DEPARTMENT OF HUMAN SERVICES

Minnesota Encounter Alert Service

Access Policies

Version: 7

Date: October 3, 2022

AUDACIOUS INQUIRY | BOLD SOLUTIONS FOR CONNECTED HEALTHCARE

Table of Contents

Introduction to the EAS Access Policies

The State of Minnesota has established the Encounter Alert Service (EAS) to enable information exchange inclusive of the ability to deliver real time alerts to interested parties. The Multi-Party Participation and Subscription Agreement (hereinafter referred to as the "Participant Agreement" provides for these Access Policies to provide additional specific requirements and processes that are needed for the smooth operation of EAS. These EAS Access Policies have been approved by the State of Minnesota, Department of Human Services (DHS) which is the governing authority for the EAS. Electronic information exchange activities, such as EAS, continue to evolve as new technology emerges, new use cases are identified, and as state and federal privacy rules change. Therefore, additional EAS Access Policies will likely be adopted as the EAS develops. It is also likely that some of these initial policies will be revised over time. Changes to the EAS Access Policies will be reviewed by the MN EAS Operations Workgroup and shared with all EAS Participants.

The EAS Access Policies are organized by category. Currently, these categories are HIPAA Privacy and EAS Operations and EAS Portal. Additional categories will be added over time.

Defined Terms

The Participation Agreement includes a list of defined terms which are incorporated by reference into these EAS Policies. Listed below are additional defined terms that are used in these EAS Policies. Any capitalized terms used herein that are not defined in the Participation Agreement or below shall have the meaning ascribed to them by any applicable statute or regulation.

Applicant: An organization that has submitted an application to become an EAS Participant.

Business Associate: A Business Associate is a person or entity who, on behalf of a Covered Entity or another Business Associate, performs, or assists in the performance of, a function or activity involving the use or disclosure of protected health information, including, but not limited to, facilitation of the exchange of health information; claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; or practice management.

Certification Testing: The tests and demonstrations of an EAS Participant's system and processes used for interoperable health information exchange, to assess conformity with the Specifications.

Covered Entity: A Covered Entity is (i) a health plan, (ii) a health care clearinghouse, or (iii) a health care provider who transmits any health information in any form, including in electronic form. For purposes of the EAS Access Policies, Covered Entity means EAS Participants who use EAS, including, but not limited to, health care providers, medical practices, and laboratories.

Dispute: Any controversy, dispute, or disagreement arising out of or relating to the use of EAS.

State of Minnesota, Department of Human Services (DHS): DHS serves as the governing body of EAS but is not a formal EAS Participant.

Electronic Protected Health Information or ePHI: Electronic PHI means PHI which is either transmitted by electronic media or maintained in electronic media.

HIPAA Regulations: HIPAA Regulations means the Health Insurance Portability and Accountability Act of 1996 and the rules and regulations promulgated thereunder, and the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. §§ 17921-17954) and the rules or regulations promulgated thereunder.

Patient Information Service: A service providing the following query options: a record locator service as defined in paragraph (j) or a master patient index or clinical data repository. Minn. Stat. 144.291 subd.2 (h).

Physical Safeguards: Physical Safeguards are physical measures, policies, and procedures to protect ESA and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Portal: The Prompt portal that Ai will make available to EAS Participants for use with the EAS.

Privacy Officer: Privacy Officer means the individual named in the Assigned Privacy Responsibility Policy.

Protected Health Information or PHI: PHI means health information that is individually identifiable.

Operations Workgroup: DHS has established the Operations Workgroup, a collaborative group of EAS Participants working together to provide feedback on EAS policies and procedures that arise throughout the program. The Operations Workgroup will be convened on an as needed basis to provide recommendations to DHS on governance topics that arise throughout the EAS implementation process. The Workgroup will be charged with responding to specific questions related to key implementation items and will be asked to provide recommendations to advise DHS. The Workgroup will develop recommendations through a consensus-based approach.

Workforce Member: All persons who are under the control of Ai, including, but not limited to, employees, independent contractors, loaned personnel, interns, and temporary personnel, and who have access to EAS or any PHI derived from EAS.

Workstation: Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

DEPARTMENT OF HUMAN SERVICES

HIPAA Privacy Policies and Procedures

EAS	HIPAA Privacy	Policy No.: **HP-1**
Title: **Uses and Disclosures of PHI**	Version: **1**	Effective Date:

HIPAA Privacy Rule Language:

Permitted Uses and Disclosures—§164.506

"Except with respect to uses or disclosures that require an authorization under §164.508(a)(2) through (4), or that are prohibited under §164.502(a)(5)(i), a covered entity may use or disclose protected health information for treatment, payment, or health care operations…provided that such use or disclosure is consistent with other applicable requirements of this subpart."

Uses and Disclosures for which an Authorization Is Required—§164.508

"Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization."

Uses and Disclosures of Protected Health Information: General Rules--§ 164.502(a)(3).

"A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement."

Uses and Disclosures: Organizational Requirements--§ 164.504(e)(2)

"A contract between the covered entity and a business associate must:

(i) Establish the permitted uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity…"

Purpose Statement: Limit the use and disclosure of PHI.

Policy/Procedure:

Ai may only use or disclose PHI in as necessary for it to perform its responsibilities to operate the Encounter Alert Service on behalf of the State of Minnesota. This includes, but is not limited to, performing proper management and administrative functions.

Responsibility: Ai Privacy Officer

Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.506, Uses and Disclosures to Carry Out Treatment, Payment, or Health care Operations [Standard; Required]
- 45 C.F.R. §164.508, Uses and Disclosures for which an Authorization is Required [Standard; Required]
- 45 C.F.R. 164.502(a)(3), Uses and Disclosures of Protected Health Information: General Rules
- 45 C.F.R. § 164.504(e)(2), Uses and Disclosures: Organizational Requirements

EAS	HIPAA Privacy		Policy No.: **HP-2**
Title: **Minimum Necessary Standard**		Version: **1**	Effective Date:

HIPAA Privacy Rule Language:

Uses and Disclosures of Protected Health Information: General Rules--§ 164.502(b)
"When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purposes of the use, disclosure or request."

Other Requirements Relating to Uses and Disclosures of Protected Health Information; Standard: Minimum Necessary Requirements--§ 164.514(d)
"In order to comply with § 164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.

"For any type of disclosure that it makes on a routine or recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure."

"For all other disclosures, a covered entity must: (A) develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and (B) review requests for disclosure on an individual basis in accordance with such criteria."

"A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

"For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

"For all other requests, a covered entity must: (A) develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and (B) review requests for disclosure on an individual basis in accordance with such criteria."

