DatCard Systems’ Adaptive Image Exchange (AIX) HIPAA Compliance Guide

Overview

Privacy, productivity and remote access

The healthcare industry has benefited greatly from the ability to use remote access to view patient data from anywhere and share data among partners and suppliers. Although transmitting patient data across networks improves care, speeds service and reduces healthcare costs, many remote access products inadvertently put patient privacy at risk, especially if the data is sent over unsecured networks such as the Internet.

For this reason, the Health Insurance Portability and Accountability Act (HIPAA) calls for privacy and security standards that protect the confidentiality and integrity of patient health information. Specifically, if you are transmitting patient data across the Internet, your remote access products and security architecture must provide end-to-end encryption so the data cannot be intercepted by anyone other than the intended recipient. In addition, the remote access products and network must provide access control to allow viewing only by authorized people.

AIX’s HIPAA Security Guide

Every business that is part of the U.S. healthcare industry needs to comply with the federal standards regulating patient information. In addition to protecting worker health insurance coverage, HIPAA sets forth standards for protecting the integrity, confidentiality and availability of electronic health information. AIX is a HIPAA-compliant Medical Image Exchange that allows clinicians as well as other healthcare organizations to share images at the request of a patient.

The following matrix is based upon the HIPAA Security Standards rule published in the Federal Register on February 20, 2003 (*45 CFR Parts 160, 162 and 164 Health Insurance Reform: Security Standards; Final Rule*). The Department of Health and Human Services provides the HIPAA Security Standards on its website: http://aspe.hhs.gov/admnsimp/final/FR03-8334.pdf. DatCard Systems created the following matrix as a guide to assist healthcare providers in navigating the various HIPAA requirements and to demonstrate how AIX supports HIPAA compliance.

Technical safeguards § 164.312				

Standard covered entities must implement	Implementation specifications
	R = Required
	A = Addressable
			Key factors	Support in AIX

(a) (1) Access Control		R	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to authorized persons or software programs.	● Host computer access is protected by strong password authentication. ● Passwords are used for authentication to view images. ● Configurable failed log-in, lockout threshold.
	Unique User Identification (Required)	R	Assign a unique name and/or number for identifying and tracking user identity.	● Users and account managers are identified by using their unique email address as their login name.
	Emergency Access Procedures	R	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	● Provides rapid, secure access to a computer desktop from virtually anywhere, which may be used as a supplementary method for providing emergency access to healthcare information.
	Automatic Logoff	A	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	● Manager-configurable session inactivity time-out ensures that AIX remote access sessions are not left running

				indefinitely. • Website inactivity time-out automatically logs users out of their AIX accounts.
	Encryption and Decryption	A	Implement a mechanism to encrypt and decrypt electronic protected health information.	• Advanced Encryption Standard (AES), FIPS 197 in 8-bit cipher feedback mode. • A unique 128-bit AES encryption key is generated at the start of each session.
(b) Audit Controls		R	Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	• All connection and session activity through AIX's distributed network service infrastructure is logged (including file transfers, remote printing and image export) for security and quality-of-service purposes. • Account managers have up-to-the-minute web-based access to advanced management and reporting tools.

AIX Product Information

Healthcare applications

Physicians, nurses, IS/IT staff, administrative employees and authorized healthcare partners can use DatCard Systems' Adaptive Image Exchange (AIX) for the sharing of medical images as it pertains to patient care from any location connected to the web. AIX protects data confidentiality through a combination of encryption, strong access control and host computer protection methods.

Security, control and customization

Organizational users and administrators have the option of granting image viewing and management privileges to groups or individual clinicians. Some viewing features may be disabled by an IT administrator to customize the level of security that is appropriate for your organization.

Encryption

AIX employs industry-standard end-to-end Advanced Encryption Standard (AES) encryption using 128-bit keys to protect the data stream and file transfers. Additional built-in security features such as strong passwords and end-to-end user authentication ensure data confidentiality. AIX encryption fully complies with HIPAA Security Standards to ensure the security and privacy of patient data.

Frequently Asked Questions

Q: What are the general requirements of the HIPAA Security Standards? (Ref: § 164.306 Security Standards: General Rules)

A: Covered entities must do the following:

- Ensure the confidentiality, integrity and availability of all electronic protected health information that the covered entity creates, receives, maintains or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the privacy regulations.
- Ensure compliance with this subpart by its workforce.

Q: How are covered entities expected to address these requirements?

A: Covered entities may use any security measures that reasonably and appropriately implement the standards; however, covered entities must first take into account the risks to protected electronic information; the organization's size, complexity and existing infrastructure; and costs.

The final rule includes three "safeguards" sections outlining standards (what must be done) and "implementation specifications" (how it must be done) that are either "required" or “addressable”. If “required”, it must be implemented to meet the standard; if “addressable”, a covered entity can either implement it, implement an equivalent measure or do nothing (documenting why it would not be reasonable and appropriate).

- Administrative Safeguards: Policies and procedures, workforce security and training, evaluations and business associate contracts.
- Physical Safeguards: Facility access, workstation security and device and media controls.
- Technical Safeguards: Access control, audit controls, data integrity, authentication and transmission security.

Q: What is AIX doing to help customers address HIPAA regulations?

A: To facilitate compliance with HIPAA security regulations, AIX is providing detailed information about the security safeguards we have implemented into AIX. This information is provided in several forms, including help documents, HIPAA-compliance matrices and other technical collateral. Additionally, AIX Services group is available to provide guidance and assistance in all deployments.

Q: What is the best way to deploy AIX in an environment subject to HIPAA regulations?

A: Just as HIPAA allows considerable latitude in the choice of how to implement security safeguards, a single set of guidelines is not applicable for all deployments. Organizations should carefully review all configurable security features of AIX in the context of their specific environments, user population and policy requirements to determine which features should be enabled and how best to implement into their organization.

Depending on organizational policy, disabling the File Printing and/or File Exporting may be advisable to ensure host integrity and maximize data containment and confidentiality. The AIX Administration website offers a comprehensive set of web-based user management, host/client end-point management and auditing features. Organizations are advised to review and use the features that they believe will achieve maximum overall system-assurance levels and compliance with HIPAA-mandated administrative, technical and physical security safeguards.