

Addressing Healthcare Providers' HIPAA Compliance Issues

Combining Sun StorageTek Compliance Archiving System and the Vignette Imaging and Document Management Application

APPLICATION NOTE

August, 2006

Abstract

With U.S. enforcement of the Health Insurance Portability and Accountability Act (HIPAA) now in full force, IT professionals responsible for helping to ensure compliance need access to cost-effective, end-to-end solutions for managing electronic protected health information. This paper describes how the Sun StorageTek Compliance Archiving System (the combination of a StorageTek Network Attached Storage (NAS) Appliance and StorageTek Compliance Archiving Software) and the Vignette Imaging and Document Management application (Vignette IDM) combine to offer healthcare providers a secure, end-to-end solution to augment electronic medical record (EMR) applications and to help address the management of protected health information (PHI).

Sun NAS/Vignette HIPAA Compliance

Abstract.....	1
Executive Summary.....	2
Introduction.....	3
Challenges to HIPAA Compliance.....	4
Unstructured -Documents.....	4
Infrastructure.....	5
EMR Limitations.....	5
The Sun and Vignette Solution.....	5
HIPAA Safeguards.....	7
Addressing HIPAA Safeguards with Sun/Vignette.....	9
WORM Protection.....	9
Remote Replication.....	9
Audit Trails.....	10
Scalability.....	10
Managing Unstructured Documents.....	11
Access Control and Identity Management.....	11
Pragmatic Service-Oriented Architecture.....	12
Conclusion.....	12
Glossary.....	13

Executive Summary

Health Insurance Portability and Accountability Act (HIPAA) compliance is a major concern for all U.S. healthcare organizations. As a first step, administrators and IT departments must identify and address the numerous individual compliance standards that apply to their particular organization.

These standards have evolved to address the growing number, type, and sensitivity of the records managed by the healthcare industry. In many care delivery organizations, patients' medical information is stored electronically in Electronic Medical Records (EMR) systems. The headaches associated with managing this data range from handling the sheer volume of records to dealing with unstructured content - paper documents, X-ray film and EKG strips to name a few - that is not natively supported within the EMR. When the StorageTek Compliance Archiving System is deployed in conjunction with the Vignette IDM application for high volume document imaging of this unstructured content, e-mail and desktop capture, business process workflow and case management, healthcare facilities can achieve a secure, scalable, end-to-end solution that handles the myriad types of information generated today.

Although not the focus of this paper, other technologies from Sun¹ compliment and enhance the StorageTek Compliance Archiving System/Vignette IDM solution, supporting aspects of daily healthcare office record keeping, caregiver mobility and secure access to information that further address HIPAA compliance. Sun's expertise helps healthcare customers by creating single patient views through integration of EMR systems, Enterprise Master Patient and Master Provider Indexes (EMPIs), and the ability to create a Service-Oriented Architecture (SOA) for the development and deployment of composite applications.

While the solution for healthcare customers described in this paper can be a critical part of HIPAA compliance as well as other compliance efforts; it can also help ensure smooth management of everyday office processes. With features ranging from write-once, read-many (WORM) data protection and remote replication, to audit trails and the ability to

1 Industry leading Java Identity Management Suite, host security with the Solaris 10 OS, workstation and thin client security with the SunRay secure desktop, smart card technology, SOA integration, composite application development and services consolidation with Java Composite Application Platform Suite (CAPS), the Center for Technology Governance and Compliance (CTGC) and its associated compliance services (see www.sun.com for additional information)

manage unstructured documents, it is truly a creation-to-archiving answer to managing electronic protected health information.

Introduction

While Congress originally passed HIPAA in 1996, enforcement was a staged process that depended on the size and nature of individual medical practices. That staging is over and all health care facilities are now required to be compliant. As anyone working for a care delivery organization knows, proper management and protection of protected health information is critical, and violations can result in fines of up to \$250,000².

Protected Health Information (PHI), which includes both electronic and non-electronic information, consists of individually identifiable health data such as name, address, social security number, account numbers, test results, and so on. In its electronic form, such information adds up to create a multi-terabyte-sized headache for IT departments required to retain the information securely for anywhere from multiple years to beyond the life of the patient (retention rules vary based on the situation and often the state or country in which the patient resides).³ In its non-electronic form, PHI creates a variety of other problems that will be described later in this paper.