Purpose Statement: Ai will use reasonable efforts to limit PHI or ePHI that it uses or discloses as part of its management and administration of ESA to the least amount necessary (the "minimum

necessary") to accomplish the intended purpose of the disclosure. This policy encompasses PHI in any format, such as oral, electronic, or written.

Policy/Procedure:

Ai will limit all uses and disclosures of PHI by its Workforce Members to the minimum necessary to achieve the purpose of the use, disclosure or request except for:

- Disclosures made to the Secretary of the US Department of Health and Human Services
- Uses or disclosures required by law
- Uses or disclosures required for compliance with HIPAA

INTERNAL USES

1. The Ai Privacy Officer will assess and determine, on a yearly basis, those Workforce Members who require access to PHI in order to carry out their responsibilities for EAS.
2. Ai will document its Workforce Members' access to PHI and take measures to limit access to PHI to only those Workforce Members who require such access.
3. The Ai Privacy Officer will ensure that reasonable efforts are used to limit the access to the persons identified and for only the types of PHI which are needed to carry out their job functions.
4. For PHI that Ai uses to perform certain management and administrative functions, Ai will limit all uses of PHI to the minimum necessary to achieve the purpose of the particular management or administrative function.

EXTERNAL DISCLOSURES

1. For any disclosure that Ai makes on a routine and recurring basis, Ai will implement protocols that establish the minimum necessary amount of PHI that may be disclosed to achieve the purpose of the disclosure.
2. For all disclosures not specifically listed on the annual disclosure survey, the disclosure request must be sent to the Privacy Officer for review and determination for compliance with the minimum necessary standard.
3. Disclosures made to public officials as required by or in accordance with the law, if the public official represents that the information requested is the minimum necessary for the stated purpose(s) do not have to be reviewed by the Privacy Officer since they are deemed to be the minimum necessary for the requested disclosure.

Responsibility: Ai Privacy Officer

Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.514(d), Other Requirements Relating to Uses and Disclosures of PHI: Minimum Necessary Requirements
- 45 C.F.R. §164.502(b), Uses and Disclosures of Protected Health Information; Standard: Minimum Necessary

EAS	HIPAA Privacy	Policy No.: **HP-3**
Title: **Access of Individuals to PHI**	Version: **1**	Effective Date:

HIPAA Privacy Rule Language: "Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set."

Purpose Statement: Ai does not create nor maintain designated record sets on behalf of EAS Participants. Therefore, Ai cannot, on behalf of EAS Participants, grant an individual access to his or her PHI. This policy sets forth how Ai shall comply with requests from an individual to inspect or obtain a copy of his or her PHI.

Policy/Procedure:

1. An individual who makes an inquiry about his or her PHI will be provided a letter which indicates that Ai does not maintain the individual's designated record set and cannot comply with the request.
2. The individual will be instructed to contact his or her health care provider(s) to request access to PHI contained within his or her medical record.
3. The following is template language for a response letter:

   On [*insert date*], Ai received a request from you for protected health information that may have been exchanged through Ai. Ai is not a custodian of records nor does it maintain a designated record set. As a result, Ai cannot provide you with the requested information. If you would like to access or obtain a copy of your health information, you should contact your health care providers directly and they will gladly assist you.

Responsibility: Ai Privacy Officer

Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.524, Access of Individuals to PHI [Standard; Required]

EAS	HIPAA Privacy	Policy No.: **HP-4**
Title: **Amendment of PHI**	Version: **1**	Effective Date:

HIPAA Privacy Rule Language: "An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set."

Purpose Statement: Ai does not create nor maintain designated record sets on behalf of EAS Participants. Therefore, Ai cannot, on behalf of the EAS Participants, amend any PHI. This policy sets forth how Ai shall comply with requests from an individual to amend his or her PHI.

Policy/Procedure:

1. In the event that Ai receives a request from an individual to amend PHI exchanged through EAS, the individual will be provided with a letter which indicates that Ai does not maintain medical records and cannot comply with the request to amend his or her medical record.
2. The individual will be instructed to contact his or her health care provider to request an amendment of his or her PHI.
3. The following is template language for a response letter:

   On [*insert date*], Ai received a request from you to amend protected health information about you that may have been exchanged through Ai. Ai is not a custodian of records nor does it maintain a designated record set. As a result, Ai cannot make the requested amendment. If you would like to amend your protected health information, you should contact your health care providers directly and they will gladly assist you.

Responsibility: Ai Privacy Officer

Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.526, Amendment of Protected Health Information [Standard; Required]

EAS	HIPAA Privacy	Policy No.: **HP-5**
Title: **Assigned Privacy Responsibility**	Version: **1**	Effective Date:

HIPAA Privacy Rule Language: "A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity."

Purpose Statement: Ai will designate a Privacy Officer who will be responsible for the implementation and day-to-day administration and oversight of Ai's compliance with the HIPAA Privacy Regulations. The Privacy Officer will also develop Workforce Member and User training programs regarding the privacy of PHI, update and implement these Privacy Policies and Procedures, and serve as the designated decision-maker for issues and questions involving interpretation of the HIPAA Privacy Regulations.

Policy/Procedure:

1. The Privacy Officer is responsible for the following tasks:
    a. Inventorying the uses and disclosures of all PHI;
    b. Ensuring that legal issues in drafting compliance documents are addressed or engage competent legal counsel to draft such documents;
    c. Administering sanctions upon Workforce Members for violations of these Privacy Policies and Procedures;
    d. Developing, updating, and revising these Privacy Policies and Procedures as necessary to comply with the HIPAA Privacy Regulations;
    e. Developing a privacy training program for Workforce Members and Ai Customers;
    f. Establishing procedures to monitor internal privacy compliance;
    g. Coordinating with the Security Officer in evaluating and monitoring operations and systems development for Privacy and Security requirements;
    h. Serving as Ai's liaison to regulatory bodies for matters relating to privacy;
    i. Coordinating any audits of the Secretary of HHS or any other governmental or accrediting organization regarding Ai's compliance with state or federal privacy laws or regulations; and
    j. Other tasks that are necessary to ensure the privacy of PHI.

