

Physical Safeguards

Alaska eHealth Network Policy 2.300

HIPAA Security Rule Language

“Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.”

Policy Summary

Alaska eHealth Network (AeHN) facilities, workstations and storage areas must be accessed and used only for authorized purposes. Workforce members must not use AeHN facilities, workstations or equipment to engage in any activity that is either illegal under local, state, federal, or international law or is in violation of AeHN policy. Access to the Alaska HIE EPHI must be controlled and authenticated.

Purpose

This policy reflects AeHN’s commitment to appropriately use and physically protect EPHI.

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

Physical Safeguards, Standard, AS 18.23.300 et seq.; 45 CFR 164.310

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
Workstation Use	2.301
Workstation Security	2.302
Device and Media Controls	2.303
Accountability	2.304
Data Backup and Storage	2.305
Facility Access	2.306

Policy

AeHN facilities, workstations, equipment and storage will be used only for authorized purposes: to support the educational, clinical, administrative, and other functions of AeHN. Such use demonstrates respect for intellectual property, ownership of data, security controls, and individuals' rights to privacy.

A. Workstations

1. All workforce members who use AeHN workstations will take all reasonable precautions to protect the confidentiality, integrity, and availability of EPHI.
2. Workforce members will not use AeHN facilities, workstations, equipment or storage to engage in any activity that is either illegal under local, state, federal, or international law or is in violation of AeHN policy.
3. Access to all AeHN workstations containing EPHI will be controlled with a username and password or an access device such as a token.
4. AeHN workstations containing EPHI will be physically located in such a manner as to minimize the risk that unauthorized individuals can gain access to them.
5. AeHN SPO approved anti-virus software will be installed on workstations to prevent transmission of malicious software. Such software will be regularly updated.
6. AeHN workforce members will activate their workstation locking software. AeHN workforce members will log off from or lock their workstation(s) when their shifts are complete or when they leave their workstation(s) during their shift. Connections from one workstation to another computer will be logged off after the session is completed.
7. Workstations removed from AeHN premises will be protected with security controls equivalent to those for on-site workstations.

B. Device and Media Control and Accountability

1. EPHI located on the Alaska HIE information systems or electronic media will be protected against damage, theft, and unauthorized access. This includes both EPHI received by the Alaska HIE and created within the Alaska HIE. EPHI must be consistently protected and managed through its entire life cycle, from origination to destruction.
2. AeHN will regularly conduct a formal, documented process that ensures consistent control of all electronic media and information systems containing EPHI that is created, sent, received or destroyed by the Alaska HIE.
3. Access to information systems and electronic media containing EPHI from the Alaska HIE will be provided only to authorized AeHN and Participating Site workforce members who have a need for specific access in order to accomplish a legitimate task.
4. All Alaska HIE information systems and electronic media containing EPHI will be located and stored in secure environments that are protected by appropriate security barriers and entry controls. The level of these controls should be commensurate with identified risks to the electronic media and information systems. All Alaska HIE information systems and electronic media containing EPHI will be disposed of securely and safely when no longer required.
5. All movement of Alaska HIE information systems and electronic media containing EPHI into and out of its facilities will be tracked and logged. Those responsible for such movement will

take all appropriate and reasonable actions to protect EPHI. This includes both EPHI received by the Alaska HIE and created within the Alaska HIE.

6. Workforce members should use only AeHN approved and tracked electronic media to store EPHI. EPHI will not be stored on AeHN workforce member home computers.
7. Appropriate AeHN management will authorize the use or sending of any information system or electronic media containing EPHI outside AeHN's premises. Such authorization will be tracked and logged.
8. AeHN employees and affiliates who move electronic media or information systems containing EPHI are responsible for the subsequent use of such items and will take all appropriate and reasonable actions to protect them against damage, theft, and unauthorized access.

C. Data Backup and Storage

1. Backup of EPHI on Alaska HIE information systems and electronic media, together with accurate and complete records of the backup copies and documented restoration procedures, will be stored in a secure remote location, at a sufficient distance from AeHN facilities to escape damage from a disaster at AeHN. This process may be carried out in a HIPAA compliant manner by AeHN's SaaS vendor.
2. AeHN will confirm that the vendor has enacted backup and restoration procedures for the Alaska HIE electronic media, and information systems containing EPHI will be regularly tested to ensure that they are effective and that they can be completed within a reasonable amount of time.
3. 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 will be defined and documented by AeHN or the vendor responsible for such backup.

Physical Safeguards Policy 2.300		
APPROVED BY: AeHN Board	ADOPTED:	7/20/2011
	REVISED:	
	REVIEWED:	9/21/2011