HIPAA mandates the security, privacy, retention, access, and disaster recovery support for PHI from creation to ultimate disposition. And as with any large-scale IT effort, there are numerous challenges to ensuring a response is compliant. For a good backgrounder on technical issues associated with the management of electronic health information, including EMR systems and Electronic Health Records (EHRs), see the paper “Sun StorageTek™ Compliance Archiving System & Vignette® Enterprise Content Management: A Solution for Electronic Health Records.”

Portable storage methods such as floppy disks and CD-ROMs constituted an acceptable early-stage solution for handling and exchanging some or all EMR data. However, the mountains of data generated in the industry today means that organizations are looking to storage solutions that enhance the protection and security of electronic patient information.

2 http://www.in.gov/dhs/fire/branches/ems/hippa_present.html and other sites

3 www.4doc.com/appendix.htm

Management of electronic PHI has matured as the number of EMR systems has increased and new storage technologies have become available.

Beyond the sheer volume of new medical information and the need for confidentiality, healthcare organizations must also identify and classify that information for proper management. HIPAA, of course, is just one of the drivers behind more-efficient and accurate records management, but it's an important one.

Such comprehensive management of electronically-stored PHI is in every healthcare organization's future — regardless of size. There is federal-level interest in confidentiality and proper management of electronic health information beyond simply enacting HIPAA. For example, the Office of the National Coordinator for Health Information Technology provides leadership for the development and nationwide implementation of an interoperable health information technology infrastructure. The goal is interoperable Electronic Health Records for most Americans within the next 10 years⁴.

No healthcare organization is immune to HIPAA compliance requirements. Regardless of size, if you handle medical records compliance is in your future to one degree or another.

Challenges to HIPAA Compliance

Healthcare organizations face several virtually universal roadblocks to compliance. These include unstructured documents, insufficient infrastructure, and a lack of appropriate management tools.

Unstructured Documents

An Electronic Medical Record (EMR) system is an integrated suite of applications that attempts to address all of the functionality required to run a healthcare practice — from scheduling appointments to tracking orders and results. The challenge of an EMR system is that it needs to deliver all patient clinical results at the point of care. This is currently not easily possible due to the volume of unstructured information coming from a variety of sources.

Some EMR systems natively support discrete, coded data only. That means that many unstructured clinical results — such as X-rays, ultrasounds, EKGs, echocardiograms, historical paper charts, and documents from outside facilities, among many others — are not well supported. As a result, even an EMR system yields an incomplete electronic patient record.

Management of electronic PHI would be much simpler if all data were already in a form compatible with relational databases. But it isn't. Unstructured content is a primary challenge for compliance.

4 <http://www.hhs.gov/onchit/framework/>
http://www.hhs.gov/healthit/pres_speeches.html
<http://www.ahrq.gov/about/hitframe.htm>

Sun NAS/Vignette HIPAA Compliance

The School of Information Management and Systems at the University of California, Berkeley reports that new content is growing at 30% per year.⁵ Much of this content is unstructured, representing new types of file formats for new testing technology, Web pages, and so on. Some traditional EMR systems are incapable of handling this type of content. Vignette IDM was specifically designed to ingest and standardize unstructured content.

Infrastructure

Infrastructure refreshes represent an opportunity for “green field” hardware installations that are tailored for compliance from the ground up. And to complement these evolving storage technologies, EMR systems need to change also (or be supported by complementary technology).

EMR Limitations

Many excellent applications are available. As previously discussed, this technology merely represents a good start to addressing the whole problem. The primary limitation is that no current product can handle the vast amount of unstructured data being generated by the healthcare industry. The Vignette IDM application integrates with many EMR systems such as Epic and Cerner, among others, to help solve this problem.

Electronic Medical Record applications are an excellent start, but can't manage the entire patient record.

The Sun and Vignette Solution

Sun and Vignette combine to create a comprehensive end-to-end patient document record management solution. Given the range of records associated with an individual patient and the number of physicians that may be involved in providing care, such a total picture has been elusive. Vignette's Healthcare Imaging and Workflow solution (Vignette IDM), coupled with the infrastructure and data management technology from Sun, provides clinical users access to structured and unstructured document content from one central portal; allowing access to patient – information that was previously fragmented -- all from within an existing, familiar Electronic Medical Record system. This one-stop access to a more complete medical record greatly facilitates information retrieval. Personnel require less training and time on task to retrieve records. For example, portal-based EMR access can introduce savings ranging from \$5 to \$12 per chart pull⁶.

