter	Committee Charters	1.0	1–5
POLICIES				
HIE-POL-001	Access Control Policy	Information Security	2.0	6–10
HIE-POL-002	Amendment of Data	Information Privacy	2.0	11–12
HIE-POL-004	Complaint Policy	Information Security	2.0	13–15
HIE-POL-005	Definitions	Information Management	2.0	16–20
HIE-POL-006	Data Encryption	Information Security	2.0	21–22
HIE-POL-007	Enforcement	Information Security	2.0	23–25
HIE-POL-008	Information System Audits	Information Security	2.0	26–27
HIE-POL-009	Malicious Software & Virus Protection	Information Security	2.0	28–29
HIE-POL-010	Privacy and Data Practices	Information Privacy	2.0	30–31
HIE-POL-011	Use and Disclosure of Health Information	Information Privacy	2.0	32–35
HIE-POL-012	Security Incident Management	Information Security	2.0	36–40
HIE-POL-013	Security Safeguards	Information Security	2.0	41–42
HIE-POL-014	Breach Management & Notification Policy	Information Security	2.0	43–49
FORMS				
HIE-FRM-001	HIE Complaint Form	Forms	1.0	50–53
HIE-FRM-002	HIE Opt-Out / Opt Back In Form	Forms	1.0	54–55

Retired, reserved, and withdrawn numbers (not reused): HIE-POL-003 reserved (legacy Koble-MN ID; no policy converted); HIE-POL-015 retired (GLB-POL-005 applies); HIE-REF-001 withdrawn (replaced by GLB-REF-001). See GLB-REF-001 for details.

MNSHINE HEALTH INFORMATION EXCHANGE • POLICIES & PROCEDURES

HIE Advisory Committee Charter

Policy Number	HIE-POL-016	Version	1.0
Policy Category	Committee Charters	Status	Active
Policy Owner	MNSHINE HIE Advisory Committee	Approval Authority	MNSHINE Board of Directors
Original Effective Date	10/19/2026	Version Effective Date	11/1/2026
Next Review Due	10/31/2027	Legacy Reference	None (Koble-MN Advisory Committee charter not adopted; Resolution §7)

1. NAME AND AUTHORITY

1. The name of this committee is the HIE Advisory Committee (the “Committee”) of Minnesota Statewide Health Information Network and Exchange, formerly known as MN Community Measurement (“MNSHINE”).
2. The Committee is a standing committee of the MNSHINE Board of Directors (the “Board”), established pursuant to Article VII, Section 1 of MNSHINE's Bylaws (the “Bylaws”) by resolution of the Board.
3. Until the effective date of the change of its legal name from “MN Community Measurement” to “Minnesota Statewide Health Information Network and Exchange,” references in this Charter to MNSHINE refer to the corporation under its then-current legal name.

2. PURPOSE

1. The Committee is charged with reviewing and making recommendations to the Board regarding the operation of MNSHINE's health information exchange business (the “HIE Business”) and MNSHINE's responsibilities as a Minnesota-certified Health Information Organization (“HIO”) under Minnesota Statutes, Section 62J.4981, including matters relating to:
 - Implementation of a statewide interoperable health information infrastructure consistent with emerging national standards;
 - Interoperability of health information systems in furtherance of health care quality, patient safety, and efficiency of health care and public health services in Minnesota;
 - Participating entity relationships, onboarding, and satisfaction;
 - Privacy, security, and data governance practices applicable to the HIE Business; and
 - Health equity considerations in the design and delivery of HIE services.

2. The Committee's role is advisory. The Committee shall make recommendations to the Board; final decision-making authority, including the enactment of MNSHINE policy, rests exclusively with the Board.

3. RELATIONSHIP TO THE BOARD

1. The Committee operates under the authority of, and is at all times subject to the control and direction of, the Board, consistent with Article VII, Section 1 of the Bylaws.
2. The Committee shall report its recommendations to the Board in writing. The Board will consider and respond to Committee recommendations within a reasonable time.
3. Nothing in this Charter shall be construed to delegate to the Committee any authority to bind MNSHINE or to make final decisions on behalf of MNSHINE.

4. STATUTORY COMPLIANCE

1. The composition of the Committee is intended to satisfy Minnesota Statutes, Section 62J.4981, subdivision 3(c)(5), which requires that a certified HIO's governance structure include representation of a cross-section of the health care community, with emphasis on organizations using the HIO's information exchange services, and consumers.
2. Membership shall include representation of minority and other target populations with an interest in health information exchange, consistent with the statutory purpose described above.

5. MEMBERSHIP

5.1 Composition

1. The Committee shall consist of up to fifteen (15) members, appointed by the Chairperson of the Board (the "Board Chair"). This number may be adjusted from time to time by resolution of the Board.
2. Members need not be directors of MNSHINE, consistent with Article VII, Section 1 of the Bylaws.
3. The Board shall endeavor to maintain representation from the following categories, consistent with the Committee's historical composition and Minnesota Statutes, Section 62J.4981, subdivision 3(c)(5):
 - Consumer representative
 - Electronic health record vendor
 - Behavioral health
 - Public health
 - Long-term care
 - Integrated delivery network (interstate, national, underserved population, and/or urban center)

- Critical access hospital
- Insurance payer
- Minnesota Hospital Association or other statewide health care association

5.2 Appointment and Terms

1. The initial members of the Committee are appointed by the Board in the resolution establishing the Committee. Thereafter, members are appointed by the Board Chair upon the recommendation of the Committee Chair.
2. Members serve terms of three (3) years, with approximately one-third of the membership's terms expiring each year to preserve continuity. The initial terms of members are designated as provided in the resolution establishing the Committee, and each membership year begins on January 1. A member's term is not renewable within eleven (11) months following the conclusion of an earlier term, except as the Board may otherwise determine.
3. A vacancy occurring during a term shall be filled by the Board Chair, upon the recommendation of the Committee Chair, for the remainder of the unexpired term.
4. A member who is absent without reasonable cause from three consecutive Committee meetings shall be deemed to have resigned, and the resulting vacancy shall be filled as provided in this Section 5.2.
5. A member may be removed by the Board, with or without cause.

6. CONFLICTS OF INTEREST

1. Each Committee member is subject to MNSHINE's Conflict of Interest Policy (the "COI Policy"), as it may be amended from time to time, consistent with Article V, Section 9 of the Bylaws.
2. Each Committee member shall execute MNSHINE's Director, Committee Member, Officer, and Key Employee Conflict of Interest Statement upon appointment and annually thereafter.
3. A Committee member with a material financial or other interest in a matter before the Committee shall disclose that interest and shall withdraw from discussion and any recommendation-related vote on that matter, consistent with the COI Policy.

7. OFFICERS

1. The Committee's initial Chair is appointed by the Board in the resolution establishing the Committee. Thereafter, the Committee's Chair is appointed by the Board Chair from among the directors of MNSHINE, consistent with Article VII, Section 3 of the Bylaws (Executive Committee composition).
2. The Committee's Vice Chair and Recording Secretary are elected by the Committee's membership for one-year terms at the first meeting of each membership year.

8. MEETINGS

1. The Committee shall meet at least four (4) times per year either in person or by remote means, or as otherwise called by the Chair.
2. Meeting dates shall be established at least one year in advance where practicable. Written notice of each meeting shall be provided to members at least ten (10) days in advance, and meeting materials shall be distributed at least two (2) days in advance.
3. Meetings shall otherwise be governed by the procedures set forth in Article V of the Bylaws, as applied to committees under Article VII, Section 2.
4. Minutes of each meeting shall be kept and provided to the Board and Committee membership within two (2) weeks following the meeting.

9. REPORTING AND RECOMMENDATIONS

1. Committee recommendations shall be submitted to the Board in writing, including: (a) the recommended action; (b) the justification for the recommendation; and (c) any supporting materials or citations.
2. The Board shall endeavor to respond in writing to Committee recommendations within a reasonable time, and in no event later than two (2) Board meetings following receipt.
3. At least annually, the Committee shall provide the Board with a report on its activities, including participating entity engagement, and shall recommend any changes to this Charter.

10. AMENDMENT

1. This Charter may be amended only by resolution of the Board. The Committee may recommend amendments to the Board for consideration.

Adopted by the Board of Directors of MN Community Measurement (to be renamed Minnesota Statewide Health Information Network and Exchange) as Exhibit A to the resolution establishing the HIE Advisory Committee on October 12, 2026.

Revision History

Version	Date	Description of Revision	Author	Approved By	Approval Date
1.0	10/12/2026	Charter adopted by the Board as Exhibit A to the resolution establishing the HIE Advisory Committee, effective as of the Closing (Committee Effective Date). Formatted in the MNSHINE HIE policy template and assigned HIE-POL-016 on 10/26/2026, with no change to the adopted text.	—	MNCM Board of Directors	10/12/2026

The establishing resolution (Section 3) directs that this Charter be reviewed by the Committee and re-approved by the Board no less frequently than annually. Section 10 provides that it may be amended only by resolution of the Board.

MNSHINE HEALTH INFORMATION EXCHANGE • POLICIES & PROCEDURES

Access Control Policy

Policy Number	HIE-POL-001	Version	2.0
Policy Category	Information Security	Status	Active – Legacy Policy
Policy Owner	MNSHINE HIE Advisory Committee	Approval Authority	MNSHINE Board of Directors
Original Effective Date	2/26/2016	Version Effective Date	11/1/2026
Next Review Due	1/31/2027	Legacy Reference	Koble-MN Policy Ref. ID 001

PURPOSE

To protect an Individual's health information from unauthorized use, the MNSHINE HIO shall verify the identity of Participants and their Authorized Users before access to MNSHINE HIO is granted. Health information available through MNSHINE HIO shall be accessed only by Authorized Users who have been granted access rights.

SCOPE

This policy applies to all MNSHINE HIO participants and workforce; participants, employees / users, temporary staff, contracted staff, and credentialed provider staff.

AUTHENTICATION

Authentication is the process of verifying that an Authorized User who is seeking to access information through the MNSHINE HIO is the individual who the Authorized User claims to be.

PARTICIPANT AUTHENTICATION

The MNSHINE CEO, or designee, and each Participant shall execute a written and signed MNSHINE HIO Participation Agreement prior to MNSHINE HIO Portal access.

The MNSHINE HIO shall review, evaluate and act upon requests submitted by organizations that want to become a MNSHINE HIO Participant.

- Each MNSHINE HIO Participant must demonstrate that it is a legitimate business by completing an application and provide the requested information. The MNSHINE HIO participant must assure that its agents and workforce access ePHI for only valid business reasons and that it participates in the types of health care transactions required of a Covered Entity or its Business Associate.

