

Alaska eHealth Network: Network Responsibilities

TABLE OF CONTENTS

RULE 100: COMPLIANCE WITH LAW AND POLICY 7

RULE 200: NOTICE OF PRIVACY PRACTICES 9

RULE 300: INDIVIDUAL CONTROL OF INFORMATION AVAILABLE THROUGH THE SYSTEM
..... 10

RULE 400: ACCESS TO AND USE AND DISCLOSURE OF INFORMATION 13

RULE 500: INFORMATION SUBJECT TO SPECIAL PROTECTION 16

RULE 600: MINIMUM NECESSARY..... 18

RULE 700: WORKFORCE, AGENTS, AND CONTRACTORS 20

RULE 800: AMENDMENT AND STORAGE OF DATA 22

RULE 900: REQUESTS FOR RESTRICTIONS 23

RULE 1000: MITIGATION 24

RULE 1100: INVESTIGATIONS; INCIDENT RESPONSE SYSTEM 25

RULE 1200: AUTHORIZED USER CONTROLS 27

INTRODUCTION

The following rules apply to the access, use and disclosure of protected health information by Participants through the AeHN Health Information Exchange ("HIE") and other data exchange services being made available to Participants in AeHN (the HIE and other services are collectively referred to as the "System").

AeHN has modeled its Network Responsibilities on the Nebraska Health Information Initiative Privacy Rules, and the Connecting For Health "Model Privacy Rules and Procedures for Health Information Exchange," with a number of differences based on state law, physical and technical safeguards available through AeHN, and AeHN's unique operating environment. Thank you to those organizations for their knowledge and expertise in this area. These core privacy principles and the rules that flow from them promote balance between consumer control of and access to health information and the operational need of covered entities to ensure that information uses and disclosures are not overly restricted, such that consumers would be denied many of the benefits and improvements that information technology can bring to the health care system. The rules are intended to reflect a carefully balanced view of all of the principles and avoid emphasizing some over others in any way that would weaken the overall approach.

The guiding AeHN privacy principles are as follows:

- Openness and Transparency. Clarity about procedures, policies, developments, and technology concerning the handling of protected health information is vital to protecting privacy. Individuals should be able to understand what information exists about them, how the personal information is used, and how they can control use of that information.
- Purpose Specification and Minimization. Access to and use of patient health information must be limited to the type and amount necessary to accomplish specified permitted purposes. Minimizing the use of patient health information will help decrease the amount of privacy violations, which may occur when data is collected for one legitimate reason and then reused for different or unauthorized purposes.
- Disclosure Limitation. Personal health information should be made available through the AeHN System to Participants only by lawful means. Electronic collection of protected information may be confusing to most individuals. Individuals should be educated about the potential health and treatment benefits as well as risks to their protected health information that are associated with participation in the System. Individuals deciding not to participate should have the opportunity to know the System-wide effect of such decision and the potential disadvantages.

- Access and Use Limitation. Personal health information should be obtained by one Participant from the System only pursuant to mutual agreement (included in the Participant Agreement) that the information is being accessed for qualifying purposes of the requesting Participant. Information recipients may use and disclose protected health information obtained through the System only for purposes and uses consistent with the Participant Agreement and consistent with their obligations as covered entities under HIPAA. Certain exceptions, such as for law enforcement or public health, may warrant reuse of information for other purposes. However, when information obtained by a Participant through the System is used for purposes other than those for which the information was originally obtained from the System, the Participant so using or disclosing the information should first apply the rules applicable to it as a covered entity under HIPAA and as a contracting Participant.
- Individual Participation and Control. Consistent with the scope of individual rights in HIPAA, individuals should have the right to request and receive in a timely and intelligible manner information regarding various parties that may have that individual's specific health information. Individuals have a vital stake in personal protected health information, such rights enable individuals to make informed decisions about participation and provide another means to monitor for inappropriate access, use and disclosure of protected health information. Individual participation promotes information quality, privacy, and confidence in privacy practices.
- Data Integrity and Quality. Health information should be detailed, complete, appropriate, and current to guarantee its value to the various parties. The effective delivery of quality health care depends on complete health information. Therefore, the System must maintain the integrity of protected health information and individuals must be allowed to view information about them and request to amend such health information so that it is accurate and complete.
- Security Safeguards and Controls. In an era of increased computer and Internet-related crime, security safeguards are vital to privacy protection. Electronic environments could be susceptible to cyber-crime without adequate controls. Such controls are put in place to prevent information loss, corruption, unauthorized use, modification, and disclosure. Safeguards that can be implemented include information scrubbing, identity management tools, hashing, auditing, authenticating, and other means to ensure information privacy. Privacy and security safeguards should be coordinated for the protection of patient health information.
- Accountability and Oversight. Privacy protections have less value to an individual if privacy violators are not held accountable for failing to follow procedures relating to such privacy protections. Participants are unlikely to fully trust the System and fully participate if they believe other Participants are not applying the same rules and being held to the same standard of

accountability. User and workforce training, privacy audits, and other oversight tools can help to identify and address privacy violations and security breaches by conditioning participation and access authority on compliance with these and the individual Participant's privacy policies, by excluding from participation those who violate privacy requirements, and by identifying and correcting weaknesses in privacy and security safeguards.