5 <http://www.sims.berkeley.edu/research/projects/how-much-info-2003/>

6 [“Benefits to an incremental approach: Easy view of the record, No chart pull \(\\$5 - \\$12 per pull\)”](#) Source: Nelson, Rosemarie. “Productivity Trends in

Sun NAS/Vignette HIPAA Compliance

The potential benefits of a combined Sun/Vignette solution range from cost savings to improving care through access to an end-to-end patient record.

Importantly, this streamlined access can also reduce processing errors. The Sun and Vignette solution is critical to helping healthcare providers meet quality and patient safety goals by providing a shared view of health records for patients and users across a health system. The portal is instrumental in enabling workflow and standardizing protocols across the continuum of care. It can also help reduce clinical inefficiencies and give caregivers access to important decision support data.

Figure 1 illustrates the entire system. The user sees all of the available patient documents from a single portal. This portal allows access to the information contained both in the EMR system and the Vignette Repository. Furthermore, the StorageTek Compliance Archiving System acts as additional intelligent storage either on-site or remotely (or, in the case of a replicated environment, both).

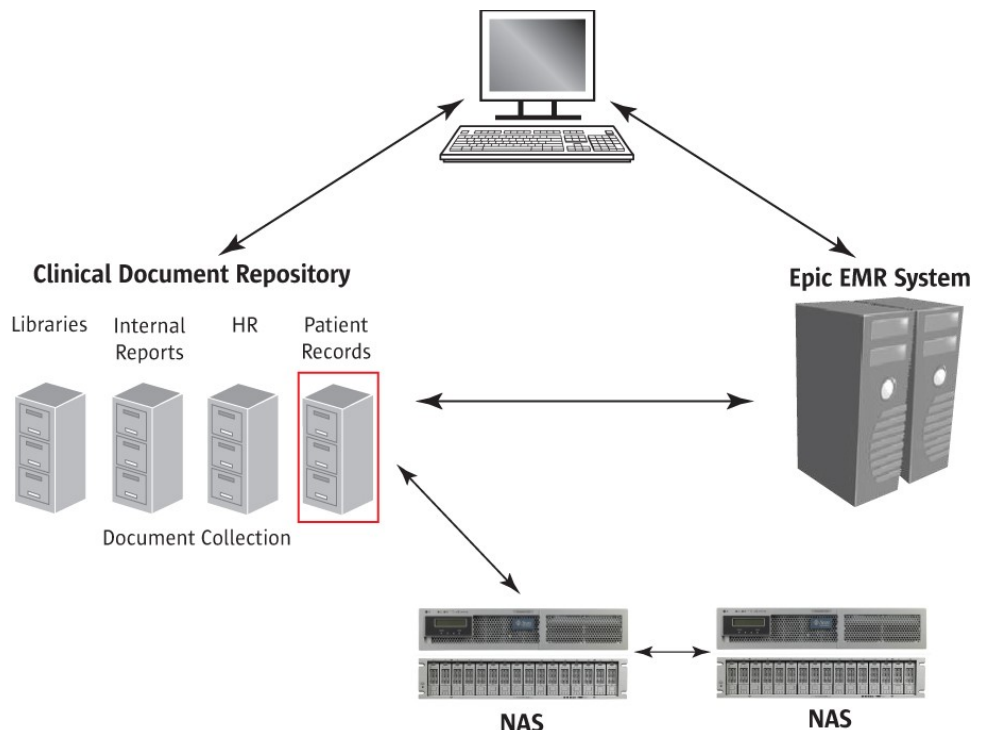


Figure 1 — The entire Sun/Vignette EHR solution. Users interface with the system from a single portal provided by the EMR application (EPIC, in this case). From this portal, the user can access the Vignette Document Repository, which in turn is supported by the StorageTek Compliance Archiving (NAS) system. In this example, the NAS storage is also mirrored to a separate site.

A key benefit of the combined Sun/Vignette solution is the ability to manage unstructured documents. The portal allows healthcare workers to

[Medical Practice Information Technology: What's the right I/T investment for my practice?" HIMSS Physicians IT Symposium. February 13, 2005. <http://www.himss.org/content/files/2005proceedings/PITS/pits06.pdf>](http://www.himss.org/content/files/2005proceedings/PITS/pits06.pdf)

Sun NAS/Vignette HIPAA Compliance

see information that was not electronic at its inception; before, it might have been paper-based, electronic, film, or any other media type. Rather than juggling several different formats, all of this information comes to the user with literally the click of a button.

The Sun StorageTek Compliance Archiving System provides cost-saving opportunities and flexibility through the use of both Serial ATA (S-ATA) disk, ideal for archiving patient information, and Fibre Channel (FC) disk storage (higher performance disk, ideal for data that is accessed more frequently). The right storage for the right data can improve competitiveness and ensure appropriate use of ever-tighter IT dollars.