- The MNSHINE CEO, or designee, in collaboration with the MNSHINE HIO participant shall determine whether the entities meet technical and operational requirements and complete the readiness assessment.
- MNSHINE HIO Participant identity shall be authenticated and unique user names and passwords shall be assigned by MNSHINE HIO to Authorized Users identified by Participant.
- Each MNSHINE HIO Participant shall designate its responsible contact person (e.g., department manager) who shall be responsible on behalf of the Participant for compliance with MNSHINE HIO policies and to receive notice on behalf of the Participant. Access rights shall be properly authorized and documented by the participant contact and access rights will be periodically audited to ensure compliance.
- MNSHINE HIO Participants shall, within five (5) working days, notify MNSHINE HIO if there is a material change in status such as a change in ownership or change in authorized user job assignments. If the Participant ceases to engage in health care transactions, it shall notify MNSHINE HIO at least 30 days before the change.
- Participants shall notify MNSHINE HIO within twenty-four hours, of termination of an Authorized User's employment or affiliation with the Participant.
- Only information technology staff at MNSHINE HIO or system administrators are permitted to create or change access control settings.

AUTHORIZED USERS

MNSHINE HIO Participants shall designate the Authorized Users within their organizations who will be authorized to access information through the MNSHINE HIO. Participants shall develop and implement policies to assure proper identification of each Authorized User.

- Authorized Users shall be required to execute a user agreement prior to MNSHINE HIO portal access.
- Authorized Users must maintain a current relationship with a Participant to access the MNSHINE HIO.

Access to health information shall be based on the Authorized User's job function and relationship to the patient. Categories of Authorized Users shall be established, at a minimum, as the following:

1. Practitioner with access to clinical data and "Break the Glass" authority.
2. Practitioner with access to clinical data but no "Break the Glass" authority.
3. Non-practitioner with access to clinical information.
4. Non-practitioner with access to non-clinical information.

MNSHINE HIO Administrative Authorized Users shall be based on the job functions. Categories of MNSHINE HIO Administrative Authorized Users shall be established, at a minimum, as the following:

1. Administrative Authorized User with access to non-clinical information.
2. Administrative Authorized User with access to clinical information to resolve technical issues or input advance directives received from third parties.

3. Administrative Authorized user with access to clinical information for audit purposes.

PASSWORDS

Each Authorized User shall be assigned a unique username and an initial password that is required to be changed at the next use of MNSHINE HIO portal.

Passwords shall meet the strong password guidelines set forth in this MNSHINE HIO Access Control Policy.

1. Authorized Users shall be required to change their passwords at least every 90 calendar days and shall be prohibited from reusing the last 5 passwords.
2. Password must be a minimum of eight characters and contain a combination of upper case letters, lower case letters, and special characters.
3. Password should not be a word found in the dictionary (English or foreign).
4. The password should not be a name, initials, birthdays or phone number associated with authorized user.

Authorized Users are prohibited from sharing their user names and passwords with others; and from using the user names and passwords of others.

MNSHINE HIO shall encrypt user authentication data stored in the Network.

FAILED ACCESS ATTEMPTS

The MNSHINE HIO shall enforce a limit of consecutive failed access attempts by an Authorized User. Upon the 5th failed attempt, MNSHINE HIO shall disable the Authorized User's access to the MNSHINE HIO. The Authorized User may reestablish access using appropriate identification and authentication procedures established by the Participant.

PERIODS OF INACTIVITY

The MNSHINE HIO will have an automatic log-off and will terminate an electronic session after 30 minutes of inactivity. A Participant may establish a shorter automatic log-off and termination period for an electronic session on its network or for any device or class of devices used by its Authorized Users to access the Participant's network.

TRAINING

Participants shall provide training for all of its Authorized Users consistent with the Participant's and MNSHINE HIO policies including privacy and security requirements.

PARTICIPANT POLICIES/REMOTE ACCESS

Each MNSHINE HIO Participant shall establish and enforce policies and procedures regarding Authorized User access to Patient Data (including Remote Access), the conditions that must be met and documentation that must be obtained prior to allowing an Authorized User access to Patient Data.

Policies shall include procedures for taking disciplinary actions for its Authorized Users or members of its workforce in the event of a breach or non-compliance with the policies.

The MNSHINE HIO Participant may suspend, limit, or revoke the access authority of an Authorized User on its own initiative upon a determination that the Authorized User has not complied with the Participant's policies or the MNSHINE HIO policies. The MNSHINE HIO Participant shall inform the MNSHINE office immediately, and in any case within twenty-four hours, of any revocation or suspension.

MNSHINE AUTHENTICATION

MNSHINE HIO shall authenticate users accessing the MNSHINE HIO with each attempt the user accesses the Network.

References: 45 C.F.R. §164.308 (3) (i), 45 C.F.R. §164.308 (3) (i), 45 C.F.R. §164.312(d), 45 C.F.R. §164.312(a) (1-2).

Revision History

Version	Date	Description of Revision	Author	Approved By	Approval Date
1.0	2/26/2016	Original policy effective date (Koble-MN).	—	—	—
1.1	7/26/2016	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	Koble-MN Advisory Group	7/28/2016
1.2	8/26/2022	Full review of policy	—	Koble-MN Exec Committee	8/26/2022
2.0	10/26/2026	Converted to the MNSHINE HIE Services policy template and numbering system; assigned HIE-POL-001 (formerly Koble-MN Ref. ID 001); organizational references updated from Koble to MNSHINE; policy owner changed to the MNSHINE HIE Advisory Committee.	—	Koble-MN Exec Committee	10/12/2026

Versions 1.x were issued by Koble-MN, the former owner of the HIE business line acquired by MNSHINE, and are numbered retroactively for continuity. Approving bodies and dates for those versions are shown as originally recorded.

MNSHINE HEALTH INFORMATION EXCHANGE • POLICIES & PROCEDURES

Amendment of Data

Policy Number	HIE-POL-002	Version	2.0
Policy Category	Information Privacy	Status	Active – Legacy Policy
Policy Owner	MNSHINE HIE Advisory Committee	Approval Authority	MNSHINE Board of Directors
Original Effective Date	2/26/2016	Version Effective Date	11/1/2026
Next Review Due	1/31/2027	Legacy Reference	Koble-MN Policy Ref. ID 002

PURPOSE

To ensure that individuals maintain the right to request an amendment of their protected health information.

SCOPE

This policy applies to all MNSHINE HIO participants and workforce; participants, employees /authorized users, temporary staff, contracted staff, and credentialed provider staff.

ACCEPTING REQUESTS FOR AMENDMENTS

If an Individual requests an amendment to the individual's Protected Health Information, MNSHINE HIO shall forward the request to the Participant that created the documentation, and inform the individual requesting the amendment that the request was transferred to that Participant.

Each Participant shall comply with applicable federal, state and local laws and regulations regarding individual rights to request amendment of health information.

INFORMING OTHER PARTICIPANTS

If the Participant that created the information accepts the requested amendment, in whole or in part, the Participant as required by 45 C.F.R. 164.526(c) must make reasonable efforts to inform and provide the amendment within a reasonable time to: (i) persons identified by the individual as having received Protected Health Information about the individual and needing the amendment; and (ii) persons, including business associates, that the Participant knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on that information to the detriment of the individual.

APPLICATION TO BUSINESS ASSOCIATES AND CONTRACTORS

Participants shall make this policy applicable to their Business Associates (“BA”) and to the contractors and subcontractors of their BAs as required by the HIPAA Rules.

Revision History

Version	Date	Description of Revision	Author	Approved By	Approval Date
1.0	2/26/2016	Original policy effective date (Koble-MN).	—	—	—
1.1	7/28/2016	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	Koble-MN Advisory Committee	7/28/2016
1.2	8/26/2022	Full review of Policy	—	Koble-MN Exec Committee	8/26/2022
2.0	10/26/2026	Converted to the MNSHINE HIE Services policy template and numbering system; assigned HIE-POL-002 (formerly Koble-MN Ref. ID 002); organizational references updated from Koble to MNSHINE; policy owner changed to the MNSHINE HIE Advisory Committee.	—	Koble-MN Exec Committee	10/12/2026

Versions 1.x were issued by Koble-MN, the former owner of the HIE business line acquired by MNSHINE, and are numbered retroactively for continuity. Approving bodies and dates for those versions are shown as originally recorded.

MNSHINE HEALTH INFORMATION EXCHANGE • POLICIES & PROCEDURES

Complaint Policy

Policy Number	HIE-POL-004	Version	2.0
Policy Category	Information Security	Status	Active – Legacy Policy
Policy Owner	MNSHINE HIE Advisory Committee	Approval Authority	MNSHINE Board of Directors
Original Effective Date	2/26/2016	Version Effective Date	11/1/2026
Next Review Due	1/31/2027	Legacy Reference	Koble-MN Policy Ref. ID 004

PURPOSE

The MNSHINE HIO provides a complaint process for any Individual or Participant to register a complaint.

DEFINITIONS

Authorized Users are individuals who have been authorized by a Participant to participate in the HIO and may include, but are not limited to, health care practitioners, employees, contractors, agents, or business associates of a Participant.

Individual means a person who is the subject of Protected Health Information (PHI) and has the same meaning as the term “Individual” in 45 C.F.R. § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

Participant means an organization, health care practitioner or institution, health plan, or health care clearinghouse who has executed a written Participation Agreement and Business Associate Agreement with the MNSHINE HIO.

WHO MAY FILE A COMPLAINT

An Individual, or individual’s personal representative, may file a complaint concerning:

- the impermissible use, disclosure or disposal of Protected Health Information
- denials of access to Individual Protected Health Information
- retaliation against an individual for filing a complaint

A Participant or its Authorized Users, or member of the MNSHINE HIO workforce may file a complaint concerning the following issues:

- violation of policies and procedures
- the impermissible use, disclosure or disposal of Protected Health Information

- retaliation against an individual for filing a complaint

COMPLAINTS RELATING TO A PARTICIPANT OR ITS AUTHORIZED USERS

Each Participant will implement a process for workforce members, agents, contractors and Individuals to report any non-compliance with policies and a process for Individuals whose health information is shared through MNSHINE HIO to file a complaint with the Participant about impermissible disclosures and uses of information about them. This process will include how to address complaints specifically to MNSHINE HIO if applicable.

COMPLAINTS RELATING TO THE MNSHINE HIO

The complaint must be in writing and contain the complainant's name and contact information. No personal health information should be included. Verbal complaints will not be accepted by MNSHINE HIO. Anonymous complaints will not be accepted by MNSHINE HIO. A Complaint Form is available at www.mnshine.org or can be requested by calling MNSHINE HIO at (612) 746-4522. The complaint form may be submitted by mail or electronically (see instructions on form).

If the complaint relates to a suspected violation or breach of PHI, the complaint must be filed within 180 days from the date of becoming aware of a suspected violation.

Upon receipt of a written complaint, it will be immediately forwarded to:

MNSHINE HIO
PRIVACY OFFICER
1915 HIGHWAY 36 WEST, SUITE 123,
ROSEVILLE, MN 55113

MNSHINE HIO shall acknowledge receipt of the complaint within 2 business days.