2. Ai's Privacy Officer's name and contact information is:
   Name: Tim Tomlinson
   Email:tim.tomlinson@pointclickcare.com
   Phone: 571-499-0770

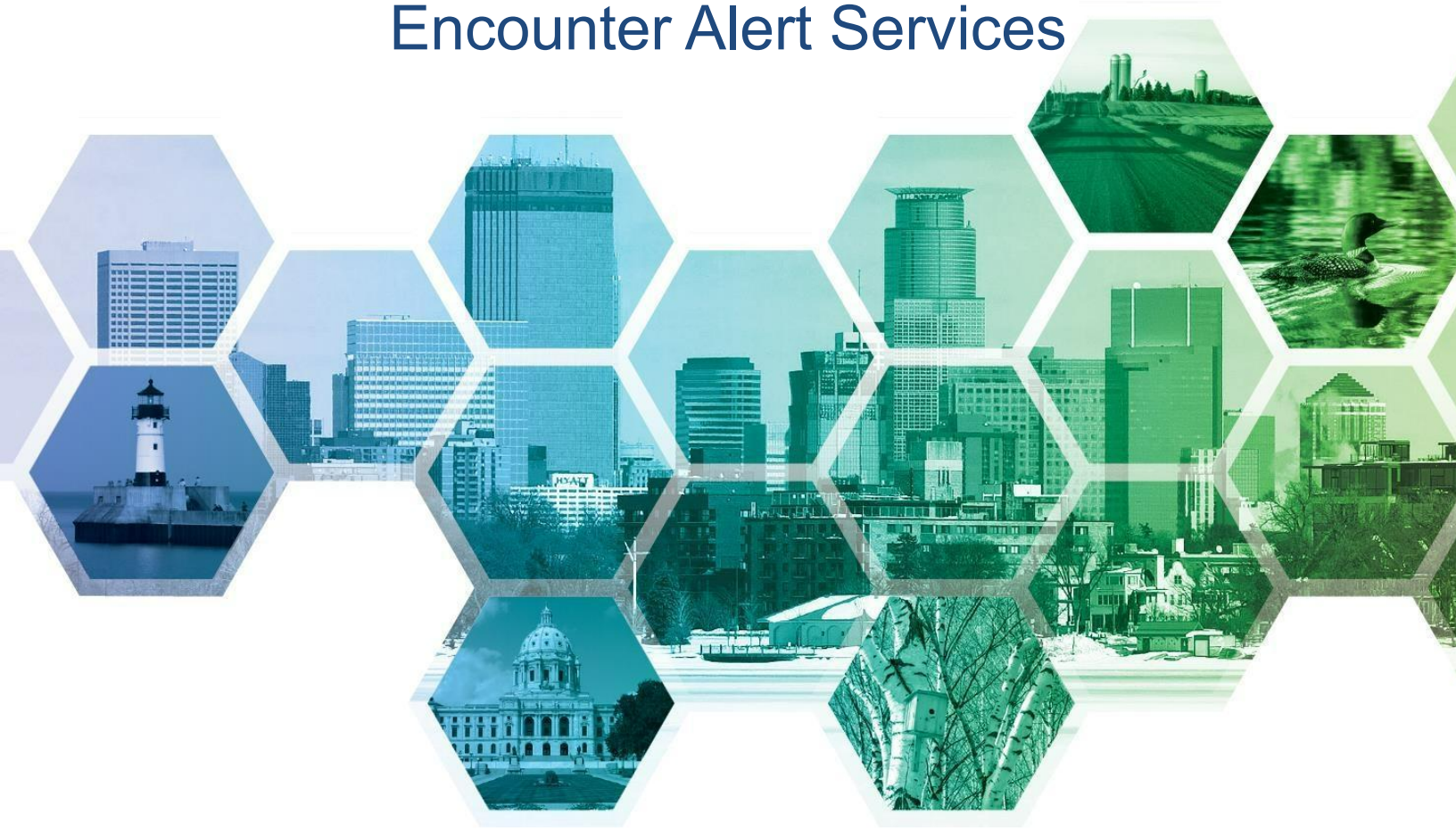
Responsibility: Ai

Regulatory Category: Privacy Regulations

Regulatory Reference:

- 45 C.F.R. §164.530(a), Personnel Designations [Standard; Required]

Operational Policies and Procedures for Encounter Alert Services



EAS	Operational Policy for Encounter Alert Notification Program	Policy No: **EA-1**
Title: **Eligibility Criteria**	Version: **2**	Effective Date: Mar 11, 2021

Purpose Statement: For consistency and fairness, the EAS has established eligibility criteria against which applications for participation can be evaluated.

Policy/Procedure:

To be eligible to be an EAS Participant, an Applicant must meet all of the following general eligibility requirements:

1. Organizational, Governance, Legal and Policy Criteria
    a. The Applicant must be a health care practitioner or institution, health plan, health care clearinghouse, accountable care organization, health information organization or other health information exchange network, Minnesota Integrated Health Partnership, a governmental agency, or other organization as defined by Ai. Community based support organizations (i.e. transportation or meal services) that are not Covered Entities are eligible to be an EAS Participant (as long as they are able to sign and support a BAA, the CBO has patient consent and the CBO has a NPP includes "HIE verbiage").
    b. The Applicant must have the organizational infrastructure and legal authority (through statutes, regulations, organizational agreements, contracts or binding policies) to comply with the obligations in the EAS Participation Agreement and to require its Participant Users to comply with applicable requirements of the EAS Participation Agreement.
    c. The Applicant must sign the EAS Participation Agreement.
2. Technical: The Applicant must attest that it has the technical resources and ability to meet the EAS Specifications.

Responsibility: Ai, EAS Applicants

EAS	Operational Policy for Encounter Alert Notification Program		Policy No: **EA-2**
Title: **Suspension and Termination**		Version: **1**	Effective Date:

Purpose Statement: Pursuant to the EAS Participation Agreement, the State or Ai have the right to suspend or terminate EAS Participant. This Policy sets forth the detailed procedures for such actions.

Policy/Procedure:

Suspension

1. Prior to suspending an EAS Participant, Ai shall provide notice of such suspension to the EAS Participant unless providing such notice will create an immediate threat to the confidentiality, privacy or security of information exchanged through EAS or will cause irreparable harm to another party (Ai, EAS Participant, EAS Participant User, the integrity or operation of EAS, or an individual). The notice shall contain a written summary of the reasons for the suspension. Examples of situations that could lead to a suspension include, but are not limited, to violations of Applicable Law or EAS Access Policies, security of system failure of the EAS Participant (i.e. malware or denial-of-service attack).
2. Ai may suspend an EAS Participant for up to thirty (30) calendar days upon completing a preliminary investigation and determining that there is a substantial likelihood that an EAS Participant's acts or omissions create an immediate threat or will cause irreparable harm to another party including, but not limited to, an EAS Participant, an EAS Participant User, the integrity or operation of EAS, or an individual whose information is exchanged through EAS.
3. Within one (1) business day of suspending an EAS Participant, Ai will provide to the suspended EAS Participant a written summary of the reasons for the suspension, if Ai did not provide this prior to the suspension. Ai will also provide notice of the suspension to all other EAS Participants. Ai will provide notice of the suspension as well as the reason(s) for the suspension to the EAS governing body.
4. The suspended EAS Participant will use reasonable efforts to respond to the suspension notice with a detailed plan of correction or an objection to the suspension within five (5) business days or, if such submission is not reasonably feasible within five (5) business days, then at the earliest practicable time.
5. If the suspended EAS Participant submits a plan of correction, Ai will, within five (5) business days, review and either accept or reject the plan of correction.
    a. If an EAS Participant submits a plan of correction that is accepted by Ai, the EAS Participant's right to participate in EAS will be reinstated upon satisfactory completion of the plan of correction that is documented in order to confirm that the problem(s)

has been adequately addressed.