IT departments can also use this network attached storage solution to store non-patient information — such as office documents or internal memos — for day-to-day access or long term archive, and for file sharing across multiple servers connected to the network. The ability to mix two types of disk in the same StorageTek Compliance Archiving System means that the system may be configured as a main storage device and archive system -- using high-performance FC disk areas to store frequently accessed data, and higher-capacity S-ATA disk storage for archive data. Another aspect of this flexibility is the ability to mix compliant and non-compliant data. In other words, while there may be no need to WORM-protect some memos, they can still utilize free space on the same storage as immutable patient information, resulting in greater deployment flexibility.

As the volume of patient information continues to grow, the cost of storing this information could become a mounting financial issue. The StorageTek Compliance Archiving System helps to enforce user quotas on storage, which can encourage more appropriate use of resources and facilitate charge backs, if appropriate.

HIPAA Safeguards

HIPAA calls for safeguards to protect sensitive patient data in three areas: administrative, physical, and technical. These safeguards come in two flavors:

- **Required** safeguards are those that *must* be followed. There is no room for argument. Complete auditability of records and record systems is an example of a required safeguard.
- **Addressable** safeguards allow for a little more latitude. Individual organizations can research each addressable safeguard to determine whether it is economically feasible and/or appropriate to their particular situation. Encryption of transmitted data is an example of an ad-

HIPAA safeguards are designated as either Required (mandatory) or Addressable (open to interpretation).

Sun NAS/Vignette HIPAA Compliance

dressable safeguard.

Sun/Vignette solutions address required safeguards in both the administrative and technical areas. Table 1 below summarizes HIPAA's administrative and technical safeguards and highlights those addressed by Sun, its partners and the Vignette solution.

Standards	Implementation Specifications R =Required, A=Addressable	
Administrative Security Safeguards		
Security Management Process	Risk Analysis	R
	Risk Management	R
	Sanction Policy	R
	Information System Activity Review	R
Assigned Security Responsibility		R
Workforce Security	Authorization and/or Supervision	A
	Workforce Clearance Procedures	A
	Termination Procedures	A
Information Access Management	Isolating Health Care Clearinghouse Function	R
	Access Authorization	A
	Access Establishment and Modification	A
Security Awareness Training	Security Reminders	A
	Protection from Malicious Software	A
	Log-In Monitoring	A
	Password Management	A
Security Incident Procedures	Response and Reporting	R
Contingency Plan	Data Backup Plan	R
	Disaster Recovery Plan	R
	Emergency Mode Operation Plan	R
	Testing and Revision Procedure	A
	Applications and Data Criticality Analysis	A
Evaluation		R
Business Associate Contracts & Other Arrangements	Written Contract or Other Arrangement	R
Technical Security Safeguards		
Access Control	Unique User Identification	R
	Emergency Access Procedure	R
	Automatic Logoff	A
	Encryption and Decryption	A
Audit Controls		R
Integrity	Mechanism to Authenticate Electronic Protected Health Information	A
Person or Entity Authentication		R
Transmission Security	Integrity Controls	A
	Encryption	A

Table 1 — HIPAA Security Safeguards (Administrative and Technical). Those that can be directly addressed by Sun, its partners and the Vignette solutions are

*highlighted.*⁷

Taking a closer look at some of the required safeguards:

- Contingency planning (a.k.a. “business continuity”) — There are several components to contingency planning. Requirements include making regular backups, disaster recovery planning, and allowing for emergency access to data. Any compliant system must be able to continue to function in the event of a major incident. Depending on the severity of the incident, a healthcare facility may need to resume operations from a mirrored system at a remote location.
- Unique user identification/authentication — Systems must ensure that every user has a unique identifier, usually in the form of login credentials. In addition, the system must verify user privileges and track all user actions while they are online.
- Record integrity — Compliant systems must ensure that files are immutable, or unchangeable. In most cases, this can be achieved with write-once, read-many (WORM) storage; however it is possible to go a step further to ensure record integrity, and this is discussed later.
- Audit controls — WORM-protected files must be covered by audit controls that allow the viewing and reporting of all actions associated with those files. Multiple attempts to access a protected file, for example, may indicate an attempt at modification or deletion.