- Remedies. To ensure privacy protection there must be legal and financial remedies that hold violators accountable for failing to comply with System policies. Such remedies will give individuals confidence in the organization's commitment to keeping protected health information private, and mitigate any harm that privacy violations may cause individuals. As a condition of continued participation, all Participants in the System must have a common duty to participate in investigation, mitigation and remediation steps for the integrity of the System.
- Reliance on Covered Entity Rules and Enforcement. While AeHN should have a number of core policies and procedures for the benefit and confidence of all Participants, AeHN should not try to replace policies, procedures and methods already adopted by Participants as covered entities under HIPAA. AeHN should identify, disseminate and enforce only those policies and procedures necessary for coordination of privacy breach response and other mitigating measures, but should recognize that existing Participant policies govern in all other areas.

These principles underlie the AeHN privacy policies. Given the level of technology available to organizations, a majority of the policies should be relatively manageable. In some cases, however, organizational and technical barriers may restrict an organization's ability to implement the policies.

The creation of a health information exchange will provide for more efficient and effective delivery of patient care. However, the creation of a network that includes a large volume of protected health information must have adequate privacy and security measures. The Network Responsibilities seek to achieve a balance between maintaining the confidentiality of health information and maximizing the benefits of such information.

STATUS OF AEHN AND PARTICIPANTS

Participants – those which provide data to the System and those which access and use data from the System – currently consist of health care providers. At some point in the future, the Participants may also include patients, health plans and health care clearinghouses. These Network Responsibilities may be updated at that time, upon changes in the law and from time to time based on the recommendation and approval of relevant AeHN workgroups. All Participants are covered entities under HIPAA. AeHN is a business associate ("BA") of the Participants. AeHN accepts and agrees to follow terms applicable to the

privacy of protected health information by virtue of its Participant Agreement with each Participant and these Network Responsibilities.

EFFECT OF LEGISLATION AND RULE CHANGES

AeHN and Participants need to remain flexible in order to adapt to the uncertainty of state and federal legislation and regulations that will affect design, safeguards, rights and responsibilities over time. This shall include monitoring and implementing design components and safeguards mandated in HIPAA and the Health Information Technology for Economic and Clinical Health Act or “HITECH” as enacted in P.L 111-5 and regulations to be issued thereunder. These Network Responsibilities currently do not address protections under 42 CFR Part 2 (Substance Abuse) or the Family Educational Rights and Privacy Act, as those laws are not currently applicable to the information in the System or the proposed uses and disclosures through the System.

SAFEGUARDS IN AN ELECTRONIC NETWORKED ENVIRONMENT

HIPAA permits covered entities that hold protected health information to disclose such information to other covered entities both for their own treatment and payment purposes and for the treatment and payment purposes of such third parties, without written authorization. HIPAA limits authority to disclose without authorization in other situations and attaches conditions. HIPAA thus places a duty on Participants holding protected health information to determine that each proposed disclosure is permitted. In an electronic environment, such as the HIE, the disclosing Participant will not receive or “process” a request for access. Other Participants using the HIE can simply locate the Participant’s record and access it as needed. The human element of analyzing individual requests is absent. See 45 C.F.R. §164.506(c)(3) and (4).

Accordingly, to permit Participants that furnish information to meet their obligation to disclose protected health information only for a qualifying purpose, and to meet certain other conditions, AeHN and Participants have placed the burden on the requesting Participant to access information from another Participant’s records only for a qualifying use by the requesting Participant. A qualifying use is one that meets the terms of the Participant Agreement and would permit the Participant from whose records the information is accessed to disclose such information to the requesting Participant under §164.506(c)(2) and (3) of the Privacy Rule.

To support this approach, AeHN and the Participants have implemented the following administrative safeguards:

- All Participants must be covered entities under HIPAA, or otherwise subject to HIPAA, and therefore individually subject to regulation and penalties.
- All Participants commit to accessing PHI only for the purposes outlined in the Participant Agreement.

AeHN Rule 100: Compliance with Law and Rule

Scope and Applicability: This Rule applies to AeHN and all Participants.

