


Navigating Compliance Advancing Security Steamlining Operations

A man and a woman in white lab coats are looking at a laptop in a hospital hallway. The woman is wearing a name tag that says "Charlotte".

**A CISOs Guide to
Network-Attached
Storage Solutions**

Introduction

The healthcare industry is experiencing an unprecedented surge in data generation, driven by advancements in technology and changing patient needs. This poses significant challenges for healthcare CISOs, who are tasked with managing vast volumes of structured and unstructured data while ensuring compliance and security.

Network attached storage (NAS) is a centralized storage solution that strikes a balance between simplicity, scalability and performance, making it ideal for healthcare environments.

**137
terabytes**

of data is created each day by the healthcare industry alone

\$8 trillion

in revenue was lost due to data breaches in 2023

60%

of healthcare organizations are utilizing IoT devices for monitoring and data collection

31%

of organizations suffered from data loss and exfiltration due to carelessness

92%

of organizations in the healthcare industry have experienced a data breach within the year

3 billion

healthcare records were compromised in 2024

Security Challenges in Healthcare

Regulatory Compliance

Healthcare organizations are bound by strict compliance standards, and failure to meet them can lead to severe penalties. Regulations such as HIPAA, GDPR, and HITECH impose stringent requirements for securing sensitive patient data, including:

- **Encryption:** All data, whether at rest or in transit, must be protected by robust encryption standards.
- **Data Retention:** Records must be stored for defined periods, requiring scalable and efficient storage solutions.
- **Access Control and Audits:** Organizations must maintain detailed logs of access and ensure only authorized personnel can retrieve sensitive information.

These requirements amplify the need for a storage system that seamlessly integrates compliance features, reduces administrative burden, and supports real-time auditing.

\$50,000

minimum fine for a HIPAA violation involving willful negligence & failure to address vulnerabilities.

73%

of healthcare providers still use outdated legacy systems, which poses significant risks.

Limitations of Legacy Systems

Outdated or fragmented storage systems exacerbate the risks and inefficiencies CISOs face. For example:

- **Limited Scalability:** Legacy systems struggle to keep pace with growing data demands, leading to costly upgrades or performance bottlenecks.
- **Higher Vulnerability:** Older infrastructure often lacks the advanced security features required to defend against modern cyber threats.
- **Data Silos:** Fragmented storage can hinder collaboration and delay critical care decisions, especially in multi-location organizations.

A Solution for CISOs

When paired with proactive security practices—such as regular updates, employee training, and comprehensive risk assessments—NAS provides healthcare organizations with the tools needed to stay ahead of threats, safeguard sensitive information, and maintain operational continuity.

What is Network Attached Storage (NAS)?

At its core, Network-Attached Storage (NAS) is a centralized storage solution connected to an organization's network, providing shared access to data for authorized users and applications. Unlike direct-attached storage (DAS) or complex storage area networks (SAN), NAS offers a middle ground of simplicity, scalability, and advanced functionality.

Key Characteristics

Centralized Storage

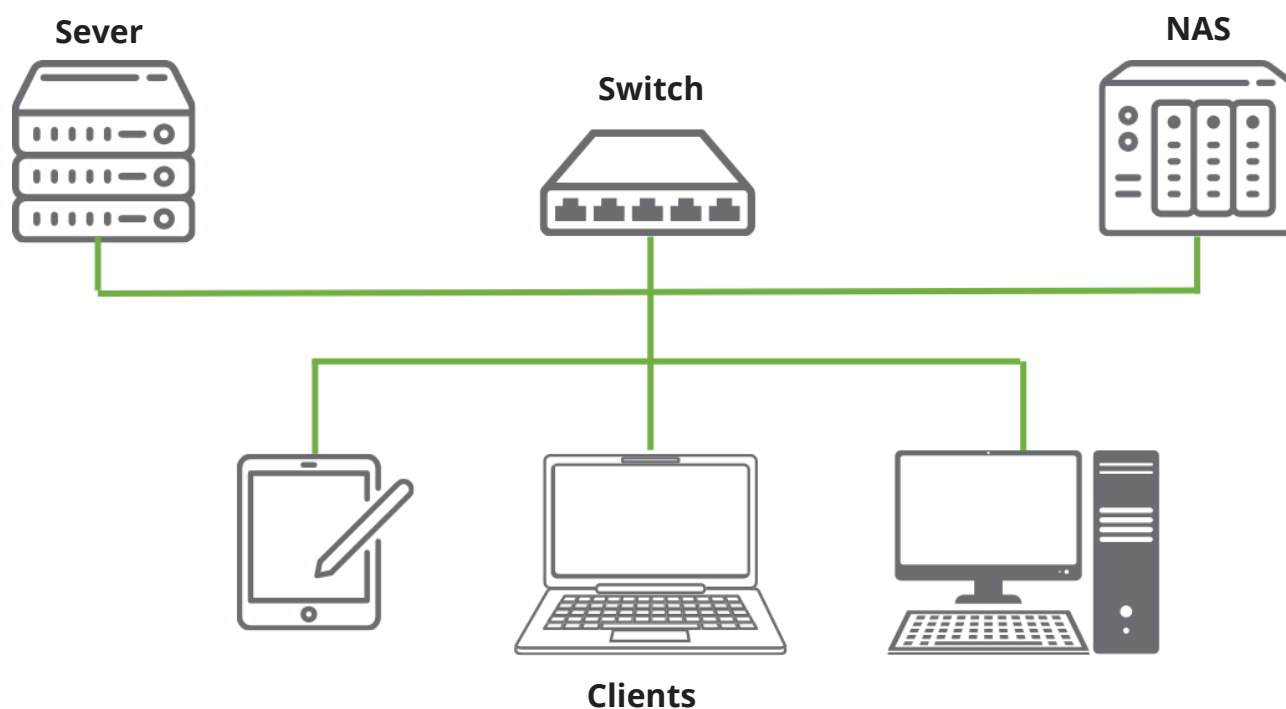
Consolidates data from multiple sources, creating a unified repository.