b. If the EAS Participant submits a plan of correction that is rejected by Ai, Ai and the EAS Participant will work together to prepare an acceptable plan of correction. If Ai and the EAS Participant cannot reach agreement on the plan of correction within fourteen (14) calendar days, the EAS governing body will address the issue by mandating a certain plan of correction. The EAS Participant will remain suspended at least until the governing body acts on the issue.

Termination

A. Voluntarily by the Participant.

An EAS Participant may voluntarily terminate its participation in the EAS in accordance with the Participation Agreement.

All requests for termination by an EAS Participant shall be directed to Ai in writing at least thirty days prior to the requested termination date. Upon receipt of a request for voluntary termination by EAS Participant, Ai will take, or direct the proper party(ies) to take, all appropriate technical actions necessary to carry out the termination including, but not limited to, termination of the EAS Participant's Digital Credentials. Ai will list active EAS Participants on the EAS website and will update the list if an EAS Participant is terminated.

B. With Cause by Ai.

Ai or the State may terminate an EAS Participant from the EAS for the reasons set forth in the EAS Participation Agreement. Within one (1) business day Ai will communicate a termination decision to the EAS Participant. Ai will take all appropriate technical actions necessary to carry out the termination including, but not limited to, termination of the EAS Participant's Digital Credentials. Ai will list active EAS Participants on the EAS website and will update the list if an EAS Participant is terminated.

Responsibility: Ai, EAS Participants

EAS	Operational Policy for Encounter Alert Notification Program		Policy No: **EA-3**
Title: **Auditing and Monitoring**		Version: **1**	Effective Date:

Purpose Statement: Monitoring compliance with the EAS requirements, policies and procedures helps to promote trust within EAS. Each EAS Participant is required to engage in self-monitoring and submit regular attestations of compliance to Ai.

Policy/Procedure:

AUDITING AND MONITORING BY EAS PARTICIPANTS

1. All EAS Participants are required to monitor and audit access to and use of their information technology systems in connection with EAS and in accordance with their usual practices based on accepted health care industry standards and applicable law.
2. Annually, each EAS Participant will be required to complete an Attestation of Compliance in which the EAS Participant attests that the Participant and its Participant Users have been and are in compliance with the EAS Participation Agreement and the EAS Access Policies and Specifications. EAS Participants must make the Attestation of Compliance available to Ai upon request. Each EAS Participant is also responsible for instituting any other self-monitoring mechanisms that it believes necessary to allow it to provide the annual Attestation of Compliance.
3. Failure to complete the Attestation of Compliance or to make it available to Ai upon request will be deemed a material breach under the EAS Participation Agreement and may result in the Participant's suspension from EAS.
4. If the EAS Participant continues to fail to provide the Attestation of Compliance within thirty (30) days of receiving notice of such failure, then the EAS Participant's participation in EAS may be terminated.

Responsibility: Ai, EAS Participants

EAS	Operational Policy for Encounter Alert Notification Program		Policy No: **EA-4**
Title: **42 CFR Part 2 Records**		Version: **1.1**	Effective Date:

Purpose Statement: The privacy and security of all health information is protected under both various federal and Minnesota laws including, but not limited to, HIPAA, 42 CFR Part 2, the Minnesota Health Records Act, and the Minnesota Health Care Bill of Rights. This Policy addresses records of federally certified substance abuse treatment centers that are subject to 42 CFR Part 2 ("Part 2 Records"). The provisions of Part 2 do not apply to records related to alcohol or drug abuse that originate from a facility that is not a federally assisted alcohol or drug abuse program.[1]

Policy/Procedure:

1. Definition: Part 2 Records are defined as alcohol and drug abuse records that would identify an individual as an alcohol or drug abuser when those records are obtained, created or maintained by a federally assisted alcohol or drug abuse program for the purpose of treating alcohol or drug abuse, making a diagnosis for that treatment, or making a referral for that treatment.[2]
2. EAS Policy: An EAS Participant may not include Part 2 Records as part of any EAS Message unless there is a documented medical emergency and the Part 2 Records are needed for treatment of the individual who is the subject of the Part 2 Records. However, if an EAS Participant meets the definition of a "Part 2 Program" as defined in 42 CFR §2.11, and the EAS Participant has provided a written attestation to that effect that includes an affirmation of such EAS Participant's intent to receive alerts for its Part 2 Program patient/client panel (each a "Part 2 EAS Participant"), then the Part 2 EAS Participant may submit a patient/client panel following execution of a Qualified Service Organization Agreement (QSOA) with Ai. Further, the Part 2 EAS Participants will receive alerts for their empaneled patients/clients but will otherwise be invisible to all other EAS Participants, meaning the Part 2 EAS Participants will not be listed as part of a Care Team (those who have a patient-to-provider relationship). Lastly, Part 2 EAS Participants cannot be ADT sources at this time so the data flow is always uni-directional, (i.e. alerts will be sent to the Part 2 EAS Participants, but not from Part 2 EAS Participants."

Responsibility: EAS Participants

[1] See Substance Abuse and Mental Health Services Administration (SAMSHA) FAQ Applying the Substance Abuse Confidentiality Regulations to HIE https://www.samhsa.gov/sites/default/files/faqs-applying-confidentiality-regulations-to-hie.pdf

[2] 42 CFR Part 2

EAS	Operational Policy for Encounter Alert Notification Program		Policy No: **EA-5**
Title: **Self-Pay**		Version: **1.1**	Effective Date:

Purpose Statement: The privacy and security of all health information is protected under both various federal and Minnesota laws including, but not limited to, HIPAA, 42 CFR Part 2, the Minnesota Health Records Act, and the Minnesota Health Care Bill of Rights. This Policy addresses the disclosure of self-pay record to EAS.

