

Administrative Safeguards

Alaska eHealth Network Policy 2.200

HIPAA Security Rule Language

“Implement policies and procedures to prevent, detect, contain, and correct security violations.”

Policy Summary

Alaska eHealth Network (AeHN) will ensure the confidentiality, integrity and availability of its information systems containing EPHI by implementing appropriate and reasonable policies, procedures and controls to prevent, detect, contain, and correct security violations. AeHN’s administrative safeguards must include a security management program based on formal and regular processes for risk analysis and management, sanction policies for non-compliance, and information system activity review.

All AeHN workforce members are responsible for appropriately protecting EPHI maintained on the Alaska HIE information systems. AeHN management is responsible for ensuring the confidentiality, integrity and availability of all EPHI maintained on the Alaska HIE information systems.

Purpose

This policy reflects AeHN’s commitment to ensure the confidentiality, integrity, and availability of its information systems containing EPHI by implementing policies and procedures to prevent, detect, contain, and correct security violations.

Scope/Applicability

This policy is applicable to all departments that use or disclose EPHI for any purposes. This policy’s scope includes all EPHI.

Regulatory Category, Type, Legal Regulatory Reference

Administrative Safeguards, Standard, AS 18.23.300 et seq.; 45 CFR 164.308(a)

Policy Authority/ Enforcement

AeHN’s Executive Director (ED) and Security and Privacy Officer (SPO) are responsible for monitoring and enforcement of this policy.

Related Procedures

Standard	Number
Security Management Process	2.201
Risk Analysis	2.202
Risk Management	2.203
Employee Sanctions	2.204
Information System Activity Review	2.205
Assigned Security Responsibility	2.206
Work Force Security	2.207
Authorization and/or Supervision	2.208

Administrative Safeguards
AeHN Policy 2.200

Workforce Clearance Procedure	2.209
Termination Procedures	2.210
Information Access Management	2.211
Access Authorization	2.212
Access Establishment and Modification	2.213
Security Awareness and Training	2.214
Security Reminders	2.215
Protecting from Malicious Software	2.216
Log-In Monitoring	2.217
Password Management	2.218
Security Incident Procedures	2.219
Contingency Plan	2.220
Data Backup Plan	2.221

Policy

A. Security Management Process

1. AeHN makes active strides to protect the integrity and confidentiality of EPHI information managed on behalf of provider organizations participating in the statewide health information exchange. These activities include, but are not limited to the use of identity protected storage, network storage, system access logging, physical protections and security, and user education.
2. AeHN actively enforces compliance with HIPAA regulations by utilizing and requiring the use of ‘best practice’ security measures, including, but not limited to, utilizing mandatory network login, strong password discipline, workstation security, protected network storage and physical security.
3. AeHN is committed to ensuring the privacy and security of EPHI that it manages on behalf of its participating provider organizations. In order to manage the facilitation and implementation of activities related to the privacy and security of PHI, AeHN will appoint and maintain an internal SPO position. The SPO will serve as the focal point for security compliance-related activities and responsibilities, as listed in the AeHN policies and procedures.

B. Employee and Workforce Management

1. AeHN workforce members will comply with all applicable AeHN security policies and procedures. Compliance is mandated to ensure the confidentiality, integrity and availability of the Alaska HIE information systems.
2. AeHN workforce members will understand and be aware of all applicable AeHN security policies and procedures. AeHN will provide regular training and awareness for workforce members on AeHN security policies and procedures.
3. AeHN will establish formal, documented procedures for applying appropriate sanctions against workforce members who do not comply with its security policies and procedures.
4. AeHN actively controls EPHI and educates its workforce members in EPHI security by any of the following:

- a. AeHN will demonstrate its commitment to enforce HIPAA regulations and secure EPHI information by establishing a SPO who will be charged with the ongoing process of establishing, maintaining and updating HIPAA rules, policies, procedures and guidelines.
 - b. The AeHN SPO will aggressively enforce HIPAA guidelines and procedures and will actively introduce new procedures in the face of rapidly changing technology.
 - c. The AeHN SPO and workforce members will meet at least semi-annually to audit existing procedures and technology to ensure that HIPAA regulations are being actively enforced.
 - d. The AeHN SPO is responsible for establishing training guidelines for each respective AeHN workforce member specifically with regards to the types and amount of training required to meet HIPAA regulations. Training for each person may be combined and presented in a group setting, or otherwise available in a format deemed appropriate by the SPO.
5. Despite the fact that all AeHN workforce members will not have regular access to or a day-to-day need to handle EPHI, all AeHN workforce members will receive initial and annual training in and will follow baseline information security policies. This will include, but not be limited to, password use and discipline, use of network storage and workstation locking.
 6. The ED and SPO will actively promote and enforce HIPAA policies and procedures to AeHN workforce members.

C. Risk Analysis & Risk Management

1. All AeHN HIPAA procedures must undergo formal risk management auditing at least yearly.
2. AeHN, or an independent 3rd party, shall annually conduct a risk analysis (“Risk Analysis”) that will, at a minimum:
 - a. Identify and prioritize the threats to the Alaska HIE information systems containing EPHI.
 - b. Identify and prioritize the vulnerabilities of the Alaska HIE information systems containing EPHI.
 - c. Identify and define the security measures used to protect the confidentiality, integrity, and availability of the Alaska HIE information systems containing EPHI.
 - d. Identify the likelihood that a given threat will exploit a specific vulnerability on the Alaska HIE information system containing EPHI.
 - e. Identify the potential impacts to the confidentiality, integrity, and availability of the Alaska HIE information systems containing EPHI if a given threat exploits a specific vulnerability.
 - f. Any report compiled will include all statistical and technology references to formulate recommendations.
 - g. Judgments used in AeHN’s Risk Analysis, such as assumptions, defaults, and uncertainties, should be explicitly stated and documented.
3. As appropriate, the AeHN SPO and management will share results of the Risk Analysis with the AeHN Board of Directors and the Audit and Compliance Committee.

4. The AeHN SPO or assigned AeHN workforce member will regularly review records of activity on information systems containing EPHI.

D. Access and Authorization - Internal

1. Individual job descriptions for AeHN workforce members will be the basis for defining access authority and the specific information system content that will be accessible. The nature and extent of access to the Alaska HIE information systems containing EPHI will be based on an ongoing risk analysis process. At a minimum, the risk analysis will consider the following factors:
 - a. The importance of the applications running on the information system
 - b. The value or sensitivity of the EPHI on the information system
 - c. The extent to which the information system is connected to other information systems
2. Access to the Alaska HIE information systems containing EPHI will be authorized only for properly trained AeHN workforce members having a legitimate need for specific information in order to accomplish job responsibilities as defined in individual job descriptions. Job descriptions will be reviewed at least annually to validate necessity of access to some or all EPHI maintained in the Alaska HIE information systems.
3. AeHN workforce members will not access the Alaska HIE information systems containing EPHI for which they have not been given proper authorization. AeHN will ensure that all workforce members who have the ability to access the Alaska HIE information systems containing EPHI are appropriately authorized or supervised. AeHN will maintain a documented process for authorizing appropriate access to the Alaska HIE information systems containing EPHI. This will include:
 - a. A definition of roles based on individual AeHN workforce job descriptions.
 - b. A summary of authorized categories of EPHI content that can be accessed by each role.
 - c. An annual review of roles and authorized categories of access to EPHI to be conducted as part of the ongoing risk analysis process.
4. AeHN workforce members will be screened during the hiring process to identify possible areas of risk which will be vetted before retention in a position that requires access to EPHI. AeHN will sustain a formal, documented process for terminating access to EPHI when the employment of a workforce member ends, or the need to access EPHI otherwise terminates.
5. All AeHN workforce members who access the Alaska HIE information systems containing EPHI will sign a confidentiality agreement in which they agree not to provide or discuss EPHI or confidential information with unauthorized persons. Confidentiality agreements will be reviewed and signed annually by AeHN workforce members who access the Alaska HIE information systems containing EPHI.