MNSHINE HIO shall issue a written response to the Individual or Participant within 30 days of receipt of the complaint, unless under extenuating circumstances, MNSHINE HIO may extend this deadline and provide the Individual or Participant written notification of the delay.

The response must include information about how the complainant may forward the complaint to the Minnesota Department of Health, which oversees the health information exchange program in Minnesota.

If the complaint relates to MNSHINE HIO, the complaint shall be reviewed by the MNSHINE Privacy Officer and a designated sub-committee of the MNSHINE HIE Advisory Committee. All complaints will be duly investigated, findings documented and final disposition communicated back to complainant.

If the complainant is not satisfied by the MNSHINE HIO investigation, findings, and any proposed resolution of the complaint, the complainant may send the complaint to the MNSHINE HIE Advisory Committee via the CEO and may forward complaint to the Minnesota Department of Health, which oversees the health information exchange program in Minnesota.

The final disposition of a complaint shall be documented by MNSHINE HIO.

GENERAL

MNSHINE HIO will maintain the confidentiality of the Individual who files a complaint.

MNSHINE HIO shall not retaliate, discriminate against, intimidate, coerce, or threaten any person who files a complaint.

Documentation concerning a complaint including response and resolution shall be maintained by MNSHINE HIO for at least six (6) years.

MNSHINE HIO shall periodically analyze filed complaints to determine if persistent or recurrent problems exist and make recommendations to correct identified problems.

FILING A COMPLAINT WITH U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Individuals are encouraged to file a complaint with a Participant or the MNSHINE HIO to resolve an issue. However, an Individual or a person on behalf of an Individual may also file a complaint with the Secretary of the U.S. Department of Health and Human Services, Office of Civil Rights, within 180 days from the date of becoming aware of a suspected violation of the Individual's Protected Health Information or privacy rights.

Revision History

Version	Date	Description of Revision	Author	Approved By	Approval Date
1.0	2/26/2016	Original policy effective date (Koble-MN).	—	—	—
1.1	7/28/2016	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	Koble-MN Advisory Committee	7/28/2016
1.2	8/26/2022	Updated address; Full review of policy.	Charles Peterson	Koble-MN Exec Committee	8/26/2022
2.0	10/26/2026	Converted to the MNSHINE HIE Services policy template and numbering system; assigned HIE-POL-004 (formerly Koble-MN Ref. ID 004); organizational references updated from Koble to MNSHINE; policy owner changed to the MNSHINE HIE Advisory Committee.	—	Koble-MN Exec Committee	10/12/2026

Versions 1.x were issued by Koble-MN, the former owner of the HIE business line acquired by MNSHINE, and are numbered retroactively for continuity. Approving bodies and dates for those versions are shown as originally recorded.

MNSHINE HEALTH INFORMATION EXCHANGE • POLICIES & PROCEDURES

Definitions

Policy Number	HIE-POL-005	Version	2.0
Policy Category	Information Management	Status	Active – Legacy Policy
Policy Owner	MNSHINE HIE Advisory Committee	Approval Authority	MNSHINE Board of Directors
Original Effective Date	2/26/2016	Version Effective Date	11/1/2026
Next Review Due	1/31/2027	Legacy Reference	Koble-MN Policy Ref. ID 005

For the purposes of the MNSHINE HIO policies, the following terms shall have the meaning ascribed to them below. All defined terms are capitalized throughout the policies.

Terms used, but not otherwise defined in MNSHINE HIO policies, shall have the same meaning as those terms in 45 C.F.R. §§ 160.103, 164.304 and 164.501.

APPLICABLE LAW

Applicable Law means all federal, state, and local statutes, laws, regulations, ordinances, administrative rules, and legally binding governmental requirements applicable to the collection, access, use, disclosure, protection, storage, transmission, or handling of health information, including but not limited to HIPAA and its implementing regulations, HITECH, 42 C.F.R. Part 2 governing Substance Use Disorder patient records, and all applicable state privacy, confidentiality, medical records, health information, and data protection laws, as each may be amended, supplemented, or replaced from time to time.

ADMINISTRATIVE AUTHORIZED USER

Administrative Authorized User means individuals who have been authorized by the MNSHINE HIO to perform services necessary for operating and maintaining the MNSHINE HIO.

AUTHORIZED USER

Authorized Users are individuals who have been authorized by a Participant to access the MNSHINE HIO and may include, but are not limited to, health care practitioners, employees, contractors, agents, or business associates of a participant.

BREACH

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Rules which compromises the security or privacy of the PHI.

BREAK THE GLASS

Break the Glass means the ability of an authorized user to access a patient's PHI after receiving or confirming the possession of written consent or in the case of a medical emergency as outlined in MN Stat. §144.293 Subd 8(a).

BUSINESS ASSOCIATE

Business Associate has the meaning set forth in 45 C.F.R. 160.103 and generally means an individual or organization that creates, receives, maintains, or transmits PHI on behalf of a covered entity.

HIPAA

HIPAA means the Health Insurance Portability and Accountability Act of 1996. Specifically including the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic PHI (45 C.F.R. Parts 160 and 164) as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), enacted as Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009 and as any further amendments, modification, or renumbering which occurs or takes effect during the term of the policies.

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

HITECH means the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act, Pub. L. No. 111-5.

INDIVIDUAL

An Individual means a person who is the subject of PHI and has the same meaning as the term "Individual" in 45 C.F.R. § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

Individually Identifiable Health Information means a subset of health information, including demographic information collected from an Individual, that is created or received by a health care provider or plan, employer, or healthcare clearinghouse, and relates to the past, present or future physical or mental health or condition or condition or payment for healthcare and that identifies or can be used to identify the Individual.

MEDICAL EMERGENCY

A Medical Emergency means a medical condition manifesting itself by acute symptoms of sufficient severity (including severe pain) such that the absence of immediate medical attention could reasonably be expected to result in:

1. placing the health of the individual (or, with respect to a pregnant woman, the health of the woman or her unborn child) in serious jeopardy, serious impairment to bodily functions, or;
2. serious dysfunction of any bodily organ or part.

This definition of a Medical Emergency Condition is found in the federal Emergency Medical Treatment and Active Labor Act (EMTALA) at 42 C.F.R. 489.24(b).

MNSHINE HEALTH INFORMATION ORGANIZATION

The MNSHINE HIO oversees, governs, and facilitates health information exchange among health care providers that are not related health care entities as defined in Minnesota Statutes section 144.291, subdivision 2, paragraph (j), to improve coordination of patient care and the efficiency of health care delivery.

PARTICIPANT

A Participant means an organization, health care practitioner or institution, health plan, or health care clearinghouse who has executed a written Participation Agreement and Business Associate Agreement with MNSHINE HIO.

PARTICIPATION AGREEMENT

Participation Agreement means the Agreement between MNSHINE HIO and a Participant which authorizes the Participant to have access to MNSHINE HIO.

PATIENT DATA

Patient Data means information that is requested, disclosed, stored, made available, or sent by a Participant through MNSHINE HIO. This includes, but is not limited to, PHI, Individually Identifiable Health Information, de-identified data (health information that does not identify an individual as defined in C.F.R. § 164.514(a)) and Limited Data Sets (PHI that excludes certain identifier information as defined in 45 C.F.R. § 164.514(e)).

PROTECTED HEALTH INFORMATION AND ELECTRONIC PROTECTED HEALTH INFORMATION

Protected Health Information (PHI and ePHI) means Individually Identifiable Health Information (e.g., any oral or recorded information relating to the past, present, or future physical or mental health of an Individual; the provision of health care to the Individual; or the payment for health care) that is maintained by any medium and transmitted by electronic media or in any other form or medium.

SECURITY RULE

The Security Rule means the Security Standards for the Protection of Electronic PHI at 45 C.F.R. Part 160 and Part 164, Subparts A and C as may be amended from time to time.

UNSECURED PROTECTED HEALTH INFORMATION (PHI)

Unsecured PHI means PHI in any form, including electronic, paper or verbal, that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance or as otherwise defined in 45 C.F.R. § 164.402.

VENDOR

Vendor means CRISP Shared Services, selected by MNSHINE HIO, to build and provide an electronic health information exchange system for Minnesota.

RELIANCE

If an Individual's health information is available through the MNSHINE HIO a Participant may assume the Individual has not opted-out of participation.

MINORS

In Minnesota, a minor is a person under the age of 18 years. A parent or legal guardian of a minor may authorize release of the minor's health care information.

A minor, who may under Minnesota law consent for certain treatment without parental consent, may restrict access to information relating to treatments that a minor may obtain without parental consent. In Minnesota a minor may consent to treatment for pregnancy and associated conditions, venereal disease, and/or alcohol and drug abuse.

When a minor reaches the age of majority or is emancipated, access or exercise of control of the minor's health information by a parent or legal guardian will cease. When a minor reaches the age of 18 the minor has the right to participate or opt out of participation in the MNSHINE HIO.

If a parent or legal guardian opted out of participation in the MNSHINE HIO on behalf of the minor that election will remain in effect following the minor's reaching the age of majority until the Individual makes a change to a prior election.

Revision History

Version	Date	Description of Revision	Author	Approved By	Approval Date
1.0	2/26/2016	Original policy effective date (Koble-MN).	—	—	—
1.1	7/28/2016	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	Koble-MN Advisory Committee	7/28/2016
1.2	8/26/2022	Full review of policy	—	Koble-MN Exec Committee	6/26/2022
2.0	10/26/2026	Converted to the MNSHINE HIE Services policy template and numbering system; assigned HIE-POL-005 (formerly Koble-MN Ref. ID 005); organizational references updated from Koble to MNSHINE; policy owner changed to the MNSHINE HIE Advisory Committee.	—	Koble-MN Exec Committee	10/12/2026

Versions 1.x were issued by Koble-MN, the former owner of the HIE business line acquired by MNSHINE, and are numbered retroactively for continuity. Approving bodies and dates for those versions are shown as originally recorded.

MNSHINE HEALTH INFORMATION EXCHANGE • POLICIES & PROCEDURES

Data Encryption

Policy Number	HIE-POL-006	Version	2.0
Policy Category	Information Security	Status	Active – Legacy Policy
Policy Owner	MNSHINE HIE Advisory Committee	Approval Authority	MNSHINE Board of Directors
Original Effective Date	2/26/2016	Version Effective Date	11/1/2026
Next Review Due	1/31/2027	Legacy Reference	Koble-MN Policy Ref. ID 006

PURPOSE

To provide a policy for the protection of ePHI from destruction or alteration. This policy applies to all forms of ePHI maintained or transmitted by MNSHINE HIO.

SCOPE

This policy applies to all MNSHINE HIO participants and workforce; participants, employees /authorized users, temporary staff, contracted staff, credentialed provider staff.

