Accelerating HIPAA Compliance with EMC Healthcare Solutions

A HealthCIO White Paper
Sponsored by the EMC Corporation

by Jonathan Bogen
2003

• E-mail: Info@HealthCIO.com • www.HealthCIO.com
This white paper describes the forces driving the need for improved storage solutions to comply with the Health Insurance Portability and Accountability Act (HIPAA) and other healthcare industry requirements. Healthcare system needs for document retention, access, and integrity controls are followed by a discussion of medical applications requiring fixed content storage. With increasing computerization of medical information, a trend to a “paperless” environment, and a vision of a lifetime electronic patient record, healthcare organizations will demand lower cost storage solutions to address this ever-increasing digital healthcare environment.

This paper also highlights the EMC Centera® Compliance Edition solution that provides a mechanism for authenticity, integrity, and access controls to meet specific HIPAA compliance requirements.
Impact of HIPAA on the Healthcare Industry

“The U.S. healthcare industry is one of the largest information industries in the world.”

The patchwork of state and federal regulations regarding health information management is coming under a set of federal regulations representing a national information infrastructure. Increasingly sophisticated technology presents opportunities in advancing healthcare, improving access and quality of care, and reducing administrative costs. In 1996, the Health Insurance Portability and Accountability Act (HIPAA Public Law 104-191) was passed with provisions subtitled Administrative Simplification. The purpose of this Act was to improve the portability of health coverage as well as the efficiency and effectiveness of the healthcare system through the development of a health information system with established standards and requirements for the electronic transmission of health information. HIPAA has important implications for all healthcare providers, payers, patients, and other stakeholders. The Administrative Simplification standards are lengthy and complex, with immediate impact being placed on healthcare organizations in the following areas:

- Standardization of electronic patient, administrative, and financial information
- Unique identifiers for providers, health plans, and employers
- Changes to most healthcare transaction and administrative information systems
- Privacy regulation ensuring the confidentiality of patient information
- Physical practices and technical procedures to safeguard data integrity, security, and availability of healthcare information

Ultimately, HIPAA will drive increasing automation to the electronic processing and exchange of information from inefficient, costly paper based transactions. In addition, this trend towards automation will be the “tipping point” towards increasing adoption of electronic medical records. These trends will drive an increasing need for improved, cost-effective storage solutions.

HIPAA REQUIREMENTS

Privacy concerns what information is covered, and security is the mechanism to protect it.

HIPAA mandates a set of rules to be implemented by covered entities and their business partners (e.g., health providers, payers, and government benefit authorities as well as pharmacies, transaction clearinghouses, and vendors and suppliers). HIPAA security and privacy requirements may be separate standards but they are closely linked. Privacy concerns what information is covered, and security is the mechanism to protect it. While the privacy rule of HIPAA applies to all individually identifiable protected health information or PHI whether it is oral or recorded in any form or medium, the security rule applies to only electronic health information. As such it will require a significant change in the way health information is handled, disseminated, communicated, and accessed. The security standard was developed with the intent of remaining technologically neutral in order to facilitate
adoption of the latest and most promising developments in evolving technology and to meet the needs of healthcare entities of different size and complexity. The privacy rule required compliance beginning on April 14, 2003, and the security rule will become effective two years later. The HIPAA Privacy Rule requires “covered” entities maintain PHI and audit disclosures for a period of six years. However, state privacy and accreditation standards may even exceed HIPAA for document retention requirements. Even though this requirement covers all types and mediums of information, the growing amount of digital information that needs to be archived may strain current healthcare organizations storage capabilities.

The HIPAA security rule is a compendium of requirements that must be satisfied or addressed. The security standard mandates numerous safeguards for records retention and protection, disaster recovery, and access controls to individual health information. A concern expressed by many healthcare organizations is the cost of addressing all or some of the standard, especially when some of the compliance requirements may seem somewhat vague. However, the security safeguards regarding the retention, protection, recovery, and accessibility of PHI are not vague and must be addressed (see below).