Addressing HIPAA Safeguards for Healthcare Customers with Sun/Vignette

WORM Protection

HIPAA requires entities to implement policies and procedures that protect electronic PHI from improper alteration or destruction. At the technical level this means WORM protection. When administrators (via the Vignette IDM application) designate a file as requiring retention for a specific amount of time, it is written to the StorageTek Compliance Archiving System as a WORM file that cannot be altered or deleted for the duration of the specified retention period. So, if HIPAA requires an agency to retain certain files for 20 years, for example, the agency simply specifies an appropriate retention policy from within the Vignette IDM application. No additional management is required to remain compliant for those 20 years. At the end of that period, the file can be deleted (and the system may do so automatically if that is the organization’s policy). Also, if there are legal hold requirements due to an investigation or

⁷ For a complete description of HIPAA standards, see <http://www.hhs.gov/ocr/hipaa/>

While Administrative and Security safeguards are dealt with separately in HIPAA, there is a great deal of overlap when it comes to actual solutions. For example, access management products from Sun help healthcare customers address requirements in both these areas.

Write-once, read-many protection is a key element to any compliant system. An organization must guarantee records are secure and be able to prove it through complete system auditability.

Sun NAS/Vignette HIPAA Compliance

litigation, the retention times can be extended by the IT department or records manager via the application interface.

Remote Replication

As part of the business continuity/disaster recovery and emergency operations requirements, as well as centralizing information and IT operations, the StorageTek Compliance Archiving System supports full mirroring (remote replication) of stored data. For example, multiple NAS-enabled clinics and hospitals could replicate to a main, centralized data center. In the event of an emergency at the main site, operations can fail-over to a designated secondary business continuity site.

And while solution expenses for HIPAA compliance may not have been a consideration in Congress, it certainly is in the real world. As a cost-saving measure, the replicated business continuity site can use the denser, less expensive S-ATA storage even if the main site is Fibre Channel.

Audit Trails

HIPAA requires covered entities to implement hardware, software, and/or procedural mechanisms that record and examine activity in systems that manage electronic PHI.

Such auditing systems begin with procedural planning, but are implemented through hardware and software. The Sun/Vignette solution audit system captures and preserves successful and attempted retention-related actions in a WORM-protected log that is easily viewable by authorized users in a report. Of course, the log file data itself cannot be altered, preserving its own integrity.

Scalability

While scalability is not directly mandated by HIPAA, it is implied by the over-arching requirement to retain comprehensive PHI for all patients for long periods of time. Simply put, pervasive monitoring and new tests create mountains of data. Consider the example of how typical radiology patient profiles can add up:

- Computerized Tomography (CT) single multi-slice: 0.5 MB/image
- Spinal cervical image: 5 MB/image
- Spinal lumbar image: 10 MB/image
- Average radiology exam: 50 MB/image⁸

A single radiology patient can generate gigabytes of test information over the course of treatment. This tremendous growth in electronic PHI is part of a larger, worldwide trend.

8 <http://archive.nlm.nih.gov/pubs/data-storage/data-storage.php>

Sun NAS/Vignette HIPAA Compliance

Multiplying these figures by the number of patients, even in a modest-sized clinic the number of years that retention is required quickly yields many terabytes of data — from one department.

The aforementioned Berkeley study estimated that up to the year 2000, humankind had produced a *total* of 12 exabytes of information. It predicts that in 2009 new content worldwide will total 31 exabytes. This is the equivalent of creating 300,000 new U.S. Libraries of Congress each year.

Electronic Health Records are part of a larger trend. With the StorageTek Compliance Archiving System's ability to scale from 2TB to 224 TB today, Sun/Vignette solutions can grow to accommodate the needs of the healthcare industry.

Managing Unstructured Documents

In addition, while also not specifically mandated by HIPAA, the appropriate management of unstructured documents is implicit in any health information management system. Federal regulations do not currently *require* that all PHI be in electronic format, but that is the inevitable trend.

A Vignette IDM application feature called the document repository provides the support for unstructured content.

Vignette's Clinical Document Repository acts as a central warehouse for all medical record information.