Policy/Procedure:

1. An EAS Participant is not required, but should as a best practice, inform EAS, as agreed upon during implementation, through mechanisms outlined in the Specifications, when sending self-pay information that may have additional restrictions from disclosure by local, state, and federal law. Please note that this is not intended to exclude uninsured nor require inclusion of uninsured patients (for which no special ADT filtering is required).
2. Self-pay filtering is not required for Public Health reporting, nor Provider-to-Provider alerting, but is mainly expected for future potential Provider-to-Payor use cases (that are not supported today, but if they are in the future, EAS is expected to use best efforts to filter out Self Pay records from generating alerts for payors.

Responsibility: EAS Participants

EAS	Operational Policy for Encounter Alert Notification Program	Policy No: **EA-6**
Title: **Use and Disclosure of PHI**	Version: 2	Effective Date: 9Apr2020

Purpose Statement: Pursuant to the EAS Participation Agreement, EAS is permitted to send PHI to other EAS Participants for any of the Permitted Purposes identified in the EAS Participation Agreement. Pursuant to the Business Associate Agreement between Ai and each EAS Participant, Ai may also use and disclose PHI, as needed, for its proper management and administration and to fulfill any other obligations described in the EAS Participation Agreement.

Policy/Procedure:

1. Ai may only use information provided by an EAS Participant, as needed, to perform certain proper management and administrative functions and fulfill its obligations under the EAS Participation Agreement.
2. Each EAS Participant is responsible for making sure that all information it sends as a Participant complies with Applicable Law. This includes obtaining any consents or authorizations required by Applicable Law prior to sending such information or to subscribing to receive alerts on a patient.
3. The Minnesota Department of Human Services has advised that every individual who obtains benefits through the Department, both Medical Assistance and MinnesotaCare, is deemed to have provided consent for their information to be exchanged via the EAS through enrollment.
4. All EAS participants acknowledge and agree that EAS does meet the definition of a Patient Information Service or record locator service as defined by the Minnesota Health Records Act 144.291.

Responsibility: Ai; EAS Participants

EAS	Operational Policy for Encounter Alert Notification Program	Policy No: **EA-7**
Title: **EAS Participation Agreement Flow-downs**	Version: **1**	Effective Date:

Purpose Statement: By signing the EAS Participation Agreement, each EAS Participant has agreed to protect the privacy, security and integrity of the information exchanged through the EAS and to comply with the terms of the Business Associate Agreement which is part of the EAS Participation Agreement. EAS Participants are required to flow-down to its EAS Participant Users, and to anyone else who is authorized to access the EAS through or on behalf of the Participant, the obligation to comply with the Participation Agreement Terms and Conditions.

Policy/Procedure:

1. All organizations that act as EAS Participants must agree to the EAS Participation Agreement before the organization is approved as a Participant.
2. EAS Participant must have in place legally enforceable means to assure that its EAS Participant Users, and anyone else who is authorized to access the EAS through or on behalf of the Participant, comply with the Participation Agreement Terms and Conditions including the EAS Access Policies. The phrase "legally enforceable means" may include contracts, agreements or policies and procedures.
3. EAS Participant must have legally enforceable mechanisms in place to take steps to discipline anyone who does not comply with the EAS Participation Agreement Terms and Conditions. EAS Participant will inform Ai of these mechanisms upon request.

Responsibility: Ai; EAS Participants

EAS	Operational Policy for Encounter Alert Notification Program	Policy No: **EA-8**
Title: **Data Retention**	Version: **1**	Effective Date:

Purpose Statement:
This policy describes how data flow into the EAS and how data are retained or purged.

Policy/Procedure:

1. Subject to Applicable Law, EAS will retain data for a minimum period of seven (7) years in order to maintain an auditable history of Transactions through EAS.
2. Data from raw messages will be deleted after sixty (60) days of receipt.
3. Data is retained in EAS for improved patient matching (i.e. combined demographics) and for HIPAA Accounting for Disclosures.
4. Data retained for care coordination will be removed after twelve (12) months.
5. If an EAS Participant terminates participation in EAS:
    a. Ai will disable the EAS Participant's data feeds and end the EAS Participant's ability to access EAS.
    b. Message Content previously submitted by the EAS Participant (if any), will be removed from EAS.
    c. All data contributed from the terminating EAS Participant will be removed, except as required by HIPAA Technical Safeguards.
6. Data for patients which do not match any EAS criteria for public health reporting or panel matches are deleted after 5 days of receipt.

Responsibility: Ai; EAS Participants

EAS	Operational Policy for Encounter Alert Notification Program		Policy No: **EA-9**
Title: **Participation Agreement Maintenance**		Version: **1**	Effective Date:

Purpose Statement: By signing the EAS Participation Agreement, each EAS Participant has agreed to a common multi-party agreement. Over time modifications to the EAS Participation Agreement may be required to comply with changes in applicable law or changes to EAS.

Policy/Procedure:

1. If the need to modify the EAS Participation Agreement arises, the changes will be reviewed and approved by the MN EAS Operations Workgroup.
2. If substantive changes result, an amendment will be made to all current executed agreements and an updated Participation Agreement will be executed by all future EAS Participants.
3. All organizations that act as EAS Participants must agree to the EAS Participation Agreement before the organization is approved as a Participant.
4. The most current version of the Participation Agreement will be posted on the MNEAS.org website.

Responsibility: Ai; EAS Participants; MN EAS Operations Workgroup

EAS	Operational Policy for Encounter Alert Notification Program	Policy No: **EA-10**
Title: **Consumer Feedback**	Version: **1**	Effective Date:

Purpose Statement: MNEAS.org is a public facing website established as a resource for EAS Participants, potential participants, and consumers. There are a number of resources on the site for consumers. Educational documents are available to provide an overview of the program and answer potential consumer questions. In addition, consumers are able to provide feedback regarding the program or file a privacy complaint. Feedback and complaints can be submitted by sending an email to MN-EAS-ServiceDesk@aing.com. A link to the email can also be found on the website.

Policy/Procedure:

1. Consumers have the ability to file a privacy complaint or provide feedback regarding EAS through the MNEAS.org website.
2. Consumer complaints will be acknowledged within five business days.
3. Confidentiality will be maintained throughout the process.
4. All documentation concerning a complaint including response and resolution will be maintained by for at least seven (7) years.

