



**NEXSAN
ASSUREON**

HIPAA
Compliance Update:
New Breach
Consequences

ASSUREON®

HIPAA Compliance Update: New Breach Consequences

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.



Changes to HIPAA

1. When a breach involves "unsecured" individual ePHI (Electronic Protected Health Information) the covered healthcare entities (CE's) must notify;
 - a) The affected individuals.
 - b) Secretary of the Department of Health and Human Services.
 - c) Certain circumstances will require the media to be notified.
2. 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.*"
3. The rule specifies technologies and methodologies that render protected health information secure.
 - a) Valid encryption for data at rest that is consistent with NIST's guide to encryption technologies.
 - b) The media on which the ePHI is stored or recorded have been destroyed. Electronic media needs must meet NIST's Media Sanitation Guidelines.²

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

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

4. Penalties for breaches.

- a) Fines have increased significantly; an organization can now be fined up to \$1.5 million per calendar year for each violation.
- b) Affected individuals may now receive a percentage of a civil monetary penalty or monetary settlement. This will most likely lead to extensive litigation.
- c) 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.



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;

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

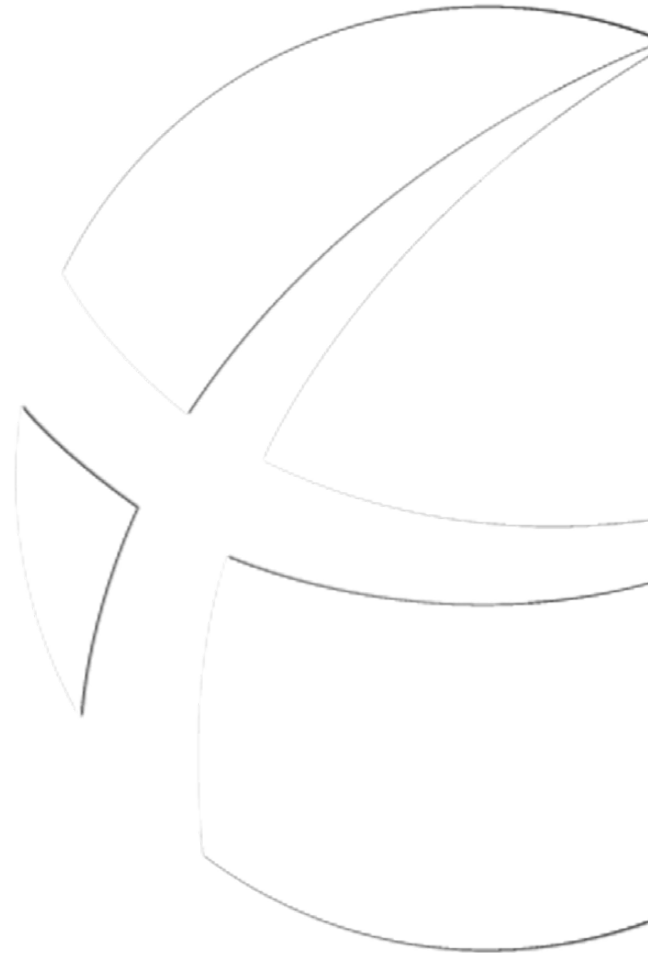
Summary

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 HIPAA compliance. Nexsan’s Assureon medical archive is the only archive product that offers encryption as a standard feature.

Presented by Nexsan

About Nexsan

Nexsan Corporation is a leading provider of energy-efficient, long-term storage systems. Nexsan delivers secure storage appliances and modular, capacity-optimized disk-storage systems for a broad range of applications including fixed content storage and archiving, email, medical imaging, compliance and litigation support, disk-based backup, digital video security, and rich media. Nexsan's solutions are the choice of small and medium-sized companies as well as large global enterprises and major governmental agencies around the world that are seeking cost-correct, high-density storage solutions. Founded in 1999 and based in Thousand Oaks, California, Nexsan sells its products exclusively through a select global network of VARs, OEMs and system integrators. For more information, please see the company's website at www.nexsan.com



555 St. Charles Drive • Suite 202 • Thousand Oaks, CA 91360
Toll-free: (866) 4NEXSAN • Main Line: (805) 418-2700 • Fax: (805) 418-2799
European Office: +44 (0) 1332 291 600 • www.nexsan.com