### Specific HIPAA Security Safeguards (Subpart C of Part 164)

<table>
<thead>
<tr>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Controls: 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.</td>
</tr>
<tr>
<td>Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic health information.</td>
</tr>
<tr>
<td>Data Backup Plan: Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.</td>
</tr>
<tr>
<td>Data Backup and Storage: Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.</td>
</tr>
<tr>
<td>Disaster Recovery Plan: Establish and implement as needed procedures to restore loss of data.</td>
</tr>
<tr>
<td>Disposal: Implement policies and procedures to address the final disposition of electronic health information, and/or the hardware or electronic media on which it is stored.</td>
</tr>
<tr>
<td>Integrity: Implement policies and procedures to protect electronic protected information from improper alteration or destruction.</td>
</tr>
</tbody>
</table>
Healthcare Industry Needs and Requirements

Today, electronic medical information needs to be accessed from multiple locations by multiple providers, hospitals or health plans. Along with the need for pervasive access to electronic health information however, come increased demands for the security of the information as well as the accompanying document retention and storage requirements for longer periods of time.

While HIPAA continues to be a top business priority among healthcare organizations, the movement to improve patient safety and reduce medical errors is gaining serious attention. Certainly, all “covered” healthcare organizations are dealing with the HIPAA privacy rule requirements and have until 2005 to implement procedures and technology to comply with the HIPAA security rule. According to a survey of healthcare CIOs, the top business issue in the 2003/2004 timeframe is reducing medical errors, closely followed by HIPAA compliance.

Healthcare CIOs’ IT and Business Priorities in 2003 *

<table>
<thead>
<tr>
<th>Priority</th>
<th>Top Business Issues</th>
<th>Top IT Priorities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reducing Medical Errors</td>
<td>Reducing Medical Errors</td>
</tr>
<tr>
<td>2</td>
<td>HIPAA Compliance</td>
<td>Upgrade Security for HIPAA</td>
</tr>
<tr>
<td>3</td>
<td>Cost Pressures</td>
<td>Implement Privacy Modification for HIPAA</td>
</tr>
<tr>
<td>4</td>
<td>Medicare Cutbacks</td>
<td>Replace/Upgrade Inpatient Clinical Systems</td>
</tr>
<tr>
<td>5</td>
<td>Improving Operational Efficiency</td>
<td>Upgrade Network</td>
</tr>
<tr>
<td>6</td>
<td>Improving Quality of Care</td>
<td>Implement a CPR</td>
</tr>
<tr>
<td>7</td>
<td>Staffing Issues</td>
<td>Implement EDI for HIPAA</td>
</tr>
</tbody>
</table>

* Based on percentage of responses as a priority from 14th Annual HIMSS Leadership Survey sponsored by Superior Consultant Company.
To drill down further into the priorities of CIOs, the top security concerns of CIOs regarding computerized medical information in 2003 are as follows:

1. Internal Breaches of Security
2. HIPAA Compliance
3. Limits of Technology

It is clear from the 2003 HIMSS survey that healthcare organizations are looking to implement solutions to improve quality and reduce medical errors while at the same time safeguarding patient health information by placing controls on information access and data integrity.

**Storage for Fixed Content**

Because of the need for rapid access to vital patient information that must be archived, a cost-effective alternative storage system is required. As an information type, fixed content has traditionally been stored for the long term on tape and optical technologies. Much of healthcare information can be considered fixed content, as it is typically static in nature. Fixed content information can be thought of as reference information such as images, medical records, e-mail, scanned or other electronic documents, and assorted medical results (e.g., lab values).

Although the industry is seeing a noticeable shift to a paperless environment, most healthcare providers still have not arrived at an all-digital hospital. Healthcare providers demand immediate access to patient information and have a vision of a lifetime patient record which will place added demands on healthcare organizations for archival and storage of electronic health information. One of the biggest drivers for information storage includes the increasing use of film-less, digital imaging systems such as PACS, supporting MRIs, CT and PET scans. Another key driver is the integration of medical devices into information systems that capture this patient information at the point of care.

The amount of information being processed by healthcare organizations extends beyond the hospital walls. For example, a recent survey of e-mail use by a state health department showed the current volume of e-mail averaging about 100,000 messages per week sent and more than 100,000 were received during that same one-week period. E-mail is one application where fixed content storage is essential and under HIPAA, mandated archiving will grow the volume of e-mail archives and associated storage capacity.

