

Introduction to Security Policies

Alaska eHealth Network Policy 2.000

Policy Summary

The Alaska eHealth Network (AeHN) is committed to protecting the privacy and security of the protected health information (PHI) contained in the systems it oversees. As such, AeHN has adopted a series of Security Policies to comply with the responsibilities outlined in the Security Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This policy provides the general terms and provisions that apply to all of the Security Policies, along with the defined terms and acronyms that are used therein.

Purpose

This policy reflects AeHN's commitment to the security of PHI and the intent to make the Security Policies easy to use, understand and apply.

Scope/Applicability

This policy is applicable to all AeHN Security Policies and Procedures.

This policy's scope includes all EPHI contained in the Alaska HIE clinical data repository.

Regulatory Type, Legal/Regulatory Reference

Standard, AS 18.23.310; 45 CFR 164

Policy Authority/ Enforcement

AeHN's Executive Director (ED) and Security and Privacy Officer (SPO) are responsible for monitoring and enforcement of the AeHN Security Policies and Procedures.

Related Policies

All AeHN Security Policies and Procedures found at 2.200 et seq.

Policy

- A. AeHN will annually review all Security Policies and Procedures to determine if they comply with current HIPAA Security regulations, applicable Alaska law and AeHN contractual obligations. In the event that significant related legal, regulatory or organizational changes occur, the policy will be reviewed and updated as needed.
- B. AeHN uses the software-as-a-service model for the transmission and storage of PHI. Although AeHN does not have PHI directly contained on its own information systems, it is the steward for such information held by contractors and in a central data repository. For that reason, AeHN must continue to comply with these policies and procedures any time it is handling PHI, in any format.
- C. AeHN employees will not directly manage or access PHI on a regular basis, but some employees will have the ability to do so when necessary. This requires such employees to comply with all responsibilities of a health information exchange under HIPAA.

- D. These policies and procedures apply to the AeHN workforce members and the information used and disclosed by AeHN. They do not apply directly to participants in the HIE. The guidelines for participation and privacy and security responsibilities for participants are outlined in the Network Responsibilities provided upon signing of the Participation Agreement.

Glossary

AS	Alaska Statutes
AeHN	Alaska eHealth Network – the designated HIE for the State of Alaska
BAA	Business Associate Agreement
CFR	Code of Federal Regulations
ED	Executive Director
EPHI	Electronic Protected Health Information
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act of 1996
PA	Participant Agreement
PHI	Protected Health Information
SaaS	Software as a Service
SPO	Security and Privacy Officer
User IDs	Unique User Identifiers

Introduction to Security Policies 2.000		
APPROVED BY: AeHN Board	ADOPTED:	7/20/2011
	REVISED:	
	REVIEWED:	9/21/2011