ENCRYPTION AT REST AND TRANSIT

The MNSHINE HIO's vendor system shall employ Federal Information Processing Standards (FIPS) 140-2 compliant cryptography and cryptographic modules.

- All ePHI will be encrypted while stored and when in transit across open communications network.
- Mail messages containing ePHI transmitted outside the MNSHINE Intranet shall be encrypted and transmitted using an approved direct secure messaging protocol.
- All other ePHI transmissions shall be encrypted using approved mechanisms (Virtual Private Networks) whenever feasible or deemed necessary based on the findings of the most recent risk analysis or audit findings.

References: 45 C.F.R. § 164.312 (c) (1-2), 45 C.F.R. § 164.312 (d), 45 C.F.R. § 164.312 (a) (1-2), 45 C.F.R. § 164.308 (3) (i), 45 C.F.R. § 164.308 (4) (i)

Revision History

Version	Date	Description of Revision	Author	Approved By	Approval Date
1.0	2/26/2016	Original policy effective date (Koble-MN).	—	—	—
1.1	7/28/2016	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	Koble-MN Advisory Committee	7/28/2016
1.2	8/26/2022	Full review of policy	—	Koble-MN Exec Committee	8/26/2022
2.0	10/26/2026	Converted to the MNSHINE HIE Services policy template and numbering system; assigned HIE-POL-006 (formerly Koble-MN Ref. ID 006); organizational references updated from Koble to MNSHINE; policy owner changed to the MNSHINE HIE Advisory Committee.	—	Koble-MN Exec Committee	10/12/2026

Versions 1.x were issued by Koble-MN, the former owner of the HIE business line acquired by MNSHINE, and are numbered retroactively for continuity. Approving bodies and dates for those versions are shown as originally recorded.

MNSHINE HEALTH INFORMATION EXCHANGE • POLICIES & PROCEDURES

Enforcement

Policy Number	HIE-POL-007	Version	2.0
Policy Category	Information Security	Status	Active – Legacy Policy
Policy Owner	MNSHINE HIE Advisory Committee	Approval Authority	MNSHINE Board of Directors
Original Effective Date	2/26/2016	Version Effective Date	11/1/2026
Next Review Due	1/31/2027	Legacy Reference	Koble-MN Policy Ref. ID 007

The MNSHINE CEO has the authority to suspend or terminate the access of any participant or authorized user in MNSHINE Health Information Organization under the following conditions:

EMERGENCY SUSPENSION

If the Vendor discovers a breach or suspicious transactions and considers it necessary to take immediate action, it may suspend access to the MNSHINE HIO immediately. The Vendor shall notify the MNSHINE HIO of the action, reason for its action, and collaborate with the MNSHINE CEO to address the situation.

AUTHORIZED USER SUSPENSION OR TERMINATION

Upon the MNSHINE CEO, or designee, completing a preliminary investigation and the MNSHINE CEO determining that there is a substantial likelihood that an Authorized User's acts or omissions create an immediate threat or will cause irreparable harm to another party, including, but not limited to, a Participant, an Authorized User, the MNSHINE HIO, Vendor, or an Individual whose health information is exchanged through the MNSHINE HIO; the MNSHINE CEO, or designee, may suspend to the extent necessary to address the threat, the Authorized User's MNSHINE access.

A Participant may suspend, limit, or revoke the access authority of its Authorized User on its own initiative upon a determination that the Authorized User has not complied with the Participant's privacy or security policies, the MNSHINE HIO policies, or the terms of the user agreement, if it is determined by the Participant to be necessary to protect the privacy of Individuals or the security of the system. The Participant must immediately notify the MNSHINE CEO, or designee, of any action limiting access of an Authorized User.

The Participant responsible for the Authorized User shall take necessary steps to resolve the problems. Once resolved, the Participant shall notify the MNSHINE CEO, or designee, and may request reinstatement of the Authorized User access.

The Participant must immediately notify the MNSHINE CEO, or designee, of any change to an Authorized User's job responsibilities or a change of employment status or provider staff privileges, including every change in an Authorized User's access whether it opens, expands, restricts, or terminates the Authorized User's access to the MNSHINE HIO.

PARTICIPANT SUSPENSION PROCESS

The MNSHINE CEO, or designee, shall immediately but within twelve hours of suspending a Participant's access provide notice of the suspension to all Participants and provide a written summary of the reasons for the suspension to the suspended Participant. The Participant shall use reasonable efforts to respond to the suspension notice with a detailed plan of correction or an objection to the suspension within three business days or, if such a submission is not reasonably feasible within three business days, then at the earliest practicable time.

Within five business days after submission of the Participants plan of correction, the MNSHINE CEO, in collaboration with Vendor shall review and either accept or reject the plan of correction. If the plan of correction is accepted, the MNSHINE CEO will, upon completion of the plan of correction, reinstate the Participant's access and provide notice to all Participants of the reinstatement. If the plan of correction is rejected, the Participant's suspension will continue, during which time the MNSHINE CEO, Vendor, and the Participant shall work in good faith to develop a plan of correction that is acceptable to all. If agreement cannot be reached, either party may appeal the dispute to the MNSHINE HIE Advisory Committee.

APPEAL PROCESS

A Participant may appeal, in writing, the MNSHINE CEO's decision to suspend or terminate its participation in the MNSHINE HIO to the Advisory Committee. The Committee shall review the written material from the Participant, Vendor, MNSHINE CEO, or any affected party. The Committee may hold a meeting with the parties to gather additional information. The Committee shall issue a final determination, in writing, and the decision shall be provided to all Participants.

TERMINATION OF PARTICIPATION AGREEMENT

Upon any termination of the Participation Agreement the terminated party shall cease to be a Participant and neither it nor its Authorized Users shall have any rights to use the MNSHINE HIO (unless the Authorized Users have an independent right to access the MNSHINE HIO through another Participant). The MNSHINE CEO, or designee, shall immediately but within twelve hours of termination of a Participation Agreement provide notice of the termination to all Participants.

DISPOSITION OF HEALTH INFORMATION UPON TERMINATION

At the time of termination, another Participant that received health information, may, at its election, retain the information in accordance with its document and data retention policies and procedures, applicable law, and the terms and conditions of the Participation Agreement and these policies.

The MNSHINE HIO shall retain an audit trail for a terminated Participant for at least six years.

PARTICIPANT POLICIES/REMOTE ACCESS

Each Participant shall establish and enforce policies and procedures regarding Authorized User access to Patient Data (including Remote Access), the conditions that must be met and documentation that must be obtained prior to allowing an Authorized User access to Patient Data.

Policies shall include procedures for taking disciplinary actions for its Authorized Users or members of its workforce in the event of a breach or non-compliance with the MNSHINE HIO policies.

Revision History

Version	Date	Description of Revision	Author	Approved By	Approval Date
1.0	2/26/2016	Original policy effective date (Koble-MN).	—	—	—
1.1	7/28/2016	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	Koble-MN Advisory Committee	7/28/2016
1.2	8/26/2022	Full review of policy	—	Koble-MN Exec Committee	8/26/2022
2.0	10/26/2026	Converted to the MNSHINE HIE Services policy template and numbering system; assigned HIE-POL-007 (formerly Koble-MN Ref. ID 007); organizational references updated from Koble to MNSHINE; policy owner changed to the MNSHINE HIE Advisory Committee.	—	Koble-MN Exec Committee	10/12/2026

Versions 1.x were issued by Koble-MN, the former owner of the HIE business line acquired by MNSHINE, and are numbered retroactively for continuity. Approving bodies and dates for those versions are shown as originally recorded.

MNSHINE HEALTH INFORMATION EXCHANGE • POLICIES & PROCEDURES

Information System Audits

Policy Number	HIE-POL-008	Version	2.0
Policy Category	Information Security	Status	Active – Legacy Policy
Policy Owner	MNSHINE HIE Advisory Committee	Approval Authority	MNSHINE Board of Directors
Original Effective Date	2/26/2016	Version Effective Date	11/1/2026
Next Review Due	1/31/2027	Legacy Reference	Koble-MN Policy Ref. ID 008

PURPOSE

Audit procedures will be used to review information system activity to detect and minimize potential risks, vulnerabilities, and security violations.

The MNSHINE HIO shall conduct audits of health information accessed and used by Authorized Users to identify inappropriate access, verify compliance with access controls to assure confidentiality, verify appropriate use of Protected Health Information and assure compliance with HIPAA Rules, Minnesota Health Records Act and MNSHINE HIO policies.

SCOPE

Policy applies to all MNSHINE HIO participants and workforce; participants, employees/authorized users, temporary staff, contracted staff, and credentialed provider staff.

Policy applies to all forms of PHI and includes system, application, and database and file activity whenever available or deemed necessary.

All activity will be logged from IT resources that store, access, maintain and transmit electronic PHI.

Whenever available audit logs will include creation, access, modification and deletion activity and the files will be retained for a period of no less than 12 months.

MNSHINE HIO AUDITS

The MNSHINE HIO shall periodically audit user authentication logs. Unusual findings must be investigated and resolved in a timely manner.

The MNSHINE HIO must audit for Break the Glass activity, including auditing queries where written patient consent is affirmed, and review findings with the Participants.

The MNSHINE HIO shall conduct periodic audits of Participant usage of MNSHINE HIO services and upon request, shall provide the Participant with audit reports.

The MNSHINE HIO may perform other Participant and Authorized User audits as it determines necessary.

Unauthorized access, use, or disclosure must be addressed by the MNSHINE CEO, or designee, by taking immediate and appropriate corrective measures including utilizing the MNSHINE HIO Enforcement policy.

Revision History

Version	Date	Description of Revision	Author	Approved By	Approval Date
1.0	2/26/2016	Original policy effective date (Koble-MN).	—	—	—
1.1	7/28/2016	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	Koble-MN Advisory Committee	7/28/2016
1.2	8/26/2022	Full review of policy	—	Koble-MN Exec Committee	8/26/2022
2.0	10/26/2026	Converted to the MNSHINE HIE Services policy template and numbering system; assigned HIE-POL-008 (formerly Koble-MN Ref. ID 008); organizational references updated from Koble to MNSHINE; policy owner changed to the MNSHINE HIE Advisory Committee.	—	Koble-MN Exec Committee	10/12/2026

Versions 1.x were issued by Koble-MN, the former owner of the HIE business line acquired by MNSHINE, and are numbered retroactively for continuity. Approving bodies and dates for those versions are shown as originally recorded.

MNSHINE HEALTH INFORMATION EXCHANGE • POLICIES & PROCEDURES

Malicious Software & Virus Protection

Policy Number	HIE-POL-009	Version	2.0
Policy Category	Information Security	Status	Active – Legacy Policy
Policy Owner	MNSHINE HIE Advisory Committee	Approval Authority	MNSHINE Board of Directors
Original Effective Date	2/26/2016	Version Effective Date	11/1/2026
Next Review Due	1/31/2027	Legacy Reference	Koble-MN Policy Ref. ID 009

PURPOSE

To detect, guard against and have formal procedures in place for the reporting of malicious software and virus protection.