Limited access to patient information due to a temporary loss of accessibility could have consequences far beyond HIPAA such as:

- Loss of timely medical orders,
- Delays in surgery,
- Quality impact if providers cannot access electronic records,
- Legal consequences, and
- Loss of 3rd party payments, poor cash flow, and even breaches of contractual obligations.
**Centera Storage Solutions**

The Centera solution is optimized for the long-term retention, protection and preservation of fixed content information that must be retained for active reference. Centera provides healthcare organizations a cost-effective disk based alternative without the limitations or resource constraints of conventional near-line and off-line technologies. The Centera system uses a unique location independent address scheme (content addressing) to completely abstract the storage layer from the application layer alleviating the application from any material or system dependencies and completely removing the storage management and scalability challenges typically encountered by healthcare IT departments.

Centera, designed for “real-time” availability and retrieval, provides assured content authenticity for the life of the stored records, and information protection for business continuance and disaster recovery in a solution that is self-configuring, self-healing and self-managing. Using Centera’s add-on software module, Compliance Edition, healthcare organizations can enforce records retention to ensure adherence to the most stringent records management guidelines. With Compliance Edition, upon expiration of a record’s retention period, Centera can further ensure compliance with patient privacy by shredding the record beyond recoverability in excess of federal standards. This vacated capacity can now be recaptured and reallocated for reuse.

The chart below compares how Centera with Compliance Edition stacks up on each of the relevant HIPAA requirements. Centera meets or exceeds many of the requirements without subjecting the end user to the most prevalent archiving challenges including slow access, exorbitant discovery costs, technology obsolescence, information degradation and inaccessibility.

<table>
<thead>
<tr>
<th>HIPAA Standard</th>
<th>How Centera Enables Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Controls</td>
<td>Record-level Auditability</td>
</tr>
<tr>
<td>Integrity</td>
<td>Assured Content Integrity, Non-Rewriteable, Non-Erasable, Record-level Retention</td>
</tr>
<tr>
<td>Access Control</td>
<td>Centera manages authorized access and use</td>
</tr>
<tr>
<td>Disposal</td>
<td>Exceeds federal requirement for information shredding</td>
</tr>
<tr>
<td>Data Backup &amp; Storage</td>
<td>Mirroring and content parity, remote replication</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>Replication from one Centera to another</td>
</tr>
</tbody>
</table>

**Centera’s Value and Benefits**

Many of Centera’s aforementioned features effectively reduce Total Cost of Ownership (TCO) to the end user. In the healthcare industry, patient records must be retained for extended periods of time depending on the type of facility and applicable state or federal requirement. To measure or justify a major upgrade in storage technology, healthcare
organizations need to consider the cost of storing, managing and retrieving records over their entire useful life. Centera provides a number of unique features that can reduce the TCO.

- Online access – reduce discovery and retrieval times and associated costs
- Single-instance storage – reduce storage overhead by eliminating duplicate records
- Efficient content disposition – enhance patient privacy and cost of non-compliance
- Recapture deleted capacity – avoid yearly media expenditure to replace destroyed platters/cartridges
- Content addressing – location and system independent address scheme eliminates costly management and migration requirements
- Self-managing – reallocate costly human resources with a system that can manage 5-50 times more content than alternative technologies
- Self-healing – lower maintenance costs with automated information regeneration capabilities
- Record level retention-flexible depending on requirements.
- Remote replication – online replication capabilities expedites recovery time and eliminates manual intervention and media management

Centera provides a cost-effective solution to address fixed content information storage. EMC is one of the leading providers of storage solutions, including CLARiiON® and Symmetrix® storage systems. EMC professional services and software solutions help customers optimize technology utilization and system availability throughout the healthcare enterprise.

CONCLUSION

Since HIPAA will require an increasing shift to the electronic processing of health records, healthcare organizations need to guarantee that the data and information systems are secure and protected. With the potential destruction of vital patient and financial information, and of the potential legal risks involved, healthcare organizations need to fully understand their information requirements for storage and document retention. Failure to develop, implement, audit, and test information security procedures could result in serious consequences, such as legal penalties and loss of reputation, market share, and patient trust. Increasing computerization of medical information requires increasing vigilance of information systems to protect private medical information. A due diligence is expected of any business having confidential health information and especially healthcare with comprehensive document retention rules. EMC, in conjunction with leading PACS, electronic medical records and health information system partners offers with Centera a unique storage solution to enable HIPAA compliance.
HealthCIO Inc. is a Massachusetts technology consulting firm supporting healthcare organizations and other related entities by integrating business and IT policies, procedures and systems into HIPAA secure solutions. Our core mission is helping healthcare providers and information technology companies develop cost-effective and compliant healthcare strategies through training and awareness.