Rule:

1. Laws. Each Participant must, at all times, comply with all federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of protected health information and establishing certain individual privacy rights. Each Participant must use reasonable efforts to stay up-to-date of any changes or updates to and interpretations of such laws and regulations to ensure compliance.
2. Network Responsibilities. Each Participant shall, at all times, comply with these AeHN Network Responsibilities ("Network Responsibilities"). These Network Responsibilities may be changed and updated from time to time upon reasonable written notice to Participants. Amendment shall be effective when adopted by the AeHN Board of Directors, ordinarily following input by the AeHN Legal Workgroup and any other relevant workgroups. AeHN shall notify Participants of all rule changes and shall post the most current version of the Network Responsibilities on its website. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these Network Responsibilities.
3. Participant Rules. Each Participant is responsible for establishing internal policies that are necessary to comply with applicable laws and these Network Responsibilities. As stated in the Participant Agreement, AeHN may request a copy of these policies for its review and reference.
4. Participant Criteria. Each Participant shall itself be a HIPAA "covered entity" and thus subject to both its individual legal duty as a regulated covered entity under HIPAA and its contractually assumed obligations under its Participant Agreement. Each Participant must agree to be a data provider in order to become a data user.
5. User Criteria. Authorized users are individuals who have been granted access authority. Each authorized user derives his or her permission to access and use the System from a Participant. Therefore each authorized user must maintain a current relationship to a Participant in order to use the System. Authorized users must therefore be: (i) Participants (for example, an individual physician) or workforce of a Participant, (ii) an individual BA or workforce of such BA, or (iii) an individual contractor or subcontractor of a BA or workforce of such contractor or subcontractor. The Participants acknowledge the need to revise Rules and certain other technical and administrative features to conform to HIPAA, HITECH and regulations to be promulgated thereunder. These changes will be made as necessary.

6. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

7. Participant Agreement Controls. If anything in these Rules shall conflict with the Participant Agreement, the terms of the Participant Agreement shall control.

8. Use of System Equipment, Programs and Information. Participants shall not use any equipment, programs or information associated with the System, whether supplied by AeHN, a Participant or a third-party, to interfere in any way with the operation of the System.

AeHN Rule 200: Notice of Privacy Practices

Scope and Applicability: This Rule applies to all Participants.

Rule: 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 the System, if such a use and disclosure is not already addressed in the Notice.

1. Content. 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 the System. AeHN 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 and health plans 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." Participants may elect more stringent language, but may not commit AeHN to any additional obligations or liabilities through the Notice.

2. Dissemination and Individual Awareness. Each Participant shall have its own policies and procedures governing distribution of the Notice to individuals, and, where applicable, acknowledgment of receipt by the individual, which policies and procedures shall comply with applicable laws and regulations.

3. Participant Choice. Participants may choose a more proactive Notice distribution or patient awareness process than provided herein and may include more detail in their Notice, so long as any expanded detail does not misstate the safeguards supporting the System. 45 C.F.R. § 164.520(b). See 45 C.F.R. § 164.520(c)(2)(ii).

AeHN Rule 300: Individual Control of Information Available Through the System

Scope and Applicability: This Rule applies to AeHN and all Participants.

Rule:

1. Choice Whether to Have Information Included in the System. All individuals will have the opportunity to opt out of participating in AeHN. A request to opt out will be treated as a request for restrictions on use and disclosure of protected health information. Participants agree to approve such requests, subject to qualifications and limitations as described in the informational brochure referred to below or in these policies.

1.1. Individuals shall be afforded the opportunity to exercise this choice at the time of any service at a Participant that is a health care provider or thereafter through a uniform "opt-out" process.

1.2. AeHN will, from time to time, furnish Participants that are health care providers with an informational brochure about the System for distribution to individuals and for use in explaining the meaning and effect of participation or opting out. Participants may customize the informational brochure as they deem appropriate to fit their circumstances, so long as AeHN does not incur any additional obligations or liabilities as a result. The brochure will also contain a link to the AeHN website where AeHN will provide an explanation of the meaning and effect of participation or opting out and a tool for opting out or revoking a prior opt-out election. The AeHN website will also include information about the current participating entities, and the types and format of information that participants can obtain through the HIE.

1.3. The brochure shall explain the System-wide scope of an opt-out decision, the risks to the individual's data privacy and security if the individual participates including a list of the ways in which the information may be used, the effect and benefits of participation, and the effect and disadvantages of opting out. The brochure will explain that a Participant's policies continue to govern access, use and disclosure in all other contexts.

1.4. The brochure shall state that the Participant (and other Participants) will not withhold coverage or care from an individual on the basis of that individual's choice not to have information about him or her included in the System.

1.5. Participants shall furnish the brochure to individuals at the initiation of an episode of care, as determined by the Participant, and note for each individual the opportunity to opt-out or ask

questions. Each Participant will have one or more persons designated to answer questions about the System or about opting out or revoking a prior opt-out election.

1.6. Participants may also direct individuals to the AeHN website and to AeHN, where the individual can ask additional questions and obtain additional information about participation in AeHN and opt-out. AeHN as a business associate of the Participants is authorized to provide information and answer individual questions about AeHN and the opt-out alternatives on behalf of Participants.

