

Healthcare Storage Encryption

Best Practice for HIPAA Compliance

The FBI reports that average financial losses associated with unauthorized access to private information increased by nearly 600% since 2004.

Less Than Half Compliant

Healthcare organizations that are not yet up to speed with Health Insurance Portability and Accountability Act (HIPAA) regulations do not stand alone. To date, less than half of healthcare providers are compliant with HIPAA security requirements.¹ What is more, non-compliant organizations are in danger of becoming complacent, due to recent Department of Health and Human Services policy that makes HIPAA enforcement primarily complaint-based.

HIPAA Security Breaches and Formal Complaints on the Rise

Even with only complaint-based enforcement, the healthcare industry knows that nearly one-third of its members experienced data security breaches in 2005. Roughly the same number faced Federal privacy violation complaints – the trigger for expensive legal liabilities and penalties associated with HIPAA. In fact, the FBI reports that average financial losses associated with unauthorized access to private information increased by nearly 600 percent between 2004 and 2005.²

As non-compliant healthcare organizations scramble to meet HIPAA requirements – while facing a backdrop of rapidly growing computer security threats – they also struggle with administrative overhead expenses that account for as much as 25 percent of healthcare costs. To maintain the bottom line and still implement HIPAA security processes, these companies must find ways to do more with less.

Encryption with “Must Have” Access and Audit Controls

HIPAA Technical Safeguards Section 164.312 points to encryption as the way to protect Personal Health Information



(PHI). By employing encryption, confidential health information is concealed. Combined with stored data encryption best practices – including centralized, enterprise-class encryption key management, access and audits controls, and authentication – healthcare providers can implement overall security and privacy measures that not only protect sensitive PHI and improve the quality of care through uniform, accessible health records but also significantly reduce backend PHI data classification costs.

NeoScale Solutions — Seamless. Reliable. Secure.

NeoScale Systems, Inc., the industry leader in enterprise storage security, uniquely meets the healthcare industry's privacy requirements with a range of storage security appliances that make network data storage unreadable to unauthorized users while making it possible to control, track, and document PHI.

With NeoScale solutions, healthcare providers can automate the encryption of PHI using centralized controls that allow for varying tiers of access. By doing so, doctors, pharmacists, insurance companies, payment processors, and others are authorized with access on a need-to-know basis so sensitive patient information is protected.

NeoScale's CryptoStor[®] storage security appliances are purpose-built, providing ubiquitous, immediate, and transparent protection of storage data regardless of application, transport, media type, or



¹ HIPAA Compliance Survey, HIPAAAdvisory.com, Summer 2005.

² 2005 CSI/FBI Computer Crime and Security Survey.

The NeoScale CryptoStor® storage security appliances for tape, virtual tape, disk, and Fibre Channel link encryption offer:

True Wire-Speed Encryption

The custom hardware data path used by purpose-built NeoScale CryptoStor storage security appliances ensures true wire-speed performance – providing virtually no latency delays and minimal response time impact.

Certified FIPS 140-2 Level 3 Security

NeoScale delivers the only storage security appliances with top-to-bottom, appliance-level FIPS 140-2 Level 3 certification. FIPS security extends from hardware components to the operating system and reaches out to system-level user-access control and key management features for both primary storage and SAN extension applications.

Global Key Management

NeoScale appliances automate and simplify encryption key security for global data storage. Comprehensive key management tools and centralized key archival make distributed information recovery simple and easy. Automation avoids inappropriate use of encryption technologies.

Local and Remote Clustering

NeoScale clustering supports highly available access to secure information via redundant network paths. In the event of a failure, data remains accessible – without any manual re-configuration – and can be recovered anywhere, via any clustered appliance.

Certified Multi-Vendor Interoperability

NeoScale certifies industry-leading solution partners, including EMC, SUN/STK, IBM, and HP, to ensure integrated products and solutions.

Lowest Cost; Lowest Operating Impact

NeoScale innovations reduce deployment risks, minimize ongoing operational complexities, and are available at the lowest possible price point.

location. This enables healthcare organizations to meet compliance regulations with the lowest operational impact and at the lowest total cost.

Protection Without Crippling Complexities

Healthcare IT professionals are justifiably concerned about the complexities that encryption can impose on the storage infrastructure. NeoScale's CryptoStor® storage security appliances provide a complete storage solution that automates and simplifies the procedures required to meet HIPAA compliance regulations, including:

- Significant reduction of backend PHI data classification and management costs
- Easily-deployed stored data access control and encryption, without disruption of applications or operations
- Streamlined storage security functions and offloading of security processing in a centralized, appliance platform
- Enhanced consolidation economies with strong access control
- Reasonable and accepted due diligence for HIPAA compliance

NeoScale Customers Protect PHI and Save Costs

With NeoScale solutions, top healthcare organizations can protect data according to HIPAA compliance standards – while reducing additional HIPAA data classifi-

cation, management, and infrastructure costs.

A case in point, the University of Texas Health Science Center (UT/HSC) at Houston uses NeoScale storage security solutions to operate a storage area network (SAN) infrastructure that supports health and billing applications. "Protecting PHI data for HIPAA compliance can require data classification and special network and storage provisions," said Kevin Granhold, manager of Network Services for UT/HSC. "By encrypting the PHI data, UT/HSC can overcome some of these added costs. The NeoScale appliance selectively encrypts based on application or owner data, so we can maintain segregated data sets by associating unique keys according to the application or owner. Ultimately, since CryptoStor is not tied to any application or platform, it should continue to provide security services as new applications are brought online or as our storage resources change."

Find Out More

Find out more about how NeoScale solutions can provide a complete encryption solution, with the lowest operational impact and at the lowest total cost. Visit us on the Web at www.neoscale.com or contact us at 1-408-473-1303.



Copyright © 2006 by NeoScale Systems, Inc. All rights reserved. NeoScale, the NeoScale logo, and CryptoStor are registered trademarks of NeoScale Systems, Inc. All other names and/or trademarks herein are the property of their respective owners.

Seamless. Reliable. Secure.