Responsibility: Ai; EAS Participants

EAS	Operational Policy for EAS Program	Policy No: EA-11
Title: **Data Breach Response Procedure**	Version: **1.1**	Effective Date:

Purpose Statement: Despite Ai's implementation of controls to safeguard the confidentiality, integrity and availability of protected health information (PHI) transmitted or stored through the EAS, cyber-incidents may occur. Ai has procedures in place that address its awareness of, response to, and creation of reports about Security Incidents and Data Breaches under HIPAA. Those procedures are integral parts of Ai's ongoing efforts to comply with the HIPAA Security and Breach Notification Rules. EAS Participants and their Participant Users are also responsible for being aware of and reporting any Security Incidents and Data Breaches that involve or impact the EAS.

Policy/Procedure:

BACKGROUND DEFINITIONS AND CONCEPTS

1. Under HIPAA, a "Security Incident" is attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Unsuccessful access attempts fall within the literal HIPAA definition of Security Incidents, but such attempts (such as pings and port scans) occur continually and routinely across the Internet. Ai monitors such events, but normally reports only aggregate monthly or quarterly statistics for routine events.

2. A "successful" Security Incident may result in unauthorized access to information in EAS systems, but may or may not result in a data Breach, depending on what information may have been accessible or accessed.

3. A data "Breach" is an unauthorized acquisition, access, use, or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of PHI – unless it is demonstrated, based on a risk assessment, that there is a low probability that PHI has been compromised.

4. The Breach notification requirements only apply to PHI that is "unsecured." Unsecured PHI is PHI that is not secured by a technology (such as encryption) that renders the data unusable, unreadable or indecipherable and is endorsed by an ANSI-accredited standards setting organization.

EAS PARTICIPANT REPORTS OF POTENTIAL DATA BREACHES

1. Any EAS Participant must report to Ai any actual or potential Breach potentially affecting the EAS (including a successful Security Incident that may have resulted in a Breach) without unreasonable delay, and preferably as soon as it is suspected, but in no event more than ten (10) business days after the discovery of the Breach.

2. The individual providing notice of the potential Breach may provide such notice in any format, including in writing, electronically, or orally.
3. The Ai Privacy Officer will document the report of a potential Breach including the date and time that he or she was notified of such event.
4. Ai will not take any retaliatory measures against a Participant, Participant User, or individual who reports a potential Breach. However, if the Breach was created by the neglect or deliberate action of an EAS Participant or Participant User, then Ai may impose sanctions as set forth in other Policies.
5. No EAS Participant will prohibit or otherwise attempt to hinder or prevent anyone from reporting a potential Breach.

INCIDENT/BREACH RESPONSE BY AI

1. An EAS Participant's or Participant User's noncompliant use of the EAS could potentially result in a Breach.
2. If Ai discovers, or receives a complaint or notice regarding, a potentially successful Security Incident or other potential Breach, Ai will do the following:
    a. The Ai Privacy Officer will immediately activate an Incident Response Team.
    b. The Incident Response Team will promptly conduct an initial review of the facts surrounding the possible Breach, including a preliminary risk assessment, to determine whether a successful Security Incident and/or a Breach occurred. The Incident Response Team will strive to make an initial determination within 48 hours of becoming aware of the potential Breach.
    c. To determine whether a Breach occurred, the Incident Response Team will conduct a "risk assessment" to examine whether there is more than a low probability of the information being compromised. In this risk assessment, the Incident Response Team will evaluate the following factors:
        i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
        ii. The unauthorized person who used the PHI or to whom the disclosure was made;
        iii. Whether the PHI was actually acquired or viewed; and
        iv. The extent to which the risk to the PHI has been mitigated.
    d. If the Incident Response Team determines that a Breach did not occur, the Privacy Officer will document this along with all of the information that supports such conclusion and no further investigation will be required.

e. If the Incident Response Team determines that a Breach did occur or is likely to have occurred, then the following steps will be followed:

   i. Depending on its preliminary risk assessment, Ai may immediately suspend all EAS access to Participant(s), Participant User(s), or individual user(s) involved in the incident pending further investigation.

   ii. The Incident Response Team will determine the scope, magnitude and severity of the Breach; mechanisms for containing the Breach if it is on-going; mechanisms for mitigating the harmful effects of the Breach and, ways to remediate the vulnerability that led to the Breach. The Incident Response Team will prepare these initial findings within ten (10) business days of becoming aware of the potential Breach and will update those findings as more information becomes available.

      - A copy of the findings of the investigation, excluding any sensitive health information;
      - Each remedial action to be taken by each person and the associated time frame of the remedial action;
      - Any action necessary to mitigate the harm that may be caused by the incident;
      - The person that is responsible for carrying out each action to mitigate harm; and
      - Any future action that Ai may take, including suspension, if the person does not comply with the remedial action.

   iii. The Incident Response Team will determine which EAS Participants, if any, should be involved in the investigation and mitigation activities and will involve such EAS Participant as the Team deems appropriate.

   iv. The Incident Response Team, in coordination with the State of Minnesota, will formally notify all affected EAS Participants of a Breach as soon as practicable, but no later than ten (10) business days after discovery:

      - The date of the Breach.
      - The identity of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such Breach if it can be determined.
      - A description of the roles of the people involved in the Breach including, but not limited to, EAS Participants or Participants Users, Vendors or unauthorized persons.

- The type of information that was breached or involved in the Breach if it can be determined.
- A brief description of the circumstances involved in the Breach.

v. Legal counsel will determine whether Ai is required to make any additional notifications pursuant to applicable breach notification laws and will discuss such notifications with the Incident Response Team.

vi. If Ai has determined that an EAS Participant or Participant User's noncompliant behavior caused a Breach, Ai and the State of Minnesota will determine the appropriate corrective action to pursue, including potential termination of the agreement authorizing access to and use of the EAS System. The EAS Participants and Participant Users must abide by whatever corrective action Ai and the State decide to pursue regarding the noncompliant behavior.

vii. The Privacy Officer will retain all documentation regarding the Breach for seven years.

3. Based on the nature of the complaint or notice, Ai, in its sole discretion, may choose to suspend access to the EAS by the EAS Participant or Participant User who is the subject of the complaint or notice. Ai will implement such suspension in accordance with the applicable suspension policy. If there is evidence that any EAS Participant or Participant User failed to comply with EAS requirements and the non-compliant behavior caused the Data Breach, then Ai can terminate such EAS Participant or Participant User.

AI'S OBLIGATIONS TO THE STATE OF MINNESOTA

1. Ai has agreed with the State of Minnesota to comply with the following State requirements:

A. Mitigation of harmful effects. Upon discovery of any actual or suspected privacy incident, security incident, or breach, Ai will mitigate, to the extent practicable, any harmful effect of the privacy incident, security incident, or breach. Mitigation may include, but is not limited to, notifying and providing credit monitoring to affected individuals.