1.7. Participants that provide only limited information through the System and have limited or no face-to-face contact with individuals shall provide a description of the System, an explanation of the right to opt out, a link to the AeHN website and a phone number individuals can use to obtain additional information about the System, insurer access, and the right to opt out in their patient documentation and otherwise as they determine necessary.

1.8. An individual's election to opt out of participation in the System shall be communicated to AeHN in the manner provided by AeHN and be of System-wide effect once so communicated and processed.

2. Change to Prior Election. An individual may opt out or revoke a prior election to opt out at a later date. The brochure and information on the AeHN website should inform the individual that withdrawing a prior opt-out election will result in information that was previously unavailable through the System becoming available to all Participants using the System.

3. Effect of Choice. An individual who completely opts out of the System opts out as to all of his or her records made available through the System, not just with respect to a particular Participant or episode of care. The effect is System-wide. An individual who opts out of the System for regular treatment, but allows access for emergency purposes will have information remain in the system, but will only allow access after certain emergent circumstances are presented. An individual's election to opt out, whether made at the time of service or subsequently, will have prospective effect only and will not impact access, use and disclosure occurring before the decision is received and communicated through the System.

4. Limited Effect of Opt-Out. A decision to opt out only affects the availability of the individual's protected health information through the System. Each Participant's policies continue to govern access, use and disclosure in all other contexts and via all other media.

5. Documentation. Each Participant shall document and maintain documentation that information about the System and about the ability to opt out of the System has been provided to the Participant.

6. Participant's Choice. Participants shall develop and implement the necessary processes to allow an individual to choose not to have information about him or her included in the System. The uniform processes described in this Rule are not exclusive, and Participants may adopt additional, not inconsistent, mechanisms.

7. Provision of Coverage or Care. A Participant shall not withhold coverage or care from an individual on the basis of that individual's choice to opt out.

8. Reliance. Participants will be entitled to assume that an individual has not opted-out if the individual's protected health information is available through the System.

AeHN Rule 400: Access to and Use and Disclosure of Information

Scope and Applicability: This Rule applies to AeHN and all Participants.

Rule:

1. Compliance with Law. Participants shall access, use and disclose protected health information through AeHN only in a manner consistent with all applicable federal, state, and local laws and regulations and not for any unlawful or discriminatory purpose.
2. Documentation and Reliance. If applicable law requires that certain documentation exist or that other conditions be met prior to disclosing protected health information for a particular purpose (such as consent to release substance abuse information), the requesting institution shall ensure that it has obtained the required documentation or met the requisite conditions. Each access and use of protected health information by a Participant is a representation to every other Participant whose protected health information is being accessed and used that all prerequisites under state and federal law for such disclosure by the disclosing Participant have been met.
3. Purposes. A Participant may request and use protected health information through the System only for the Participant's purposes, and only to the extent necessary and permitted by applicable federal, state, and local laws and regulations and these Rules. A Participant may request and use protected health information through the System only if the Participant has or has had or is about to have the requisite relationship to the individual whose protected health information is being accessed and used. The requisite relationships include, but are not limited to, the primary care provider for each patient and other providers in a treatment relationship with the patient. A list of the types of persons who can qualify to have the requisite relationship will be contained on the AeHN website. The permissible purposes under the Participant Agreement are as follows:
 - a. Treatment of a patient of or by Participant (as defined by HIPAA).
 - b. Payment for healthcare services (as defined by HIPAA).
 - c. Healthcare Operations (as defined by HIPAA).
 - d. Mitigation of a breach of confidentiality (as defined in the AeHN Breach Disclosure Policy) or unauthorized access of PHI.
 - e. Auditing and monitoring compliance of Participant's Users with the terms and conditions of this Agreement.
 - f. Providing information as required by law or regulation.

4. Prohibitions. Information may not be requested for marketing or marketing related purposes without specific patient authorization. Under no circumstances may information be requested for a discriminatory purpose. In the absence of a permissible purpose, a Participant may not request or access information through the System.

5. Participant Rules. Each Participant shall reference and maintain compliance with its own internal policies and procedures regarding disclosures of protected health information and the conditions that shall be met and documentation that must be obtained, if any, prior to making such disclosures. See 45 C.F.R. § 164.530(j). 45 C.F.R. § 164.502(a), (b). 45 C.F.R. § 164.502(b). In the event that Participant's internal policies and procedures conflict with these Network Responsibilities or the Participant Agreement, the provision that provides for greater privacy and security of protected health information shall govern.

6. Subsequent Use and Disclosure. A Participant that has accessed information through the System and merged the information into its own record shall treat the merged information as part of its own record and thereafter use and disclose the merged information only in a manner consistent with its own information privacy policies and laws and regulations applicable to its own record. A Participant shall not access protected health information through the System for the purpose of disclosing that information to third parties, other than for the Participant's qualifying treatment and payment purposes.