E. Access & Authorization – External or Participating Site Workforce Members

AeHN will have a formal, documented process for establishing, documenting, reviewing, and modifying access to the Alaska HIE information systems containing EPHI. The process will be based

on AeHN and the Participating Organizations' access authorization policy. At a minimum, the process must include:

- a. Procedure for establishing different levels of access to the Alaska HIE systems containing EPHI.
- b. Procedure for documenting levels of access established to the Alaska HIE information systems containing EPHI.
- c. Procedure for regularly reviewing AeHN and Participating Organizations workforce member access privileges to the Alaska HIE information systems containing EPHI.
- d. Procedure for modifying AeHN and Participating Organizations workforce member access privileges to the Alaska HIE information systems containing EPHI.
- e. Procedure for terminating AeHN and Participating Organization workforce members' access privileges to the Alaska HIE information systems containing EPHI.

F. Information Security

1. AeHN will make certain that all of its workforce members, including those who work remotely, are regularly reminded of information security risks and how to follow AeHN security policies. Additionally, workforce members will be provided with information about AeHN security procedures and how to use the Alaska HIE information systems in ways that minimize possible security risks.
2. AeHN will ensure that the confidentiality, integrity, and availability of EPHI on the Alaska HIE information systems is maintained when its information systems are accessed by third parties. Before third party persons are granted access to the Alaska HIE information systems containing EPHI, a risk analysis will be performed. After a successful risk analysis, access by third party persons to the Alaska HIE information systems containing EPHI will be allowed only after an agreement has been signed defining the terms for access.
3. AeHN must be able to effectively detect and prevent malicious software, particularly viruses, worms and malicious code. AeHN will develop, implement, and regularly review a formal, documented process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems and data.

G. Passwords and Log-In

1. AeHN will develop, implement, and regularly review a formal process for monitoring log-in attempts and reporting discrepancies. Access to all the Alaska HIE information systems will be via a secure log-in process.
2. AeHN will develop, implement, and regularly review a formal process for appropriately creating, changing and safeguarding passwords used to validate a user's identity and establish access to its information systems and data.

H. Security Incidents

1. AeHN will also maintain a documented process for quickly and effectively detecting and responding to security incidents that may impact the confidentiality, integrity, or availability of the Alaska HIE information systems. At a minimum, AeHN's SPO will ensure that:

- a. All actions taken are intended to minimize the damage of a security incident and prevent further damage.
 - b. Only authorized and appropriately trained AeHN employees are allowed access to affected information systems in order to respond to or recover from a security incident.
 - c. All actions taken are carefully documented.
2. AeHN will maintain a mechanism for quantifying and monitoring the types, volumes and costs of security incidents. This information will be used to identify the need for improved or additional security controls. AeHN's SPO is authorized to investigate any and all alleged violations of AeHN security policies, and to take appropriate action to mitigate the infraction and apply sanctions as warranted.

I. Disaster Recovery & Backup

- 1. AeHN will have a formal process for both preparing for and effectively responding to emergencies and disasters that damage the confidentiality, integrity or availability of its information systems. This will include coordination with our SaaS vendor to ensure that it has appropriate disaster recovery and backup procedures in place.
- 2. AeHN, independently or through its SaaS vendor, must have a formal, documented backup plan for its information systems. At a minimum, the plan must:
 - a. Identify information systems and electronic media to be backed up.
 - b. Provide a backup schedule.
 - c. Identify where backup media are stored and who may access them.
 - d. Outline restoration procedures.
 - e. Identify who is responsible for ensuring the backup of information systems and electronic media.
- 3. Restoration procedures for the Alaska HIE electronic media and information systems containing EPHI must be regularly tested to ensure that they are effective and that they can be completed within the time allotted in the Alaska HIE's disaster recovery plan.
- 4. The retention period for backup of EPHI on the Alaska HIE information systems and electronic media and any requirements for archive copies to be permanently retained must be defined and documented.

Risk analysis should be used to determine and document the maximum amount of loss that may occur if backup of the Alaska HIE information systems and electronic media is disrupted. Such analysis should be used to determine if all appropriate and reasonable measures are being used to backup the Alaska HIE information systems and electronic media.

Administrative Safeguards Policy 2.200		
APPROVED BY: AeHN Board	ADOPTED:	7/20/2011
	REVISED:	
	REVIEWED:	9/21/2011

Administrative Safeguards
AeHN Policy 2.200

