

STRATEGIC BRIEF – HIPAA



Regulation Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) enacted reform and standardization in the healthcare industry to protect patient confidentiality. The goals of HIPAA are to improve the access and portability of patient health records, while maintaining strict privacy and security of healthcare information. HIPAA is comprised of two sections:

- Title 1 deals with the protection of health insurance coverage for those who lose or change jobs
- Title 2 deals with standardization of healthcare-related information systems, including the privacy and security of patient medical information and standard formatting of electronic transactions.

Requirements for Handling Patient Health Records

HIPAA requires the most records be retained for a 6 year period. These and other requirements regarding the handling of patient records are outlined within the Privacy Rule and Security Rule. A partial list of these requirements include:

- > **Access controls** – User identification, encryption and data access lockdown
- > **Integrity controls** – policies and processes to protect files from alteration or destruction
- > **Authentication** – verification of person or entity requesting information
- > **Transmission security** – integrity controls and encryption
- > **Contingency plans** – backup and disaster recovery
- > Additionally, HIPAA requires that most records be retained for a 6-year period.

How Do Organizations Comply

The Privacy and Security Rules are very careful not to specify any specific technologies for an organization to use to comply. Instead, the rules outline the requirements as noted above and ask each organization to review their specific situations and adopt processes and technologies to comply with the requirements. One of the key steps the Security Rule calls for in outlining a compliance solution, is to perform a risk assessment to understand the key areas of concern and then design solutions to mitigate risk according to the specifications of the regulation. This process of assessing risk should take a broad view of understanding business and operational practices that are subject to the regulation.

How Alliance Storage Technology Can Help Your Organization Remain Compliant

Alliance's Plasmon archival solutions provide unique features and benefits to help organizations comply with the requirements of HIPAA.

- > Embedded AES encryption (128, 192 and 256 bit) helps IT architects place controls in their environment to comply with HIPAA
- > UDO Guard ensures that media cannot be accessed outside of the Archive Appliance environment by preventing media spin-up via unique authorization keys.
- > Alliance's Plasmon UDO™ technology provides a strong foundation with true hardware-based WORM media, creating unmatched data authenticity and integrity.
- > Access and Authenticity to the Alliance's Plasmon system is secured using local users, LDAP or CIFS.
- > The Alliance's Plasmon solution utilizes a NAS (Network Attached Storage) architecture that can be secured using industry-leading security tools.
- > The UDO Archive Appliance™ allows for automated creation of duplicate UDO media for offsite storage, aiding in the ability to create contingency plans for protected health information.
- > UDO media provides the ultimate technology for data longevity and permanence, providing a lifespan of 50+ years while simultaneously providing a low total cost of ownership via its green technology.

QuickView

Organization:
>> Southeast Louisiana
Veterans Hospital

Industry:
> Healthcare

Application:
> Image Storage

Integrator:
> Hewlett-Packard

Solution:
> Plasmon™
G-Series Library
> UDO Archive
Appliance™

ROI:
> 95% patient data
recovery after Katrina

**UDO™ stands up to a
Category 5 hurricane,
when other storage
technologies fail.**

Archiving Designed with Healthcare in Mind

At Alliance Storage Technologies, we have designed our optical data storage solutions with the specific needs of healthcare organizations like yours in mind. With over 1 BILLION healthcare records stored on our media, we know that longevity, authenticity and accessibility are key components of your organization's medical archiving success.

Below are just a few examples of how the functionality of our Plasmon Technology directly correlate to HIPAA requirements:

REQUIREMENT HIPAA SECTIONS

Access Controls Access Controls 164.312(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).

Data Integrity 164.312(c)(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

164.312(c)(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.

Authentication 164.312(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Contingency Planning 164.308(a)(7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

164.308(a)(7)(ii) Implementation specifications: (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. (B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

ALLIANCE FUNCTIONALITY

Plasmon AA provides compliant file management including access controls ensuring that only users with appropriate permissions can gain access to data stored on the AA infrastructure.

Access to the Plasmon AA system is secured using standard industry authentication, such as permissions to file shares (LDAP, Active Directory, Local users).

The underlying UDO media is a Write-Once Read Many (WORM) technology that ensures data integrity within the archive. Once data is written to UDO, the recording is physically permanent and cannot be hacked as with WORM simulation technologies for disk and tape media.

Plasmon AA ensures data integrity by first performing a write verification pass on all data committed to UDO media. Additionally, the Plasmon AA also utilizes checksums to ensure data integrity on data recall.

Plasmon AA restricts user access via an authorized user name and password to ensure that the access attempt is authentic.

Removable Media. Plasmon UDO libraries create removable and redundant copies of patient data, ensuring that the patient record archive is not "trapped" at the primary site during a failure event – whether operational or a site disaster.

Disaster Recovery Site Deployment – The Plasmon AA can be configured to receive data via the WAN and can be deployed as a disaster recovery shadow system to provide redundancy for any primary site system including another AA.

High Availability Archive – Plasmon AA can be deployed in a high-availability mode so that a secondary archive storage unit at the disaster recovery site can be brought live immediately in response to primary site failure or down-time.

Alliance Storage Technologies offers the only enterprise-class active archive solution that ensures data permanence, authenticity, access, longevity and removability, at the low total cost of ownership that businesses demand.

Archive Without Compromise™.

Alliance is ISO 9001 certified.

© 2010 Alliance Storage Technologies, Inc. All rights reserved. Plasmon, the Plasmon logo, Archive Without Compromise, UDO, the UDO logo, UDO2, the UDO2 logo, UDO Archive Appliance and the UDO Archive Appliance logo are trademarks or registered trademarks of Alliance Storage Technologies, Inc. All other trademarks are the property of their respective owners.

CS_HIPAA 09.10



Global Sales & Marketing
Alliance Storage Technologies, Inc.
9925 Federal Drive
Colorado Springs, CO 80921
Tel: 719-593-7900
Fax: 719-593-4164
alliancestorage.com

To learn more about Alliance Storage Technologies' products and services please visit us on the web at www.alliancestorage.com.