7. Accounting of Disclosures. Each Participant shall be responsible to account only for its own disclosures. All requests for an accounting of disclosures will be forwarded back to the Participants to address for their respective patients.

8. Audit Logs. AeHN shall develop an audit log capability to document which Participants posted and accessed the information about an individual through the System and when such information was posted and accessed.

9. Authentication. AeHN shall follow a uniform authentication requirement for verifying and authenticating the identity and authority of each authorized user and Participant. Participants shall be entitled to rely on AeHN's user access and authorization safeguards and may be assured an authorized user making a request for protected health information on behalf of another Participant is authorized to do so. Participants shall be responsible for their own authorized users and ensuring that their own authorized users are appropriately authorized and accessing information.

10. Access. Each Participant should have a formal process through which it permits individuals to view information about them that has been posted by the Participant to the System. For HIPAA Covered Entities, this is currently required by law. See 45 C.F.R. §§ 164.316, 164.308(a)(1)(i). See 45 C.F.R. §§

164.514(h), 164.312(d). See Connecting for Health, "Authentication of System Users." See 45 C.F.R. § 164.524. This capability will not be available at the AeHN launch date.

11. Application to BAs and Contractors. Participants shall make this rule applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

AeHN Rule 500: Information Subject to Special Protection

Scope and Applicability: This Rule applies to AeHN and all Participants.

Rule:

1. Special Protection. The System and these policies are geared to the HIPAA level of privacy. Some health information may be subject to special protection under federal, state, and/or local laws and regulations. Other health information may be deemed so sensitive that a Participant has made special provision to safeguard the information, even if not legally required to do so. Each Participant shall be responsible to identify what information is legally subject to special protection under applicable law and what information (if any) is subject to special protection under that Participant's policies, prior to disclosing any information through AeHN. Participants should not make protected health information requiring special protection available to the System. Each Participant is responsible for complying with laws and regulations and its own policies in regard to identifying and providing special treatment for information needing special protection. AeHN has worked with the HIE system provider to filter certain sensitive codes and diagnoses, but this filter cannot be relied upon by Participants to remove all sensitive information.

2. Information Not Furnished. For System data to be useful, the Participant using it must know if it is complete or whether certain information would be withheld due to more stringent state and federal law or Participant policies.

2.1. Accordingly, Participants accessing and using another Participant's information obtained through the System may act with the understanding that the information made available would not include any of the following:

(a) Alcohol and substance abuse treatment program records subject to 42 CFR Part 2;

(b) Records of emergency protective custody proceedings;

(c) HIV testing information;

(d) Certain records of minors if under state law only the minor's consent to treatment is needed, the minor has consented to the care, but the minor is not the party electing not to opt out. In Alaska, this may include, but is not limited to the following records:

- Records of STD testing and treatment (including HIV testing);

- Diagnosis and treatment of suspected abuse by a parent, guardian or personal representative; and
- Provision of birth control and other reproductive treatment.

(e) Records of mental health treatment centers.

2.2. This list is suggestive only. Other records may be added to the list. Data recipients are not entitled to rely on records being inclusive of the above listed records.

3. Application to Business Associates and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

AeHN Rule 600: Minimum Necessary

Scope and Applicability: This Rule applies to AeHN, all Participants and their BAs and contractors.

Rule:

1. Requests. Each Participant shall request only the minimum amount of health information through the System as is necessary for the intended purpose of the request. However, in some cases, a standard set of information will be received in return for a limited request, due to the technical limitations of the System. When this occurs, Participant will not be deemed to be in violation of this Rule.
2. Disclosures. A Participant is entitled to rely on the scope of a requesting Participant's request for information as being consistent with the requesting Participant's minimum necessary policy and needs.
3. Workforce, BAs and Contractors. Each Participant shall adopt and apply policies to limit access to the System to members of its workforce who qualify as authorized users and only to the extent needed by such authorized users to perform their job functions or duties for the Participant.
4. Entire Medical Record. A Participant shall not use, disclose, or request an individual's entire medical record unless necessary and justified to accomplish the specific purpose of the use, disclosure, or request.
5. Application to Providers and Treatment Purposes. While this minimum necessary policy is not required by HIPAA for providers accessing, using and disclosing health information for treatment purposes, they are encouraged to follow it when consistent with treatment needs.
6. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

AeHN Rule 700: Workforce, Agents, and Contractors

Scope and Applicability: This Rule applies to AeHN and all Participants and their BAs and contractors.