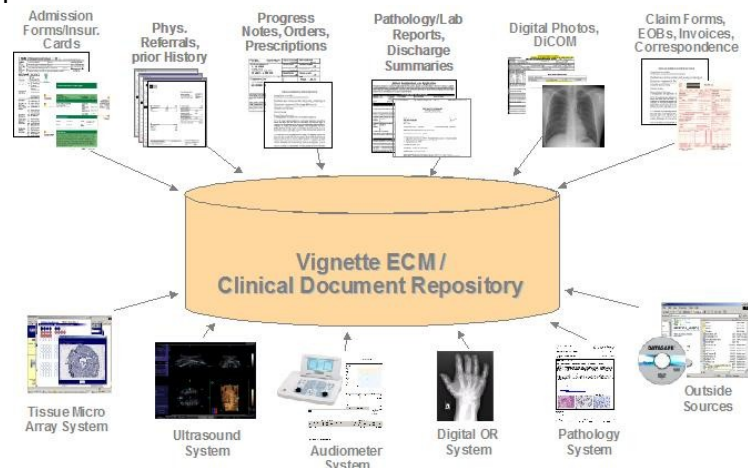


Figure 2 — *Vignette's Enterprise Content Management acts as a central warehouse for all content types.*

Capturing unstructured content is a simple process: Healthcare organizations begin by indexing documents and other unstructured digital assets using a Web-based user interface. The data can then be forwarded to a central scanning department for high-volume capture utilizing Vignette's Image Capture capabilities. These unstructured assets would then be stored in the StorageTek Compliance Archiving System where they could be accessed seamlessly via the EMR.

Sun's Identity Management solutions allow organizations to assign data access to specific roles rather than individuals. Identity management is described in detail at the Sun website and in other papers.

Access Control and Identity Management

While beyond the scope of this paper, IT managers should be aware that Sun also helps healthcare customers address HIPAA workforce security and information access management administrative standards through its comprehensive identity management product line. Identity management facilitates HIPAA privacy and security enforcement through the efficient management of identity data, entitlements, and permissions. Sun helps healthcare customers provide everything an enterprise needs to securely manage user access control to sensitive information.

Pragmatic Service-Oriented Architecture

Furthermore, Service-Oriented Architecture (SOA) can enable enterprises to better leverage and integrate IT assets, while increasing flexibility to respond to business change and opportunity. The Sun Java™ Composite Application Platform Suite (CAPS), part of the Sun Java Enterprise System delivers one of the most comprehensive and productive composite application integration platforms available for SOA. Users of the suite can deliver immediate business value through the construction of composite applications that reuse existing IT application assets in combination with newly created functionality. This enables the creation of new views of information, including Single Patient Views, master patient / provider indexes, electronic prescribing and more.

Conclusion

In the increasingly competitive healthcare field, it makes sense for organizations to employ document and records management systems with secure storage systems that not only meet federal requirements, but provide overall business advantages. The Vignette Imaging and Document Management application combines with the Sun StorageTek Compliance Archiving System to provide features healthcare organizations need to be both compliant and cost-effective.

Taking a broader view, providing solutions for healthcare means more than providing critical technologies - it also means fostering a virtual healthcare IT community that actively promotes the sharing of best-practices and new ideas. To this end, Sun - in collaboration with the Healthcare Information and Management Systems Society (HIMSS) - founded [Sun Solutions for Healthcare: Information, Networking, Education \(SunSHINE\)](http://www.sunshine-healthcare.org/)⁹ in 2003.

9 <http://www.sunshine-healthcare.org/>

Sun NAS/Vignette HIPAA Compliance

At Sun, our vision of the future of healthcare shows a world where technology comes to the aid of everyone — not just patients and practitioners but also labs, clinics, hospitals, insurers, administrators, and data centers. We see the healthcare environment of tomorrow as a single integrated community -- a place where patient information flows seamlessly across departments, facilities, regions, and even nations. It's a world where information moves almost at the speed of thought, where crucial medical records are available at the snap of a finger, where the right information gets into the right hands at the precise moment it's needed.

Building on its decades of experience working with hospitals, clinics, and insurers, Sun's recent acquisitions of SeeBeyond and StorageTek, along with its industry leading identity and access management technologies, have put the company in a position to offer end-to-end healthcare infrastructure solutions that can both improve patient care and save healthcare organizations money.

Glossary

Addressable Safeguards: HIPAA standards that are recommended, but may not be implemented by all organizations due to cost or general appropriateness.

CERNER: A third-party EMR application

ECM: Enterprise Content Management

EHR: Electronic Health Record

EMR: Electronic Medical Record application

EPIC: A third-party EMR application

HIPAA: Health Insurance Portability & Accountability Act

NAS: Network Attached Storage

PHI: Protected Health Information

Required Safeguards: HIPAA standards that compliant organization must meet.

WORM: Write Once Read Many (non-erasable, non-rewritable storage protection)

© 2006 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, StorageTek, and the StorageTek logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Vignette Corporation's Enterprise Content Management suite is a trademark or registered trademark of Vignette Corporation.