Network Connectivity

Provides seamless access for users and applications across the organization.

File-Level Storage

Specializes in handling structured and unstructured data, such as EHRs, imaging files, and telehealth session recordings.



How NAS Compares

Feature	NAS	SAN	Cloud Storage
Scalability	Easy to scale with additional devices	High, but complex to expand	Virtually unlimited
Initial Investment	Moderate	High (requires dedicated infrastructure)	Low (pay-as-you-go)
Integration	Straightforward, plug and play	Complex, requires significant IT expertise	Easy, but may need additional tools or APIs for compatibility
Accessibility	Network-based, ideal for multi-department access	High-speed block access for critical workloads	Accessible anywhere with internet
Security	Built-in encryption and access controls	Requires separate tools for encryption	Dependent on provider's policies
Control	Fully managed in-house	Fully managed in-house	Limited control over infrastructure
Security & Compliance Costs	On-premise control reduces third-party risks, requires internal security protocols	Strong security but complex to manage across multiple facilities	Built-in security features, but compliance and data sovereignty risks exist
Long-Term Cost Predictability	One-time investment with predictable maintenance costs	Expensive upfront, but reliable for large-scale environments	Ongoing operational costs can increase unpredictably

How NAS Can Benefit Your Operations

Strengthen Security & Streamline Regulatory Compliance

NAS systems can enhance IoT security by providing encrypted storage and role-based access controls, helping to protect sensitive data from unauthorized access. When integrated with network segmentation and best practices for secure authentication, NAS helps mitigate risks without slowing down operations.

Reduce Attack Surface & Minimize Third-Party Impacts

Unlike fully cloud-based storage, NAS allows on-premises control over sensitive data, reducing exposure to third-party vulnerabilities. Ciphertex Data Security's SecureNAS solutions support zero-trust architectures, ensuring that only authorized users and applications can access critical systems.

Support Scalability Without Increasing Complexity

With growing data from EHRs, PACS, and medical IoT, storage demands are skyrocketing. NAS solutions scale seamlessly, allowing expansion without disrupting existing workflows or requiring costly infrastructure overhauls.

Improve Disaster Recovery & Business Continuity

Ransomware attacks and system failures are a growing threat in healthcare. NAS provides automated backups, replication, and built-in redundancy, ensuring rapid data recovery and uninterrupted access to patient records, imaging files, and research data.

Enhance Secure Collaboration Across Multiple Facilities

Modern NAS solutions enable secure, high-speed data sharing across hospitals, clinics, and remote teams—critical for telemedicine, research collaborations, and cross-location patient care—while maintaining strict access control policies.

Reduce Long-Term Storage Costs

Healthcare IT budgets are under pressure, but compliance and security can't be compromised. NAS provides a predictable, cost-effective alternative to cloud storage, eliminating recurring cloud fees while offering full control over data lifecycle management.

Our SecureNAS® Solutions

Ciphertex SecureNAS® solutions provide a powerful, customizable, all-in-one platform designed to empower organizations to safeguard critical data while ensuring operational efficiency and regulatory adherence.

Military-Grade Encryption

Our solutions feature FIPS 140-2 Level 3 certified hardware encryption, delivering robust protection against unauthorized access and breaches.

Back Up & Recovery

Ciphertex SecureNAS® products simplify backup and recovery, helping to prevent data and corruption while ensuring continuity in care.

Rugged Portability

SecureNAS® devices feature durable, shock-resistant construction and portable form factors, ensuring reliable performance in demanding environments and easy transport when needed.

Centralized Data Management

SecureNAS® provides a customizable, user-friendly web-based interface for centralized management of storage, access controls, and system monitoring, streamlining operations.

Proactive Threat Mitigation

Our solutions includes antivirus protection and firewalls to proactively detect and neutralize threats, ensuring data integrity and availability.

No-Cost Software Updates

Our RhinOS 24.1 operating system is pre-installed on SecureNAS® devices, with no license or renewal fees, keeping systems updated at no extra cost.

Learn more at
ciphertex.com