Rule:

1. Participant Responsibility. Each Participant is responsible to establish and enforce policies designed to comply with its responsibilities as a covered entity under HIPAA and a Participant in the System, and to train and supervise its authorized users, to the extent applicable to their job responsibilities. Training shall include, but not be limited to, the requirements of these Rules, the Participant Agreement, and applicable law governing the confidentiality, privacy and security of protected health information, such as HIPAA. All such training will be conducted at the sole cost of Participant prior to any access to the System by authorized users.
2. Authorized Users. All authorized users, whether members of a Participant's workforce or member of the workforce of a BA or contractor, shall execute an individual user agreement and acknowledge familiarity with and acceptance of the terms and conditions on which their access authority is granted. This shall include familiarity with applicable privacy and security policies of the Participant, BA, or contractor, as applicable. Participants shall determine to what extent members of their workforce or the workforce of BAs and contractor require additional training on account of the Participant's obligations under their Participant Agreement and these policies, and arrange for and document such training. AeHN shall reserve authority in the Participant Agreement to suspend, limit or revoke access authority for any authorized user or Participant for violation of Participant and/or AeHN privacy and security policies.
3. Access to System. Each Participant shall allow access to the System only by those authorized users who have a legitimate and appropriate need to use the System and/or release or obtain information through the System. No workforce member, agent, or contractor shall have access to the System except as an authorized user on behalf of a Participant and subject to the Participant's privacy and security policies and procedures and the terms of the individual's user agreement.
4. Discipline for Non-Compliance. Each Participant shall disciplinary policies to hold authorized users, BAs and contractors accountable for following the Participant's policies and procedures and for ensuring that they do not use, disclose, or request health information except as permitted by these Rules. Examples of disciplinary measures include, but are not be limited to, verbal and written warnings, demotion, and termination and may provide for retraining in certain circumstances.

5. Reporting of Non-Compliance. Each Participant shall have a procedure, and shall encourage all workforce members, BAs and contractors to report any noncompliance with the Participant's policies or the policies applicable to authorized users. Each Participant also shall establish a mechanism for individuals whose health information is included in the System to report any non-compliance with these Rules or concerns about improper disclosures of protected health information.

6. Enforcing BAAs and Contractor Agreements. Each Participant shall require in any relationship with a BAs, contractor, or other third party (which may include staff physicians) that will result in such third party becoming an authorized user on behalf of the Participant, or that will result in members of the workforce of such third party becoming an authorized user on behalf of the Participant, that: (i) such third party and any member of its workforce shall be subject to these Rules when accessing, using or disclosing information through the System; (ii) that such third parties and/or authorized users on its workforce may have their access suspended or terminated for violation of these Rules or other terms and conditions of the authorized user agreement; and (iii) that such third party may have its contract with the Participant terminated for violation of these Rules or for failure to enforce these policies among its workforce. See 45 C.F.R. § 164.530(a), (d).

AeHN Rule 800: Amendment and Storage Of Data

Scope and Applicability: This Rule applies to AeHN and all Participants.

Rule:

1. Accepting Amendments. Each Participant shall comply with applicable federal, state and local laws and regulations regarding individual rights to request amendment of health information. Only the Participant responsible for the record being amended may accept an amendment. If one Participant believes there is an error in the record of another Participant, it shall contact the responsible Participant.
2. Informing Other Participants. A Participant shall notify AeHN using a method established by AeHN for such purpose when it has amended an individual's protected health information via a mechanism developed by AeHN. AeHN shall cooperate in identifying other Participants who have accessed the information in its pre-amendment form, to the extent reasonably possible. Participants shall also notify AeHN of data errors reported to it by patients or providers that cannot be lawfully amended through the automated transmission of an update or amendment from the Participant's electronic system.
3. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements. 45 C.F.R. § 164.526.
4. Data Backup. Participants shall not hold AeHN responsible for protecting and backing up the source data used in connection with or furnished for processing by the System, unless expressly agreed upon pursuant to the Participant Agreement. AeHN will perform backups as required to comply with HIPAA and its obligations to Participants, but Participants should not rely upon this backup for its own data.

AeHN Rule 900: Requests For Restrictions

Scope and Applicability: This Rule applies to all Participants.

Rule:

1. Recipient Responsibility. A Participant, when accessing data as a data recipient, shall not be expected to know of or comply with a restriction on use or disclosure agreed to by a Participant that provides data.
2. Data Provider Responsibility. If a Participant agrees to an individual's request for restrictions, as permitted under the HIPAA Privacy Rule, such Participant shall ensure that it complies with the restrictions. This shall include not making the individual's information available to the System, including opting the individual out of the System, if required by the restriction. Participants should advise individuals that opting out only affects access, use and disclosure of their protected health information through the System. When evaluating a request for a restriction, the Participant shall consider the implications that agreeing to the restriction would have on the accuracy, integrity and availability of information through the System.

AeHN Rule 1000: Mitigation

Scope and Applicability: This Rule applies to AeHN, all Participants and their BAs and contractors.

