

# Technical Safeguards

## Alaska eHealth Network Policy 2.400

---

### HIPAA Security Rule Language

*“Implement policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights...”*

### Policy Summary

Alaska eHealth Network (AeHN) must purchase and implement information systems that comply with AeHN’s Technical Safeguards policy. Alaska HIE information systems must support a formal process for granting appropriate access to the Alaska HIE information systems containing EPHI. Access to Alaska HIE information systems containing EPHI must be limited to AeHN and Participating Site workforce members and software programs having a need for specific information in order to accomplish a legitimate task.

### Purpose

This policy reflects AeHN’s commitment to purchase and implement information systems that comply with AeHN’s HIPAA Security policies.

### 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

Technical Safeguards, Standard, AS 18.23.300 et seq.; 45 CFR 164.312

### 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
Access Control	2.401
Unique User Identification	2.402
Automatic Logoff	2.403
Encryption and Decryption	2.404
Audit Controls	2.405
Integrity	2.406
Person or Entity Authentication	2.407
Transmission Security	2.408
Breach Notification	2.409

## Policy

### A. Information Systems

1. AeHN will purchase and implement information systems that comply with AeHN's HIPAA Security policies.
2. All current Alaska HIE information systems that do not currently comply with AeHN's Administrative Safeguards will be identified and evaluated according to AeHN's risk analysis process.

### B. Access Control and Unique User IDs

1. As appropriate, Alaska HIE information systems will support one or more of the following types of access control to protect the confidentiality, integrity and availability of EPHI contained on Alaska HIE information systems:
  - a. User based
  - b. Role based
  - c. Context based
2. Alaska HIE information systems will support a formal process for granting appropriate access to the Alaska HIE information systems containing EPHI. At a minimum, the process will include:
  - a. Procedure for granting different levels of access to the Alaska HIE information systems containing EPHI.
  - b. Procedure for tracking and logging authorization of access to the Alaska HIE information systems containing EPHI.
  - c. Procedure for regularly reviewing and revising, as necessary, authorization of access to the Alaska HIE information systems containing EPHI.
3. As appropriate, security controls or methods that allow access to the Alaska HIE information systems containing EPHI will include, at a minimum:
  - a. Unique user identifiers (user IDs) that enable persons and identities to be uniquely identified. User IDs will not give any indication of the user's privilege level. Group identifiers will not be used to gain access to the Alaska HIE information systems containing EPHI.
  - b. A secret identifier (password).
  - c. The prompt removal or disabling of access methods for persons and entities that no longer need access to the Alaska HIE EPHI.
  - d. Verification that redundant user identifiers are not issued.
4. AeHN and Participating Site workforce members will not provide access to the Alaska HIE's information systems containing EPHI to unauthorized persons.
5. Appropriate Alaska HIE information system owners or their designated delegates will regularly review workforce member and software program access rights to Alaska HIE information systems containing EPHI to ensure that access is granted only to those having a need for specific information in order to accomplish a legitimate task. Such rights will be revised as necessary.

6. All revisions to AeHN workforce member and software program access rights will be tracked and logged. This information will be securely maintained.

#### C. Automatic Logoff

1. AeHN workforce members will end electronic sessions on information systems that contain or can access EPHI when such sessions are completed, unless the information system is secured by an appropriate locking method, e.g. a password protected screen saver.
2. AeHN workforce members will log off from or lock their workstation(s) when their shift is complete or they leave their workstation(s).

#### D. Encryption and Decryption

When risk analysis indicates it is necessary, appropriate encryption will be used to protect the confidentiality, integrity, and availability of EPHI contained on the Alaska HIE information systems. The risk analysis will also be used to determine the type and quality of the encryption algorithm and the length of cryptographic keys.

#### E. Audit Controls

1. AeHN will be able to record and examine significant activity on its information systems that contain or use EPHI. AeHN will conduct a risk analysis to identify and define what constitutes “significant activity” on a specific information system.
2. Appropriate hardware, software, or procedural auditing mechanisms will be implemented on Alaska HIE information systems that contain or use EPHI. The level and type of auditing mechanisms that will be implemented on Alaska HIE information systems that contain or use EPHI will be determined by AeHN’s risk analysis process.
3. Logs created by audit mechanisms implemented on Alaska HIE information systems will be reviewed regularly. The frequency of such review will be determined by AeHN’s risk analysis process.

#### F. Data Integrity

1. AeHN will appropriately protect the integrity of all EPHI contained on its information systems. Such EPHI will be protected from improper alteration or destruction. AeHN will perform regular risk analysis to determine the appropriate means to protect the integrity of all EPHI contained on its information systems.
2. AeHN will implement a formal, documented process for appropriately protecting the integrity of all EPHI contained on its information systems. At a minimum, the process must include:
  - a. A procedure for ensuring that the methods and controls used to protect integrity are effective and do not significantly impact Alaska HIE functionality and workflow.
  - b. A procedure defining how the Alaska HIE will detect and report instances of attempted or successful improper alteration or destruction of Alaska HIE EPHI.
  - c. A procedure defining how AeHN will respond to instances of attempted or successful improper alteration or destruction of Alaska HIE EPHI.

- d. A procedure defining when and how unnecessary Alaska HIE EPHI can be destroyed. Such destruction will be conducted only by properly authorized AeHN workforce members, or their delegates.
- 3. Methods used to protect the integrity of EPHI contained on Alaska HIE information systems will ensure that the value and state of the EPHI is maintained and it is protected from unauthorized modification and destruction.

G. Person or Entity Authentication

- 1. AeHN must create and implement a formal, documented process for verifying the identity of a person or entity before granting them access to EPHI.
- 2. AeHN must use an appropriate and reasonable system(s) to ensure that only properly authenticated persons and entities access Alaska HIE EPHI.

H. Data Transmission & Integrity

- 1. AeHN will appropriately protect the confidentiality, integrity and availability of all data it transmits over electronic communications networks.
- 2. Unless risk analysis indicates that there is not significant risk when sending Alaska HIE data over an electronic communications network, the data will be sent in encrypted form and have controls to safeguard the integrity of the data. AeHN SPO will approve all encryption and integrity controls prior to their use.
- 3. Integrity controls will always be used when highly sensitive Alaska HIE data such as passwords are transmitted over electronic communications networks.
- 4. The Alaska HIE’s integrity controls will ensure that the value and state of all transmitted data is maintained and the data is protected from unauthorized modification.

H. Breach Detection and Notification

AeHN, through its contract with the SaaS vendor, will put in place reasonable systems to detect, address, mitigate and report breaches of PHI.

<b>Technical Safeguards Policy 2.400</b>		
APPROVED BY: AeHN Board	ADOPTED:	7/20/2011
	REVISED:	
	REVIEWED:	9/21/2011