SCOPE

This policy applies to all MNSHINE HIO participants and workforce; participants, employees / authorized users, temporary staff, contracted staff, and credentialed provider staff.

SECURITY CONTROLS TO MITIGATE RISK OF MALWARE AND VIRUS DISRUPTION

MNSHINE HIO, their Vendor, and each MNSHINE HIO Participant shall ensure that it employs security controls that meet applicable industry or Federal standards.

Security controls shall be implemented to ensure that information transmissions, and the methods used to transmit such information, do not introduce malware, malicious code, or other software designed to impair, disrupt, or compromise the operation, security, or integrity of systems, networks, hardware, or software utilized by MNSHINE HIO, its Vendors, or Participants.

In the absence of applicable industry standards, MNSHINE HIO, Vendor, and each Participant shall use all commercially reasonable efforts to comply with the requirements of this policy.

In addition, Malware (Virus) protection shall be installed and activated on all applicable MNSHINE HIO resources. This includes all computer equipment kept up to date with operating systems security software patches and fixes.

The MNSHINE HIO IT Department will regularly check that software is in place and up-to-date for all MNSHINE HIO systems to identify spyware, viruses, worms, Trojans and other forms of various malicious software.

Revision History

Version	Date	Description of Revision	Author	Approved By	Approval Date
1.0	2/26/2016	Original policy effective date (Koble-MN).	—	—	—
1.1	7/26/2016	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	Koble-MN Advisory Committee	7/28/2016
1.2	8/26/2022	Full review of policy	—	Koble-MN Exec Committee	8/26/2022
2.0	10/26/2026	Converted to the MNSHINE HIE Services policy template and numbering system; assigned HIE-POL-009 (formerly Koble-MN Ref. ID 009); organizational references updated from Koble to MNSHINE; policy owner changed to the MNSHINE HIE Advisory Committee.	—	Koble-MN Exec Committee	10/12/2026

Versions 1.x were issued by Koble-MN, the former owner of the HIE business line acquired by MNSHINE, and are numbered retroactively for continuity. Approving bodies and dates for those versions are shown as originally recorded.

MNSHINE HEALTH INFORMATION EXCHANGE • POLICIES & PROCEDURES

Privacy and Data Practices

Policy Number	HIE-POL-010	Version	2.0
Policy Category	Information Privacy	Status	Active – Legacy Policy
Policy Owner	MNSHINE HIE Advisory Committee	Approval Authority	MNSHINE Board of Directors
Original Effective Date	2/26/2016	Version Effective Date	11/1/2026
Next Review Due	1/31/2027	Legacy Reference	Koble-MN Policy Ref. ID 010

MNSHINE HIO PROTECTS HEALTH INFORMATION

MNSHINE HIO is committed to protecting patient privacy in accordance with state law and HIPAA. Substance use disorder treatment information protected under federal law is not shared with other health care providers unless the patient has provided specific consent or disclosure is otherwise permitted by law, such as during a medical emergency.

REVISION OF PARTICIPANT NOTICE OF PRIVACY PRACTICES

Each Participant shall revise its notice of privacy practices (the "Notice") to describe the uses and disclosures of protected health information contemplated through the Participant's participation in MNSHINE HIO, if such a use and disclosure is not already addressed in the Notice.

The Notice must meet the content requirements set forth under the HIPAA Privacy Rule and comply with applicable laws and regulations. Participants shall individually determine whether their current Notice requires amendment to reflect their contemplated uses and disclosure of protected health information through MNSHINE HIO.

MNSHINE HIO provides the following sample language for Participants who elect to amend their Notice: "We may make your protected health information available electronically through an electronic health information exchange to other health care providers that request your information for their treatment and payment purposes. Participation in an electronic health information exchange also lets us see their information about you for our treatment and payment and healthcare operation purposes. You are permitted to request and review documentation regarding who has accessed your information through the electronic health information exchange. Your provider will have information on how to make this request, or you may find the information at www.mnshine.org."

Participants may elect more stringent language but may not commit MNSHINE HIO to any additional obligations or liabilities through the Notice.

MNSHINE INFORMATION

At the point of care, an Individual or Individual's Representative must be provided with written information in plain language about information exchange and MNSHINE HIO. The material shall describe the benefits of participation, risks of participation, how and where to obtain additional information, contact information, and a description as to how the Individual's health information will be used.

In Minnesota, individuals must be informed that they have the right to opt-out of participation in the Record Locator Service so that their health care records are not found or located as a mechanism to preserve an individual's right to privacy. Individuals have a right to change a prior election and must be provided information on how to exercise those options, at no cost to the Individual. If an Individual later changes a prior election, the Participant receiving the new election shall maintain that documentation and shall notify MNSHINE HIO of the change.

OPT-OUT

If an Individual opts out of participation in the MNSHINE HIO, that Individual's information will not be searchable through MNSHINE HIO in the future. Minimal identifying information about the Individual will also be maintained in the master patient index.

A Participant may not withhold coverage or care from an Individual on the basis of that Individual's choice to opt out of participation in MNSHINE HIO.

Revision History

Version	Date	Description of Revision	Author	Approved By	Approval Date
1.0	2/26/2016	Original policy effective date (Koble-MN).	—	—	—
1.1	7/28/2016	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	Koble-MN Advisory Committee	7/28/2016
1.2	8/26/2022	Full review of policy	—	Koble-MN Exec Committee	8/26/2022
2.0	10/26/2026	Converted to the MNSHINE HIE Services policy template and numbering system; assigned HIE-POL-010 (formerly Koble-MN Ref. ID 010); organizational references updated from Koble to MNSHINE; policy owner changed to the MNSHINE HIE Advisory Committee.	—	Koble-MN Exec Committee	10/12/2026

Versions 1.x were issued by Koble-MN, the former owner of the HIE business line acquired by MNSHINE, and are numbered retroactively for continuity. Approving bodies and dates for those versions are shown as originally recorded.

MNSHINE HEALTH INFORMATION EXCHANGE • POLICIES & PROCEDURES

Use and Disclosure of Health Information

Policy Number	HIE-POL-011	Version	2.0
Policy Category	Information Privacy	Status	Active – Legacy Policy
Policy Owner	MNSHINE HIE Advisory Committee	Approval Authority	MNSHINE Board of Directors
Original Effective Date	2/26/2016	Version Effective Date	11/1/2026
Next Review Due	1/31/2027	Legacy Reference	Koble-MN Policy Ref. ID 011

PURPOSE

To comply with Minnesota State Law and HIPAA requirements for the use and disclosure of protected health information (PHI) on behalf of MNSHINE **HIO** participants.

SCOPE

This policy applies to all MNSHINE HIO participants and workforce; participants, employees/ authorized users, temporary staff, contracted staff, and credentialed provider staff.

COMPLIANCE WITH LAW

All uses and disclosures of health information through the MNSHINE Health Information Exchange (HIE) must comply with all applicable federal and state laws, regulations, and MNSHINE HIO policies and procedures. Health information may not be used or disclosed for any unlawful, unauthorized, discriminatory, or otherwise prohibited purpose.

When applicable law requires a valid authorization, consent, or other supporting documentation, or imposes specific conditions before health information may be used or disclosed, the requesting MNSHINE HIO Participant is responsible for ensuring that all required documentation has been obtained and all applicable conditions have been satisfied prior to the use or disclosure. Upon request, the Participant shall provide evidence of such documentation or compliance with required conditions to the disclosing Participant.

PARTICIPANT PERMITTED PURPOSES

A participant may request and may disclose individual health information through the MNSHINE HIO with a signed consent from the individual and only for purposes of treatment, payment, health care operations, or to comply with public health reporting requirements and as required by law.

Each MNSHINE HIO Participant shall provide or request Protected Health Information (PHI) through the HIO only to the extent necessary for the permitted purpose.

Any other use of Individually Identifiable Health Information data is prohibited.

MNSHINE HIO PERMITTED PURPOSES

MNSHINE HIO may use and disclose Protected Health Information (PHI) for the following purposes:

- for the proper management and administration of the Business Associate, in accordance with 45 C.F.R. § 164.504(e)(4);
- subject to the Participation Agreement, MNSHINE HIO policies and procedures, and 45 C.F.R. §§ 164.504(e)(2)(i) and 164.504(e)(2)(i)(B), provide data aggregation services related to the health care operations of the covered entities with which MNSHINE HIO has a Participation Agreement;
- manage authorized requests for, and disclosures of, PHI among Participants in the network;
- create and maintain a master patient index;
- provide a record locator or patient matching service;
- standardize data formats;
- facilitate Public Health reporting;
- implement business rules to assist in the automation of data exchange;
- facilitate correction of errors in health information records; and
- subject to the MNSHINE HIO Participation Agreement and policies and procedures, aggregate data on behalf of multiple covered entities.

PROHIBITIONS

Except as permitted by Minnesota State Law and the HIPAA Rules, Patient Data may not be used by MNSHINE HIO or their participants for marketing, marketing related purposes, or sales without the authorization of the Individual or the Individual's designated representative.

INFORMATION SUBJECT TO SPECIAL PROTECTION

Certain health information may be subject to special protection under federal, state, or local laws and regulations (e.g., substance use disorder). Each Participant shall identify any information that is subject to special protection under applicable law prior to disclosing any information through MNSHINE HIO. Each Participant is responsible for complying with all applicable laws and regulations.

MINIMUM NECESSARY**45 CFR 164.502(B), 164.514(D)**

The HIPAA Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. Protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function.

The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information.

The minimum necessary standard does not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an individual's authorization.
- Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.

Each Participant may share health information through MNSHINE HIO and allow access to the information by only those workforce members, business associates, and other authorized agents who need the information in connection with their job function or duties.

TREATMENT AND INSURANCE DENIAL PROHIBITION

A health care practitioner may not deny a patient health care treatment, and a health insurer may not deny a patient a health insurance benefit based solely on the provider's or patient's decision not to participate in MNSHINE HIO.

PARTICIPANT POLICIES

Each MNSHINE HIO Participant shall have in place and shall comply with its own internal policies and procedures regarding the use and disclosure of health information and the conditions that shall be met and documentation that shall be obtained, if any, prior to making any such disclosure.

Revision History

Version	Date	Description of Revision	Author	Approved By	Approval Date
1.0	2/26/2016	Original policy effective date (Koble-MN).	—	—	—
1.1	7/26/2016	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	Koble-MN Advisory Committee	7/28/2016
1.2	8/26/2022	Full review of policy	—	Koble-MN Exec Committee	8/26/2022
2.0	10/26/2026	Converted to the MNSHINE HIE Services policy template and numbering system; assigned HIE-POL-011 (formerly Koble-MN Ref. ID 011); organizational references updated from Koble to MNSHINE; policy owner changed to the MNSHINE HIE Advisory Committee.	—	Koble-MN Exec Committee	10/12/2026

Versions 1.x were issued by Koble-MN, the former owner of the HIE business line acquired by MNSHINE, and are numbered retroactively for continuity. Approving bodies and dates for those versions are shown as originally recorded.