Rule:

1. Duty to Mitigate. Each Participant shall implement a process to mitigate, and shall mitigate to the extent practicable, the harmful effects that are known to the Participant of an access, use or disclosure of protected health information through the System that is in violation of applicable laws and/or regulations and/or these Rules and that is caused or contributed to by the Participant or its workforce members, agents, and contractors. Steps to mitigate could include, but are not limited to, Participant notification to the individual or Participant request to the party who improperly received such information to return and/or destroy impermissibly disclosed information.
2. Duty to Cooperate. A Participant that has caused or contributed to a privacy breach or that could assist with mitigation of the effects of such breach shall cooperate with AeHN and with another Participant that has the primary obligation to mitigate a breach in order to help mitigate the harmful effects of the breach. This obligation exists whether the Participant is directly responsible or whether the breach was caused or contributed to by members of the Participant's workforce or by its BAs or contractor or their workforce.
3. Notification to AeHN. A Participant primarily responsible to mitigate shall notify AeHN of all events requiring mitigation and of all actions taken to mitigate. AeHN may facilitate the mitigation process if asked. AeHN shall attempt to use examples of breaches and mitigation steps for education and for policy and other safeguard development.
4. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

AeHN Rule 1100: Investigations; Incident Response System

Scope and Applicability: This Rule applies to AeHN, all Participants and their BAs and contractors.

Rule:

1. Duty to Investigate. Each Participant shall promptly investigate reported or suspected privacy breaches implicating privacy or security safeguards deployed by AeHN (or its contractors), or involving unauthorized access, use or disclosure of the System, according to its own policies. Upon learning of a reported or suspected breach, the Participant shall notify AeHN and any other Participant whom the notifying Participant has reason to believe is affected or may have been the subject of unauthorized access, use or disclosure. AeHN shall have the right to participate in the investigation and to know the results and remedial action, if any, taken, except that AeHN need not be notified of specific workforce disciplinary actions. Each investigation shall be documented. At the conclusion of an investigation, a Participant shall document its findings and any action taken in response to an investigation. A summary of the findings shall be sent to AeHN. AeHN shall attempt to use examples of breaches for education and for policy and other safeguard development.

2. Incident Response. AeHN shall implement an incident response system in connection with known or suspected privacy breaches, whether reported by Participants or discovered by AeHN. The incident response system shall include the following features, each applicable as determined by the circumstances:

2.1 Cooperation in any investigation conducted by the Participant or direct investigation by AeHN;

2.2 Notification of other Participants or authorized users as needed to prevent further harm or to enlist cooperation in the investigation and/or mitigation of the breach;

2.3 Cooperation in any mitigation steps initiated by the Participant;

2.4 Furnishing audit logs and other information helpful in the investigation;

2.5 Developing and disseminating remediation plans to strengthen safeguards or hold Participants or authorized users accountable;

2.6 Any other steps mutually agreed to as appropriate under the circumstances; and

2.7 Any other step required under the incident reporting and investigation system contained in the AeHN Security Rules.

3. AeHN Cooperation. AeHN shall cooperate with a Participant in any investigation of the Participant's privacy and security compliance, whether conducted by an agency of state or federal government or conducted as a self-investigation by the Participant, when the investigation implicates AeHN conduct, or the conduct of another Participant or authorized user, or the adequacy or integrity of System safeguards.

4. Participant Cooperation. Each Participant shall cooperate with AeHN in any investigation of AeHN or of another Participant into AeHN's or such other Participant's privacy and security compliance, whether conducted by an agency of state or federal government or conducted as a self-investigation by AeHN or the other Participant, when the investigation implicates such Participant's compliance with Network Responsibilities or the adequacy or integrity of System safeguards.

5. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

AeHN Rule 1200: Authorized User Controls

Scope and Applicability: This Rule applies to AeHN, all Participants and their BAs and contractors.

Rule:

1. Participant Responsibilities. Each Participant is responsible to:

1.1 Designate its responsible contact person who shall be initially responsible on behalf of the Participant for compliance with these policies and to receive notice on behalf of the Participant. For Participants that have their own system administrator, this shall ordinarily be the system administrator.

1.2 Designate its own authorized users from among its workforce, and designate BAs and contractors authorized to act as (or designate from among their workforce) authorized users on its behalf. A list of these authorized users, along with the dates of authorization (and termination, if applicable) shall be made available to AeHN on a quarterly basis, or upon reasonable advanced written notice by AeHN.

1.3 Train and supervise its authorized users and require any BA or contractor to train and supervise its authorized users consistent with the Participant's and AeHN's privacy policies and with the terms of the Participant's privacy policies and the BA Agreement as applicable.

1.4 In the case of Participants with a System Administrator, suspend, limit or revoke access authority as soon as possible upon a change in job responsibilities or employment status of an authorized user. Revocation shall occur prior to, contemporaneously with, or immediately following such a change so as to prohibit continued access authority for individuals who no longer need it on behalf of the Participant. Participant's list of authorized users should be updated to reflect such change.

1.5 For Participants without their own System Administrator, immediately notify AeHN of the change so that AeHN may revoke access authority. Notification shall occur prior to, contemporaneously with, or immediately following such a change so as to prohibit continued access authority for individuals who no longer need it on behalf of the Participant.