B. Investigation. Upon discovery of any actual or suspected privacy incident, security incident, or breach, Ai will investigate to (1) determine the root cause of the incident, (2) identify individuals affected, (3) determine the specific protected information impacted, and (4) comply with notification and reporting provisions of the Contract, this Attachment and applicable law.

C. Corrective action. Upon identifying the root cause of any privacy incident, security incident, or breach, Ai will take corrective action to prevent, or reduce to the extent practicable, any possibility of recurrence. Corrective action may include, but is not limited to, patching information system security vulnerabilities, employee sanctions, or revising policies and procedures.

D. Notification to individuals and others; costs incurred.

i. Protected Information. Ai will determine whether notice to data subjects and/or any other external parties regarding any privacy incident or security incident is required by law. If such notice is required, Ai will comply with the State's and Ai's obligations under any applicable law requiring notification, including, but not limited to, Minn. Stat. §§ 13.05 and 13.055.

ii. Protected Health Information. If a privacy incident or security incident results in a breach of protected health information, as these terms are defined in this Attachment, then Ai will provide notice to individual data subjects under any applicable law requiring notification, including but not limited to providing notice as outlined in 45 C.F.R. § 164.404.

iii. Failure to notify. If Ai fails to notify individual data subjects or other external parties under subparagraphs (a) and (b), then Ai will reimburse the State for any costs incurred as a result of Ai's failure to provide notification.

E. Obligation to report to the State. Upon discovery of a privacy incident, security incident, or breach, Ai will report to the State in writing.

i. Communication with authorized representative. Ai will send any written reports to, and communicate and coordinate as necessary with, the State's authorized representative.

ii. Cooperation of response. Ai will cooperate with requests and instructions received from the State regarding activities related to investigation, containment, mitigation, and eradication of conditions that led to, or resulted from, the security incident, privacy incident, or breach.

iii. Information to respond to inquiries about an investigation. Ai will, as soon as possible, but not later than forty-eight (48) hours after a request from the State, provide the State with any reports or information requested by the State related to an investigation of a security incident, privacy incident, or breach.

F. Documentation. Ai will document actions taken under paragraphs A through E above, and provide such documentation to the State upon request.

1. Ai has agreed with the State of Minnesota to comply with the following additional State requirements:

A. Protected Health Information. Ai will report breaches and security incidents involving protected health information to the State and other external parties. Ai will notify the State, in writing, of (1) any breach or suspected breach of protected health information; (2) any security incident; or (3) any violation of

an individual's privacy rights as they involve protected health information created, received, maintained, or transmitted by Ai or its Agents on behalf of the State.

i. Breach reporting. Ai will report, in writing, any breach of protected health information to the State within five (5) business days of discovery, in accordance with 45 C.F.R § 164.410.

Reports to the authorized representative regarding breaches of protected health information will include:

(1) Identities of the individuals whose unsecured Protected Health Information has been breached.

(2) Date of the breach and date of its discovery.

(3) Description of the steps taken to investigate the breach, mitigate its effects, and prevent future breaches.

(4) Sanctions imposed on members of Ai's workforce involved in the breach.

(5) Other available information that is required to be included in notification to the individual under 45 C.F.R. § 164.404(c).

(6) Statement that Ai has notified, or will notify, affected data subjects in accordance with 45 C.F.R. § 164.404.

ii. Security incidents resulting in a breach. Ai will report, in writing, any security incident that results in a breach, or suspected breach, of protected health information to the State within five (5) business days of discovery, in accordance with 45 C.F.R § 164.314 and 45 C.F.R § 164.410.

iii. Security incidents that do not result in a breach. Ai will report all security incidents that do not result in a breach, but involve systems maintaining protected health Information created, received, maintained, or transmitted by Ai or its Agents on behalf of the State, to the State on a monthly basis, in accordance with 45 C.F.R § 164.314.

iv. Other violations. Ai will report any other violation of an individual's privacy rights as it pertains to protected health information to the State within five (5) business days of discovery. This includes, but is not limited to, violations of HIPAA data access or complaint provisions.

v. Reporting to other external parties. Ai will report all breaches of protected health information to the federal Department of Health and Human Services, as specified under 45 C.F.R 164.408. If a breach of protected health information involves 500 or more individuals:

(1) Ai will immediately notify the State.

(2) Ai will report to the news media and federal Department of Health and Human Services in accordance with 45 C.F.R. §§ 164.406-408.

B. Other Protected Information. Ai will report all other privacy incidents and security incidents to the State.

i. Initial report. Ai will report all other privacy and security incidents to the State, in writing, within five (5) days of discovery. If Ai is unable to complete its investigation of, and response to, a privacy incident or security incident within five (5) days of discovery, then Ai will provide the State with all information under Section 2.2(E)(1)-(4), of this Attachment that are available to Ai at the time of the initial report.

ii. Final report. Ai will, upon completion of its investigation of and response to a privacy incident or security incident, or upon the State's request in accordance with Section 2.2(E)(5) submit in writing a report to the State documenting all actions taken under Section 2.2(E)(1)-(4), of this Attachment.

2. Ai will take such additional or different actions as may be required by law, its contract with the State of Minnesota, or applicable Business Associate Agreements.

Responsibility: Ai, Privacy Officer, EAS Participants, EAS Participant Users

EAS	Operational Policy for Encounter Alert Notification Program	Policy No: **EA-12**
Title: **Expected Data from ADT Sources**	Version: 4	Effective Date: 1Jan2022

Purpose Statement: EAS Participants agree that the service provides the most value to all stakeholders when there is a uniform level of participation in terms of the data contributed by the ADT sources. This policy describes the expected data sent by the ADT sources, and sets expectations for not data filtering by payor or insurance types.

Policy/Procedure:

1. Until December 31, 2022, EAS Participants are expected to submit all patient ADT data (and not filter based on the type of patient insurance. This is enabled by declaring EAS a "Patient Information Service" (in EA-6) and by adjusting the data retention policy (EA-8) to only keep data for patients that trigger alerts based on an EAS panel match or based on meeting public health reporting criteria. This policy will be revisited later in 2022 as the COVID-19 crisis and surveillance methods stabilize, and further clarity is available regarding other regulatory requirements (for example: info-blocking and CMS e-Notifications).

2. Unless otherwise revised, after December 31, 2022, EAS Participants will submit, at minimum, ADT data for patients who have Medicare and Medicaid insurances (including primary, secondary, tertiary or dual Medicare/Medicaid scenarios). However, EAS Participants may stop submitting Medicare ADT data if subscribers are not using the data. Medicare subscription usage will be reviewed as part of the annual compliance checklist.