MNSHINE HEALTH INFORMATION EXCHANGE • POLICIES & PROCEDURES

Security Incident Management

Policy Number	HIE-POL-012	Version	2.0
Policy Category	Information Security	Status	Active – Legacy Policy
Policy Owner	MNSHINE HIE Advisory Committee	Approval Authority	MNSHINE Board of Directors
Original Effective Date	2/26/2016	Version Effective Date	11/1/2026
Next Review Due	1/31/2027	Legacy Reference	Koble-MN Policy Ref. ID 012

PURPOSE

Provides guidelines to MNSHINE HIO Participants for the identification and reporting of information security incidents.

SCOPE

This policy applies to all MNSHINE HIO participants and workforce; participants, employees /authorized users, temporary staff, contracted staff, and credentialed provider staff.

ROLES & RESPONSIBILITIES

It is the primary responsibility of MNSHINE HIO Participants and workforce to identify and respond to suspected or known security incidents to limit risk of exposure and mitigate harmful effects of such incidents.

MNSHINE HIO will provide incident management training to all staff on how to identify and report security incidents and how to continuously and proactively monitor for security incidents.

Violation of this policy may result in disciplinary action up to and including termination of employment for MNSHINE HIO employees and temporary or contract staff.

REFER TO [BREACH MANAGEMENT AND NOTIFICATION POLICY](#) FOR SPECIFIC REPORTING REQUIREMENTS

DEFINITION OF SECURITY INCIDENT

For purposes of this policy, security “incident” means the act of violating an explicit or implied security policy, which includes unwanted disruption or denial of service, the unauthorized access to a system or its data; and changes to system hardware, firmware, or software characteristics without the owner’s knowledge, instruction, or consent. [45 CFR § 164.304](#), a **HIPAA security incident** is defined as the

attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operations in an information system.

Examples of incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

While certain adverse events (e.g. floods, fires, electrical outages, excessive heat, etc.) can cause system crashes, they are not considered incidents.

SEVERITY OF AN INCIDENT

When determining the severity of a security incident the following criteria will be considered:

- Scope of the impact
- Critical nature of the system or service that is affected
- Sensitivity and type of information accessed
- Likelihood that the negative impact will affect other systems or services or spread?

Response will be guided by the level of severity of the incident.

Level of Severity will be rated as – HIGH, MEDIUM, LOW AND PENDING CLASSIFICATION.

SECURITY INCIDENT SEVERITY CLASSIFICATION AND RESPONSE GUIDELINES

High Severity Incident: A security incident that significantly impacts the confidentiality, integrity, or availability of MNSHINE HIO systems, data, or services. This includes incidents that:

- Affect a large number of participants, patients, or connected organizations.
- Result in, or have the potential to result in, unauthorized access, disclosure, alteration, or loss of protected health information (PHI) or other sensitive data.
- Disrupt critical HIE operations, interfaces, or services.
- Create substantial financial, regulatory, legal, or reputational risk to MNSHINE HIO.

Response Requirements:

- Immediate investigation and coordinated response by designated incident response personnel.
- Immediate notification of the CEO, Legal Counsel, and applicable stakeholders.
- Documentation and maintenance of a formal incident response report.
- Assessment of notification obligations and implementation of any required regulatory, participant, or individual notifications.
- Ongoing executive oversight until incident resolution.

Medium Severity Incident: A security incident that affects a system, application, network segment, or non-critical HIE service and has a moderate operational impact but does not significantly impair enterprise-wide operations.

Examples may include:

- Limited-service interruptions.
- Security events affect a moderate number of users or systems.
- Suspected unauthorized access with no confirmed compromise of sensitive data.
- Incidents contained to a specific business function or operational area.

Response Requirements:

- Investigation and response initiated by the responsible personnel within four (4) hours of identification.
- Notification of the CEO, Legal Counsel, and applicable stakeholders.
- Documentation of incident details and corrective actions.
- A formal incident response report shall be completed when deemed necessary by the CEO or Incident Response Lead.

Low Severity Incident: A security incident with minimal operational impact that affects a limited number of users, systems, or business processes and presents little to no risk of expansion, data compromise, or service disruption.

Examples may include:

- Minor security policy violations.
- Isolated malware detections that are immediately contained.
- Limited system or user issues with no impact to sensitive data or HIE operations.

Response Requirements:

- Investigation and remediation by the next business day.
- Notification of the CEO and applicable stakeholders as appropriate.
- Incident documentation maintained in accordance with established procedures.
- A formal incident response report is not required unless requested to support trend analysis, audit activities, or risk management efforts.

Pending Classification

Used for reported or suspected security incidents that are currently under investigation and have not yet been assigned a severity level.

Response Requirements:

- Initiate appropriate investigative and containment activities.
- Assign a severity classification as soon as sufficient information is available.
- Escalate the incident in accordance with the assigned severity level.

REPORTING PROCEDURES

MNSHINE HIO participant or workforce member will immediately notify the MNSHINE HIO Help Desk (at (612) 746-4522) of any reportable security incident.

A ticket will be opened, and notification of the appropriate resources will begin as stated above.

Each incident will be documented as per the MNSHINE HIO BREACH MANAGEMENT AND NOTIFICATION POLICY and the record of that incident retained for at least six years .

MNSHINE HIO will report security breaches affecting individuals within 60 days of the breach via email or postal service mail and HHS will be notified of any security breach that reaches the harm thresholds outlined in the HIPAA Security Rule.

MNSHINE HIO REPORTING OF SECURITY INCIDENTS TO PARTICIPANTS

MNSHINE HIO will report to a Participant any successful impermissible access, use, disclosure, modification, or destruction of Participant's electronic PHI or interference with system operations in an information system containing Participant's electronic PHI of which MNSHINE HIO becomes aware, within five (5) business days of MNSHINE HIO's learning of the event.

When feasible, MNSHINE HIO will also report to a Participant the aggregate number of unsuccessful attempts of impermissible access, use, disclosure, modification, or destruction of electronic PHI or interfere with system operations in an information system containing electronic PHI of which MNSHINE HIO becomes aware, provided that these reports will be provided only as frequently as the parties mutually agree.

RECOGNITION OF UNSUCCESSFUL ATTEMPTS – PROACTIVE MONITORING PROCEDURE

MNSHINE HIO recognizes the number of unsuccessful attempts to the network, that is, remote access attempts without authorization.

The number of unauthorized remote access attempts have a demonstrable effect on incident handling capability.

Therefore, an “unsuccessful security event” is defined as one that does not result in unauthorized access, use, disclosure, modification, or destruction of electronic PHI or does not result in interference with an information system.

No further notice of any such unsuccessful security event will be required.

References: 45 C.F.R. § 164.312 (c) (1-2), 45 C.F.R. § 164.312 (d), 45 C.F.R. § 164.312 (a) (1-2), 45 C.F.R. § 164.308 (3) (i), 45 C.F.R. § 164.308 (4) (i)

Revision History

Version	Date	Description of Revision	Author	Approved By	Approval Date
1.0	2/26/2016	Original policy effective date (Koble-MN).	—	—	—
1.1	7/26/2016	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	Koble-MN Advisory Committee	7/28/2016
1.2	8/26/2022	Full review of policy	—	Koble-MN Exec Committee	8/26/2022
2.0	10/26/2026	Converted to the MNSHINE HIE Services policy template and numbering system; assigned HIE-POL-012 (formerly Koble-MN Ref. ID 012); organizational references updated from Koble to MNSHINE; policy owner changed to the MNSHINE HIE Advisory Committee.	—	Koble-MN Exec Committee	10/12/2026

Versions 1.x were issued by Koble-MN, the former owner of the HIE business line acquired by MNSHINE, and are numbered retroactively for continuity. Approving bodies and dates for those versions are shown as originally recorded.

MNSHINE HEALTH INFORMATION EXCHANGE • POLICIES & PROCEDURES

Security Safeguards

Policy Number	HIE-POL-013	Version	2.0
Policy Category	Information Security	Status	Active – Legacy Policy
Policy Owner	MNSHINE HIE Advisory Committee	Approval Authority	MNSHINE Board of Directors
Original Effective Date	2/26/2016	Version Effective Date	11/1/2026
Next Review Due	1/31/2027	Legacy Reference	Koble-MN Policy Ref. ID 013

PURPOSE

The MNSHINE HIO, its Vendors, and each Participant shall be responsible for maintaining a secure environment that supports access to, use of, and the continued development of the MNSHINE HIO.

SCOPE

This policy applies to all MNSHINE HIO participants and workforce; participants, employees /authorized users, temporary staff, contracted staff, and credentialed provider staff.

SAFEGUARDS

MNSHINE HIO, its Vendors, and each Participant shall use appropriate safeguards to prevent the impermissible access, use or disclosure of Protected Health Information (PHI) other than as permitted by the MNSHINE HIO policies, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of PHI through MNSHINE HIO. Appropriate safeguards for MNSHINE HIO, its Vendors, and Participants shall be those identified in the HIPAA Rules and other applicable federal and state standards and requirements, regardless of whether MNSHINE HIO, its Vendors, and Participants are subject to HIPAA Rules. MNSHINE HIO, its Vendors, and each Participant shall be responsible for requiring each of their Business Associates and Subcontractors to agree to comply with this Security Policy.

ADMINISTRATIVE AUTHORIZED USER

Definition: Administrative Authorized User means individuals who have been authorized by the MNSHINE HIO to perform services necessary for operating and maintaining the access controls and user profiles of MNSHINE HIO participants.

MNSHINE HIO Administrative Authorized Users and Participant Authorized Users will be granted access to the MNSHINE HIE environment. All authorizing access will use the principle of “Least Privilege”, that is, granting access to the minimal amount of resources required for the function that the user performs. A list of Authorized

Users is maintained in the MNSHINE HIO Participant Authorized User List. MNSHINE HIO will verify each Participant's Authorized Users with Participant periodically.

MNSHINE HIO Administrative Authorized Users shall comply with MNSHINE HIO Annual Security Awareness Training.

Revision History

Version	Date	Description of Revision	Author	Approved By	Approval Date
1.0	2/26/2016	Original policy effective date (Koble-MN).	—	—	—
1.1	7/26/2016	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	Koble-MN Advisory Committee	7/28/2016
1.2	8/26/2022	Full review of policy	—	Koble-MN Exec Committee	8/26/2022
2.0	10/26/2026	Converted to the MNSHINE HIE Services policy template and numbering system; assigned HIE-POL-013 (formerly Koble-MN Ref. ID 013); organizational references updated from Koble to MNSHINE; policy owner changed to the MNSHINE HIE Advisory Committee.	—	Koble-MN Exec Committee	10/12/2026

Versions 1.x were issued by Koble-MN, the former owner of the HIE business line acquired by MNSHINE, and are numbered retroactively for continuity. Approving bodies and dates for those versions are shown as originally recorded.

