



ASSUREONTM

HIPAA & Assureon

Compliance by Nexsan

Rule 21
CFR part 11

HIPAA (Health Insurance Portability and Accountability Act of 1996) called upon the Department of Health and Human Services (HHS) to publish new rules that would ensure:

- Standardization of electronic patient information
- Unique health identifiers for individuals, employers, health plans and health care providers
- Security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present or future.

Who Needs to
Comply?

HIPAA affects virtually all health care providers, health plans, public health authorities, healthcare clearinghouses, life insurers, self-insured employers etc

HIPAA calls for severe civil and criminal penalties for noncompliance:

Fines up to \$25K for multiple violations

Fines up to \$250K and/or imprisonment for knowing misuse of information.

Tamper proof
Records

The final Security Rule was published April 21, 2003, and compliance for most entities is required by April 21, 2005.

Compliance claims made by vendors concerning their products can be misleading.

Below are excerpts from HIPAA's Technical Safeguard's that refer to requirements that a compliant storage solution should address. In violet are the capabilities Nexsan Assureon provides its customers.

Information
Integrity
Guaranteed with
Digital Fingerprint
Technology

"Sec. 164.312 Technical safeguards.

(a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4)."

Assureon's Access Control has two components.

1) Authentication verifies that a client is who they say they are:

a) Assureon uses Microsoft's Authentication System

b) Assureon optionally uses security certificates (Smart Cards)

2) Authorization determines that the client has the appropriate permissions to access the resources they are requesting.

Integrated
Retention
Management
System

Authorization is given to an authenticated client by policies established within Assureon and then published into Microsoft's Active Directory.

Protect Your Health Records and Meet Your Compliance Obligations

User Authentication

“(2) Implementation specifications:

(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.”

Assureon’s supports Microsoft Authentication System which establishes a unique single user logon. Assureon provides an audit trail tracking user identity and time-stamps access to information.

Encryption for Privacy Protection

“(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.”

Assureon offers the capability to encrypt and decrypt all files or selected files using the Advanced Encryption Standard (AES).

Audit Trail: Access

“(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.”

Assureon provides an audit trail of all access to the protected health care information.

Tamperproof Health Care Records

“(c)(1) Standard: Integrity. Implement policies and procedures to

protect electronic protected health information from improper alteration or destruction.”

Assureon controls access to the information, controls the ability to change a file, keeps a copy of an original, keeps new copy when a change occurs, and provides an audit trail of who and when a change occurs.

Information Integrity Guaranteed with Digital Fingerprint Technology

“(2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.”

Assureon uses digital fingerprint technology to verify whether a file has been tampered with or not.



This brochure is not a legal opinion or intended to be legal advice.
Please seek legal counsel for questions on compliance.

© 2006 Nexsan Technologies Inc. All rights reserved.
Tel: USA 886 4 NEXSAN (International) Tel: +1 818 715 9111
E-Mail: sales@nexsan.com or visit our Web site: www.nexsan.com