3. EAS Participants may be exempt from sending the minimum ADT data, and may filter by insurance type, if the number of patients with certain insurance types seen at the facility is low and less than a few percent of the visits (for example, a Children's hospital may filter ADTs to not send Medicare patients since the volume is so low).

4. EAS Participants may optionally ask Ai to filter and only process ADT data for patients with active subscriptions or those that meet specific event criteria for public health reportable conditions.

5. It is understood that compliance with this policy is within the overall policy (including EA-5 Self-Pay) and MN EAS Participation Agreement framework, which describes the overall need to be compliant with applicable laws.

Responsibility: EAS Participants (that are ADT data sources)

EAS	Operational Policy for Encounter Alert Notification Program	Policy No: **EA-13**
Title: **Patient Information Service Opt-Out**	Version: 1	Effective Date: 9Apr2020

Purpose Statement:

EAS, as a Patient Information Service as defined in MN statute:

https://www.revisor.mn.gov/statutes/cite/144.291,

shall provide support for a patient to opt-out, which is further described in MN statute:

**********.revisor.mn.gov/statutes/cite/144.293.

Policy/Procedure:

EAS will support multiple mechanisms for a patient to opt-out of EAS and the Patient Information Service:

#1: A patient can directly submit a request via the MNEAS.org website (phone, eMail, etc.).

#2: A patient can complete an opt-out form on the MNEAS.org website.

#3: A patient can indirectly opt-out of EAS by submitting a request to their provider, who if connected via HL7 ADT, can submit an opt-out flag in the HL7 ADT CON segment.

#4: A patient can opt-out of allowing a provider to query (or opt-out of inclusion in an EAS panel).

In the case of methods #1 and #2, the patient's identity will be verified using reasonable and practical best practice methods, aligned Identity Assurance Level 1, or "IAL 1", as defined by NIST Special Publication 800-63, Revision 3 (https://pages.nist.gov/800-63-3/sp800-63-3.html).

Operational Policies and Procedures for EAS Portal

EAS	Operational Policy for EAS Portal	Policy No: **PORT-1**
Title: **Portal Participant Enrollment**	Version: **1**	Effective Date:

Purpose Statement: Ai supports a portal, Prompt, to enable access by EAS Participant and EAS Participant Users to the EAS. To protect the confidentiality, integrity, and availability of ePHI exchanged through the Ai Portal, Ai has implemented a strict enrollment process to ensure that only those individuals and organizations that meet the eligibility criteria have access to Prompt.

Policy/Procedure:

1. Each organization that desires for its employees and contractors to access Prompt will be responsible for completing the enrollment process.
2. To enroll, the organization must complete and submit the Prompt Portal Enrollment Form, which is available on the EAS website.
    a. The Enrollment Form will require an individual who is authorized to act on behalf of the organization to attest to the following:
        i. the organization is either (i) a valid legal entity in good standing in the State of Minnesota or (ii) a local, state or Federal government agency;
        ii. the organization has a reason to send and receive PHI or other information related to the provision of health care; and
        iii. all information provided in the Enrollment Form is true, accurate and complete.
    b. Organizations requesting access to the Prompt Portal must also attest that they provide treatment and/or care coordination services to individuals in the State of Minnesota.
    c. In the Enrollment Form, the enrollee will be required to identify a central point of contact for all correspondence between Ai and the organization (the "POC").
    d. In the Enrollment Form, the enrollee will also be required to provide the following:
        i. The services that the enrollee would like access to through the Prompt Portal;
        ii. A list of individuals who are employed or engaged by the enrollee who will be provided with access to the Prompt Portal;
        iii. The role(s) to be assigned to each individual (refer to the EAS Portal User Roles policy (PORT-2) for more information on the types of roles);
        iv. Up to two individuals who will serve as Delegates for the organization's Prompt account.
    e. When identifying Delegates, the individual submitting the Enrollment Form must attest that:

i. Each Delegate is under the direction and control of the organization's Site Administrator; and

ii. The enrollee has provided true and accurate contact information for the Prompt Delegate(s). A separate enrollment form must be submitted for each account desired under a single Portal Participant account.

3. The POC is responsible for maintaining accurate enrollment information and notifying Ai of changes to such information so long as the organization remains an EAS Participant. This includes notifying Ai of changes to the organization's POC and Portal Users in accordance with the processes established by Ai.
4. Once the organization submits all required enrollment information to Ai, if the organization is a legal entity, Ai will verify with the State of Minnesota that the organization is active in Minnesota. Such verification is not required if the organization is a local or state government agency.
5. Once Ai completes any required verification, Ai will activate the organization's Users' Portal accounts. Ai will notify the POC once these accounts have been activated.
6. Each of the EAS Participant's Users will be assigned a unique username and temporary password to activate the EAS Participant User's access to Prompt. The first time each Portal User signs-on to Prompt, he/she will be required to accept the applicable Portal End User License Agreement.

Responsibility: Ai; EAS Participants and EAS Participant Users

EAS	Operational Policy for EAS Portal	Policy No: **PORT-2**
Title: **Prompt User Roles**	Version: **1**	Effective Date:

Purpose Statement: Prompt will employ role-based access controls to ensure that Portal Users have access to the minimum amount of information necessary for them to perform their job functions and effectively use Prompt.

Policy/Procedure:

1. Each EAS Participant must assign each of its Users a role and the Panel(s) they will have access to.
2. Users may be assigned more than one role.
3. The Portal Roles are set forth below along with the associated access rights:
    a. *Portal Participant Point of Contact (POC)*: An individual employed or contracted by an EAS Participant who has been identified as the primary point of contact between Ai and that Portal Participant.
    b. *Portal User*: An individual who is employed or contracted by an EAS Participant and who is authorized by that EAS Participant to access information through Prompt.

Responsibility: Ai; EAS Participants and EAS Participant Users

EAS	Operational Policy for EAS Portal	Policy No: **PORT-3**
Title: **Portal Password Management**	Version: **1.1**	Effective Date:

Purpose Statement: To prevent unauthorized access to and use of Prompt, Ai requires EAS Participant Users to take appropriate measures to select and secure passwords.

Policy/Procedure:

1. All EAS Participant Users will be given a username and password that allows them to access Prompt.
2. When an EAS Participant User logs-on to Prompt for the first time, he/she will be prompted to change the initial, temporary password provided to him/her by Ai.
3. All passwords must comply with the following requirements:
    a. Must be at least 8 characters long;
    b. Password cannot be same as old password if changing password;
    c. User is locked out after 5 failed attempted logins; and
    d. Password must have one non-letter or digit character.

Responsibility: EAS Participant and EAS Participant Users