1.6 Hold their authorized users accountable for compliance with AeHN and the Participant's policies and, as applicable, the terms of any BA Agreement. Participant is solely responsible under this Agreement for all acts and omissions of Participant and/or Participant's users who

access the Network either through Participant or by use of any password, identifier or log-on received or obtained, directly or indirectly, lawfully or unlawfully, from Participant or any of Participant's authorized users, with respect to the System, the System services and/or any confidential and/or other information accessed in connection therewith.

2. AeHN Responsibilities. AeHN is responsible to:

2.1 Grant access authority to individuals designated by a Participant, subject to reserved authority to suspend, limit, or revoke such access authority as described later.

2.2 Train and supervise its own authorized users on these policies and the standard terms required by its BA Agreement with Participants.

2.3 Suspend, limit or revoke access authority for its own authorized users or any authorized user who is a member of the workforce of any subcontractor of AeHN as required by these policies or the terms of its BA Agreement in the event of breach or non-compliance.

2.4 Immediately revoke access authority upon a change in job responsibilities or employment status of its own authorized users or the authorized user of its contractor.

2.5 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 privacy policies, Network Responsibilities or the terms of the user agreement, if AeHN determines that doing so is necessary for the privacy of individuals or the security of the System.

2.6 Monitor access and notify Participants if a user may not have used the system for a prolonged period of time, or if AeHN notices any other reason to review an authorized user's access for potential suspension or termination.

3. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

4. Denial of Access. Participants should be aware that individuals may be denied access to the System based on past performance or behavior reported by a former employer or other participating entity.

AeHN Rule 1300: Sanctions

Scope and Applicability: This Rule applies to AeHN, all Participants and their BAs and contractors.

Rule:

1. Participant Responsibilities. Each Participant is responsible to:

1.1 Implement policies and procedures to sanction and hold authorized users, workforce members, agents and contractors accountable for failure to comply with any internal policies and procedures set by the Participant with regard to the use, disclosure or access of protected health information accessed through the System.

1.2 Implement policies and procedures to sanction and hold authorized users, workforce members, agents and contractors accountable for ensuring that they do not use, disclose or access protected health information except as permitted by the Participant Agreement and these Network Responsibilities.

1.3 Such sanctions may include, but need not be limited to, verbal and written warnings, required retraining, suspension or termination of access to the System, suspension of employment without pay, and termination of contract or employment.

1.4 Notify AeHN in writing of the name of individual, date and nature of violation (as well as action taken to remedy) of security violations.

2. AeHN Responsibilities. AeHN is responsible to:

2.1 Impose sanctions on AeHN personnel who are determined to have failed to adhere to AeHN Privacy and Security Policies. Such sanctions shall be imposed and enforced in accordance with AeHN's Employee Sanction Policy and may include, but not be limited to, verbal or written warnings, required retraining, suspension without pay, and termination of contract or employment.

2.2 Upon receiving a report, discovering or being notified of a reportable event from a Participant, AeHN shall coordinate with the affected Participant to determine if the appropriate sanctions have been imposed by the Participant. If AeHN's privacy and security officer determines that further action is necessary, AeHN shall impose one or more additional sanctions, consistent with the violation. Depending on the circumstances, sanctions may be on an individual authorized user level or a Participant level.

2.3 Upon receiving a report, discovering or being notified of a reportable event that cannot be attributed directly to any one Participant, AeHN shall impose one or more sanctions on the identified offender, consistent with the violation. Sanctions for an unintentional violation may include, but are not limited to: verbal warnings; written warnings; suspension of access privileges; and revocation of access privileges. Sanctions for an intentional violation may include, but are not limited to: immediate suspension of access; revocation of access; a complaint filed with the violator's professional licensing board, if the violator is professional licensed; information turned over to a prosecutor for criminal prosecution; and potential other legal action.

2.4 Create a database or other resource to verify if a prospective authorized user has been sanctioned previously or has had a complaint filed against them for a potential security violation.

3. Appeals. Persons who are sanctioned by AeHN, or who otherwise have their privileges limited, may appeal the sanctions or limitation to AeHN. Appeals must follow the following guidelines:

3.1 Appeals must be filed in writing and received at AeHN's offices within 10 business days of the sanction being imposed.

3.2 AeHN staff will consider the appeal and make a determination of whether to continue the sanction within 10 business days of receiving the written appeal.

3.3 AeHN will provide the party filing the appeal with a written notice of its decision within 10 business days of making the decision. Sanctions will remain in effect while the appeal is being considered.

3.4 If the appeal is denied, and the appealing party believes there has been an error, it may file a request with AeHN for an external review. Such requests must be made in writing within 30 calendar days of the appeal being denied. AeHN will refer the case to an independent party, which will review the evidence and make a recommendation to AeHN's board of directors, which will make the final decision.