MNSHINE HEALTH INFORMATION EXCHANGE • POLICIES & PROCEDURES

Breach Management & Notification Policy

Policy Number	HIE-POL-014	Version	2.0
Policy Category	Information Security	Status	Active – Legacy Policy
Policy Owner	MNSHINE HIE Advisory Committee	Approval Authority	MNSHINE Board of Directors
Original Effective Date	2/26/2016	Version Effective Date	11/1/2026
Next Review Due	1/21/2027	Legacy Reference	Koble-MN Policy Ref. ID 014

PURPOSE

To establish requirements for the reporting, assessment, and notification of breaches involving Protected Health Information (PHI), and to ensure Participant compliance with the applicable breach notification requirements under 45 C.F.R. Part 164, Subpart D.

SCOPE

This policy applies to all MNSHINE HIO participants and workforce; participants, employees /authorized users, temporary staff, contracted staff, and credentialed provider staff.

DEFINITION OF BREACH

Breach means the acquisition, access, use, or disclosure of ePHI in a manner not permitted under the HIPAA Rules which compromises the security or privacy of the ePHI.

The impermissible or unauthorized acquisition, access, use, or disclosure ePHI is presumed to be a breach unless the covered entity or the business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

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

EXCEPTIONS. **Breach** does not include:

- Unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a covered entity or business associate.
- Inadvertent disclosure of PHI from a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate.
- Good faith by the covered entity or business associate that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

REPORTING

Participants shall notify the MNSHINE HIO of any breach of unsecured PHI in the most expedient time possible and without unreasonable delay but no later than five (5) calendar days following discovery.

MNSHINE HIO will report to a Participant any use or disclosure of the Participant's ePHI that is not permitted. In addition, MNSHINE HIO will report to the Participant, following discovery and without unreasonable delay, but in no event later than five (5) calendar days following discovery, any "breach" of "Unsecured PHI" as these terms are defined by the HIPAA Rules. MNSHINE HIO shall cooperate with the Participant in investigating any suspected or known breach and assist in meeting the Participant's obligations under the Breach Notification Rule and any other state or federal privacy or security breach notification laws.

Any incident response report must include the following information, if known at the time of the report:

1. The identification of each Individual who's unsecured ePHI has been, or is reasonably believed by MNSHINE HIO to have been, accessed, acquired, or disclosed during the breach, including their contact information if available to MNSHINE HIO;
2. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
3. A description of the types of Unsecured ePHI involved in the breach (such as name, Social Security number, date of birth, home address, or account number);
4. The identity of any person who received the non-permitted PHI;
5. Any steps Individuals should take to protect themselves from potential harm resulting from the breach;
6. A brief description of what MNSHINE HIO is doing or has done to investigate the breach, mitigate losses to Individuals and the Participant, and protect against any further breaches;
7. Contact procedures for Individuals to ask questions or learn additional information about the breach, which must include a toll-free telephone number and an e-mail, website, or postal address at MNSHINE HIO; and;
8. Identification of the names and respective titles of those who conducted the investigation on the part of MNSHINE HIO, be delivered on MNSHINE's official letterhead, signed by an officer or director of MNSHINE HIO or other responsible person and contain appropriate contact information should the Participant need further clarification regarding the content of the report.

If deemed necessary by the Participant, MNSHINE HIO may follow internal procedures to report directly to Individuals. Under this circumstance, MNSHINE HIO will prepare a draft notice, and allow Participant(s) to provide input on and review the draft notice prior to it being sent; or conduct its own reporting, if so desired. If the required information is not known at the time of the initial report to a Participant or Participants, MNSHINE HIO will follow up with an additional report or reports when the information becomes known until the time at which the incident response case is closed.

REPORTING IF MORE THAN ONE PARTICIPANT INVOLVED

In the event a breach impacts PHI associated with multiple Participants, MNSHINE HIO shall coordinate with affected Participants and provide all information, documentation, and reasonable assistance necessary to support breach investigation, risk assessment, reporting, mitigation, and notification activities. To avoid duplicative notifications and ensure affected individuals receive consistent communications regarding the incident, MNSHINE HIO shall provide notification directly to affected individuals only upon the express written direction of the affected Participant(s), unless such notification is independently required by applicable law. Participants and MNSHINE HIO shall cooperate in coordinating notification efforts to ensure compliance with applicable legal and regulatory requirements.

REPORTING TO INDIVIDUALS

If directed by the Participant, MNSHINE HIO must provide the report to Individuals in writing, by first class mail, sent to the last known address of the Individual (or to the next of kin or personal representative if the Individual is deceased). If an Individual has specified a preference for electronic mail in communications with MNSHINE HIO, then MNSHINE HIO must use electronic mail. In any case in which there is insufficient or out-of-date information to provide the written notice required, MNSHINE HIO must include a conspicuous posting on its website that includes a toll-free phone number so that affected Individuals may learn whether or not their Unsecured PHI may have been included in the breach.

REPORTING TO MNSHINE HIO

Participant will immediately notify MNSHINE HIO Help Desk at (612) 746-4522) of any breach of Unsecured PHI.

REPORTING TO THE MEDIA

Breach of Unsecured PHI involving more than 500 Individuals residing within a State, MNSHINE HIO may be directed by the Participant to provide notice to prominent media outlets serving that State. The media announcement must include a toll-free phone number so that Individuals may learn whether or not their Unsecured PHI may have been included in the breach.

REPORTING TO HHS

Breach of Unsecured PHI involving 500 or more Individuals, MNSHINE HIO may be directed by the Participant to immediately notify the Secretary of the U.S. Department of Health and Human Services (HHS) and must indicate in its notice to HHS that the report is made on behalf of Participants in the MNSHINE HIO to avoid duplicative reporting.

For breaches affecting fewer than 500 individuals, MNSHINE HIO will maintain a log of all such breaches occurring during the year and annually submit such log to the Secretary, as directed by the Participant.

RESPONSIBILITY OF VENDOR

If Vendor discovers a breach or suspicious transaction and considers it necessary to take immediate action, it may suspend the Authorized User's access to the MNSHINE HIO immediately. Vendor shall notify the MNSHINE HIO of the action, reason for its action, and collaborate with the MNSHINE CEO, or designee, to address the incident.

MNSHINE HIO RESPONSE TO A BREACH

The MNSHINE HIO may conduct an investigation of the breach as outlined in SECURITY INCIDENT POLICY, to determine the extent of the breach, determine corrective actions, and may apply sanctions, as considered necessary. Participants shall cooperate in any investigation conducted by MNSHINE HIO, state, or federal government authorities.

MNSHINE HIO shall document its findings and any actions taken in response to an investigation. A copy shall be provided to the Participant.

SANCTIONS

MNSHINE CEO may apply sanctions to Participants and their Authorized Users in the event of a breach. Sanctions may include restricting, suspending, or terminating a Participant or an Authorized User's access to the MNSHINE HIO pursuant to the ENFORCEMENT POLICY, requiring Participants or Authorized Users to undergo additional training, requiring the Participant to develop a remediation plan, terminating a Participant's Agreement, or other remedies as the MNSHINE CEO may reasonably deem necessary.

Each Participant, Vendor, or MNSHINE HIO shall be respectively liable for any monetary penalties imposed as a result of a state or federal investigation and shall implement identified corrective actions at its expense.

PARTICIPANT POLICIES

Each Participant shall implement a process to mitigate and shall mitigate to the extent practicable or required by law, the harmful effects that are known to the Participant of a known or suspected breach of access, use or disclosure of PHI.

Participants shall make this policy applicable to their business associates and their contractors and subcontractors.

RESPONSIBILITY TO EHEALTH EXCHANGE

In addition to any other requirements, as MNSHINE HIO joins the eHealth Exchange, the Participant agrees to comply with the provisions in Section 15.04 of the Restatement II of the Data Use and Reciprocal Support Agreement (“DURSA”) that require the Participant:

To comply with all Applicable Law;

- To reasonably cooperate with MNSHINE HIO regarding issues related to the DURSA.
- To Request, retrieve and send data only for a Permitted Purpose as defined in the DURSA (which is more restrictive than HIPAA);
- To use data received from MNSHINE HIO or another eHealth Exchange Participant in accordance with the terms and conditions of the DURSA;
- To refrain from disclosing to any other person any passwords or other security measures issued to the Participant or to an Authorized User of the Participant by the MNSHINE HIO; and

To as soon as reasonably practicable, but no later than:

1. One (1) hour after discovering information that leads a MNSHINE HIO Participant to reasonably believe that a Breach related to Transacting Message Content pursuant to the DURSA may have occurred, alert MNSHINE HIO to the suspected breach; and
2. Twenty-four (24) hours after determining that a Breach related to Transacting Message Content pursuant to the DURSA has occurred, provide a Notification of any such Breach to MNSHINE HIO;

In other words, if a breach (or suspected breach) occurs WHILE the Participant is sending, requesting, receiving, or accessing an electronic transmission of health information through the DURSA, the breach must be reported as required by this subsection. BUT IF the breach was from the Participant’s EHR or electronic records system and did not occur WHILE (i.e., at the same time) the Participant or the Participant’s Authorized user was using the DURSA (even though the information is ePHI received or accessed through the DURSA), the breach is considered to be not directly related to the DURSA and should not be reported under this subsection. (Although the Participant may be required to report the breach under other MNSHINE HIO and HIPAA Notification rules).

As used in Subsection (6.), “Transacting Message Content pursuant to the DURSA” means sending, requesting, receiving, asserting, responding to, submitting, routing, subscribing to, or publishing information contained within an electronic transmission of health information transacted by an MNSHINE HIO Participant using the DURSA Specifications, including any information contained in an electronic transmission, or accompanying any such transmission such as Protected Health Information (PHI), de-identified data (as defined in the HIPAA Regulations at 45 C.F.R. § 164.514), individually identifiable information, pseudonyms level (partially de-identified) data, metadata, Digital Credentials, and schema.

The Notification of a DURSA breach should include sufficient information for MNSHINE HIO to understand the nature of the Breach. For instance, the Notification could include, to the extent available at the time of the 24-hour Notification, the following information:

- One or two sentence description of the breach
- Description of the roles of the people involved in the breach (e.g. employees, Participant Users, service providers, unauthorized persons, etc.)
- The type of Message Content breached
- Participants likely impacted by the breach
- Number of individuals or records impacted or estimated to be impacted by the breach
- Actions taken by the Participant to mitigate the breach
- Current Status of the breach (whether under investigation or resolved)
- Corrective action taken and steps planned to be taken to prevent a similar

The Participant shall supplement the information contained in the Notification as it becomes available and cooperate with other Participants and MNSHINE HIO in investigating and taking corrective action in response to the breach.

