NEXSAN

NEXSAN ASSUREON
HIPAA COMPLIANCE UPDATE: NEW BREACH CONSEQUENCES

WHITE PAPER

EVOLUTION OF ENFORCING PATIENT PRIVACY

Healthcare providers are required to retain, protect and secure patient records for extensive periods of time. Ever since the enactment of the Healthcare Insurance Portability and Accountability Act (HIPAA) in 2006, critics argued that the guidelines were arbitrary and left too much to interpretation. Fines and penalties were seldom imposed causing most organizations to assume that compliance was discretionary. New, tougher and more specific regulations are now in place, which impose punitive fines when they are not followed and thus strengthen HIPAA's privacy regulations.

On August 24th of 2009, the Department of Health and Human Services (HHS) published "Breach Notification for Unsecured Protected Health Information; Interim Final Rule"[1], which provided specificity to the protection requirements of electronic health records. This clarifying document was a prescribed mandate of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), signed by President Obama on February 17, 2009. The Interim Final Rule was necessary to provide enforceability to HIPAA and to address confusion caused by the original ambiguities.

The final rule is expected in the beginning of 2011.

[1] US Federal Register, Dept of Health and Human Services: 45 CFR Parts 160 and 164. http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf

NEXSAN 1445 Lawrence Drive, Thousand Oaks, CA 91320 | p. 866.4.NEXSAN f. 805.418.2799 | www.nexsan.com

CHANGES TO HIPAA

When a breach involves "unsecured" individual ePHI (Electronic Protected Health Information) the covered healthcare entities (CE's) must notify;

- The affected individuals.
- Secretary of the Department of Health and Human Services.
- Certain circumstances will require the media to be notified.

While a breach of unsecured ePHI requires notification, unauthorized access of secured ePHI does not. The rule defines secured ePHI as "Unusable, Unreadable, or Indecipherable to Unauthorized Individuals."

The rule specifies technologies and methodologies that render protected health information secure.

- Valid encryption for data at rest that is consistent with NIST's guide to encryption technologies.
- The media on which the ePHI is stored or recorded have been destroyed. Electronic media needs must meet NIST's Media Sanitation Guidelines.[2]

Penalties for breaches.

- Fines have increased significantly; an organization can now be fined up to $1.5 million per calendar year for each violation.
- Affected individuals may now receive a percentage of a civil monetary penalty or monetary settlement. This will most likely lead to extensive litigation.
- In addition to fines, organizations are exposed to additional expenses when notifying those affected by a breach. Once emails, first-class mailings, toll-free numbers, media outreach, man-hours and more are tabulated, a breach can quickly turn into a multimillion-dollar expense.

[2] NIST Special Publication 800-88, Guidelines for Media Sanitization. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

NEXSAN 1445 Lawrence Drive, Thousand Oaks, CA 91320 | p. 866.4.NEXSAN f. 805.418.2799 | www.nexsan.com

ASSUREON MEDICAL IMAGE ARCHIVE: EQUIPPED FOR THE NEW REGULATIONS

Assureon, from Nexsan, is quickly becoming a leader in the medical archive market. Assureon combines fast, scalable, disk storage with "lights-out" storage management and compliance features to address the evolving needs of the healthcare industry. Healthcare IT professionals are choosing Assureon because it includes built-in capabilities that enforce patient privacy to meet the requirements of new regulations. These include;

- Encryption of all data at rest utilizing AES 256 bit encryption.
- A patent pending "Key Management" system.
- Encryption of the data in flight between storage units.
- Full data wipe - DOD process (NIST standard) for overwriting data in order to ensure electronic cleansing of the information.

SUMMARY

The Interim Final rule is unambiguous, providing clear guidance on what steps should be taken to protect electronic healthcare information. If healthcare information is not encrypted and data breach occurs, the facility will be facing large financial penalties. If the patient data is encrypted, that information is secure and protected under HIPAA. Encrypting a PACS image archive is a necessary step towards HIPPA compliance. Nexsan's Assureon medical archive is the only archive product that offers encryption as a standard feature.

ABOUT NEXSAN

Nexsan® is a leading independent provider of disk-based storage systems purpose-built and priced for the mid-market, offering industry-leading reliability, space and power efficiency. Overcoming the challenges of traditional storage, the company's disk-based systems reduce the complexity and cost of storage with easy-to-use, efficient and enterprise-class features, delivering a different kind of storage experience.

NEXSAN 1445 Lawrence Drive, Thousand Oaks, CA 91320 | **p.** 866.4.NEXSAN **f.** 805.418.2799 | www.nexsan.com