The requirements do not apply to any acquisition, access, disclosure or use of information contained in or available through the DURSA if the acquisition, access, disclosure or use:

- Is not directly related to Transacting Message Content through the DURSA; or
- Is an unintentional acquisition, access, disclosure, or use of Message Content by an employee or individual acting under the authority of the MNSHINE HIO or Participant if—
- The acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the MNSHINE HIO or Participant and
- The Message Content is not further acquired, accessed, disclosed or used by that employee or individual.

The requirements are addition to and do not supersede a Participant's obligations, if any, under relevant security incident, breach notification, or confidentiality provisions of the Participation Agreement, the Participant's Business Associate Agreement with MNSHINE HIO, the HIPAA Rules, or other applicable law.

Revision History

Version	Date	Description of Revision	Author	Approved By	Approval Date
1.0	2/26/2016	Original policy effective date (Koble-MN).	—	—	—
1.1	7/28/2016	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	Koble-MN Advisory Committee	7/28/2016
1.2	8/26/2022	Full review of policy	—	Koble-MN Exec Committee	8/26/2022
2.0	10/26/2026	Converted to the MNSHINE HIE Services policy template and numbering system; assigned HIE-POL-014 (formerly Koble-MN Ref. ID 014); organizational references updated from Koble to MNSHINE; policy owner changed to the MNSHINE HIE Advisory Committee.	—	Koble-MN Exec Committee	10/12/2026

Versions 1.x were issued by Koble-MN, the former owner of the HIE business line acquired by MNSHINE, and are numbered retroactively for continuity. Approving bodies and dates for those versions are shown as originally recorded.

MNSHINE HEALTH INFORMATION EXCHANGE

Health Information Exchange Complaint Form

Use this form to file a complaint with the Minnesota Statewide Health Information Network and Exchange (MNSHINE) Health Information Organization (MNSHINE HIO) about privacy or the use of health information exchanged through MNSHINE HIO, or about a violation of MNSHINE HIO policies. This form follows the MNSHINE HIE Complaint Policy (HIE-POL-004).

Before you begin

- **Do not include health information.** Please do not include diagnoses, test results, treatment details, medical record numbers, insurance member ID numbers, or Social Security numbers. Describe what happened without these details; we will contact you if we need more information.
- **Your name and contact information are required.** We cannot accept anonymous complaints or complaints made by phone. We will keep your identity confidential.
- **File within 180 days.** If your complaint is about a suspected privacy violation or breach of health information, it must be filed within 180 days of the date you became aware of it.
- **Complaints about your provider or health plan.** If your complaint is about how a health care provider, clinic, hospital, or health plan handled your information, you may also contact that organization directly. Each MNSHINE HIO Participant has its own complaint process.
- **MNSHINE will not retaliate** against anyone for filing a complaint.

1. YOUR CONTACT INFORMATION

Fields marked * are required.

Full name *	
Organization (if filing for an organization)	
Mailing address *	
Phone *	
Email	

How should we contact you about your complaint?

☐ Mail ☐ Email ☐ Phone

2. WHO IS FILING THIS COMPLAINT?

Check one.

Individuals

- ☐ I am the individual whose health information this complaint is about.
- ☐ I am the individual's personal representative (for example, a parent of a minor child, a legal guardian, or a person with health care power of attorney).
- ☐ I am filing on behalf of an individual.

Participants and workforce

- ☐ I represent a MNSHINE HIO Participant organization.
- ☐ I am an Authorized User of a MNSHINE HIO Participant.
- ☐ I am a member of the MNSHINE HIO workforce.

If you are filing for someone else, tell us about the individual:

Individual's name	
Your relationship to the individual	

3. WHAT IS YOUR COMPLAINT ABOUT?

Check all that apply.

- ☐ Health information was used, shared (disclosed), or disposed of in a way that is not allowed
- ☐ An individual was denied access to their own health information
- ☐ Someone was retaliated against for filing a complaint

For Participants, Authorized Users, and MNSHINE HIO workforce only:

- ☐ A violation of MNSHINE HIO policies and procedures
- ☐ Other (please describe in Section 5)

4. WHO IS THE COMPLAINT ABOUT, AND WHEN DID IT HAPPEN?

The complaint is about:

- ☐ MNSHINE HIO
- ☐ A MNSHINE HIO Participant (for example, a clinic, hospital, or health plan) – please name it below
- ☐ I'm not sure

Name of the Participant organization (if applicable)	
Date the problem happened (if known)	
Date you became aware of the problem *	

Have you already filed this complaint with the Participant organization?☐ Yes ☐ No ☐ Not applicable

If yes, please include a copy of the Participant's written response, if you received one. Remove any health information from it first.

5. DESCRIBE YOUR COMPLAINT

Tell us what happened, who was involved, and how you learned about it. **Please do not include health information** such as diagnoses, test results, or medical record or insurance numbers. Attach additional pages if needed.

What happened *	
------------------------	--

What would you like to happen as a result of your complaint?	
---	--

6. SIGNATURE

I confirm that the information in this complaint is true and complete to the best of my knowledge. I understand that MNSHINE HIO may need to contact me, and may need to share information about this complaint with the Participant organization involved, in order to investigate it.

Signature *	
Date *	

For MNSHINE HIO Use Only			
Complaint number		Date received	
Acknowledgment sent (2 business days)		Written response due (30 days)	
Extension notice sent (if any)		Within 180-day filing period?	☐ Yes ☐ No ☐ N/A
Assigned to		Date of final disposition	

HIE-FRM-001 · Version 1.0 · Related policy: HIE-POL-004 Complaint Policy. Records of complaints are kept for at least six years.

Information About Filing a Complaint

Please keep this page for your records.

HOW TO SUBMIT THIS FORM

Submit your completed and signed form by mail or electronically. MNSHINE HIO does not accept complaints by phone.

By mail

MNSHINE HIO – Privacy Officer
1915 Highway 36 West, Suite 123, Roseville, MN 55113

Electronically

Email the completed form to support@mnshine.org or use the online submission option at www.mnshine.org.

To request a paper copy of this form

Call MNSHINE HIO at (612) 746-4522.

WHAT HAPPENS AFTER YOU FILE

- **We acknowledge your complaint** within 2 business days of receiving it.
- **We review and investigate.** Complaints about MNSHINE HIO are reviewed by the MNSHINE Privacy Officer. Findings are documented.
- **We respond in writing within 30 days.** If we need more time because of extenuating circumstances, we will tell you in writing.
- **We keep your identity confidential** and will not retaliate against anyone for filing a complaint.
- **If you are not satisfied with our response,** you may ask that your complaint be sent to the MNSHINE HIE Advisory Committee through the MNSHINE CEO. You may also forward your complaint to the Minnesota Department of Health (MDH), which oversees health information exchange in Minnesota.

Your right to file with the federal government

You are encouraged to file your complaint with the Participant or with MNSHINE HIO so we can resolve it. You also have the right to file a complaint with the U.S. Department of Health and Human Services, Office for Civil Rights (OCR), within 180 days of becoming aware of a suspected violation of your health information privacy rights. You can file with OCR online at www.hhs.gov/ocr/complaints or by calling 1-800-368-1019. Filing with OCR does not prevent you from filing with MNSHINE HIO.

MNSHINE HEALTH INFORMATION EXCHANGE

Health Information Exchange Opt-Out Form

About the MNSHINE Health Information Exchange

The Minnesota Statewide Health Information Network and Exchange (MNSHINE) Health Information Exchange (HIE) uses a secure system that allows your health care providers to view essential health information, such as medications, allergies, test results, health problems, and treatments, to help them make better decisions about your care. Information is encrypted and kept on a secure network.

Authorized Users may look up your information through the HIE only with your consent, or in a medical emergency as allowed by Minnesota law. Your provider and MNSHINE keep records of who accessed your information. MNSHINE provides the health information exchange services formerly provided by Koble-MN.

Your choice

Participation is voluntary. You may choose to **opt out** of the HIE, or **opt back in** if you opted out before, at any time and at no cost, by completing and signing this form.

Things to know before you decide

- **Your care will not be affected.** Participation is not a condition of receiving care or health coverage. Providers and health plans may not withhold care or coverage because you opt out.
- **Your information will not be searchable.** If you opt out, health care providers will not be able to search for your health information through the MNSHINE HIE, except as required by law. This may limit the information available to your providers, which could affect treatment options and health care decisions.
- **Other ways of sharing are not affected.** Opting out does not affect the sharing of your health information between your health care providers and health insurers by other methods, such as fax, mail, or other electronic communications. A treating provider may still use an HIE to receive your lab results, radiology reports, and other information that would otherwise be sent by fax, mail, or other electronic means.
- **Information required by law.** Opting out does not prevent a health care provider from disclosing your health information when required by law (for example, immunization records of minors and required public health reporting). Information reported as required by law will not be available to other health care providers except as permitted by law.
- **We keep a record of your choice.** To honor your choice, your name and limited identifying information will be kept in MNSHINE's master patient index, the directory used to match patient records. Information shared before you opt out will only be available to your health care provider.
- **Minors.** A parent or legal guardian may complete this form for a minor. When a minor turns 18, they may make their own choice to participate or opt out.

Opt-Out / Opt Back In Form

1. YOUR CHOICE (CHECK ONE)

- ☐ I do not want to participate in the MNSHINE HIE Record Locator Service, even in the case of an emergency.
- ☐ I want to fully participate in the MNSHINE HIE and am revoking my prior opt-out choice.

2. PATIENT INFORMATION (PLEASE PRINT CLEARLY; * REQUIRED)

Full name (first, middle, last) *		Date of birth *	
Mailing address *	City *	State *	ZIP code *
Email address		Telephone number *	
Maiden or previous name(s)		Last 4 digits of Social Security number	

3. PATIENT'S LEGAL REPRESENTATIVE (IF APPLICABLE)

Name of legal representative	Relationship to patient or legal authority (for example, parent, guardian, health care agent)
------------------------------	---

4. SIGNATURE

Signature of patient or patient's legal representative *	Date *
--	--------

How to submit: Return your signed form to your health care provider, or mail it to **MNSHINE HIO – Privacy Officer, 1915 Highway 36 West, Suite 123, Roseville, MN 55113**. Processing takes up to five (5) business days. Questions? Call (612) 746-4522 or email support@mnshine.org (please do not email this form, because it includes personal information).

For Health Care Provider Use Only

Authorized User entering the patient's choice in the clinical portal: complete this section, keep a copy with the patient's record, and send the form to MNSHINE HIO by Direct secure messaging to notifications@mnshinedirect.org.

Authorized User's name	Title	Organization
Date entered in clinical portal	Date sent to MNSHINE HIO	MNSHINE HIO use: date processed