



The Security Division of EMC

White paper

Information Risk Management for Healthcare Organizations

Six Best Practices for Protecting
Your Health Information



Nearly 220 million electronic records have been breached since January 2005.

The numbers are staggering. Nearly 220 million electronic records have been breached since January 2005, according to Privacy Rights Clearinghouse (www.privacyrights.org), a non-profit consumer information and advocacy organization. 15 to 20 percent of Americans withhold information from their physicians due to privacy concerns, and as many as 85 percent of physicians may have kept information out of their patients' records due to privacy concerns*.

A recent survey of health IT executives indicated that "74 percent do not completely trust external partners to maintain the security and privacy of health data" (source: Health Information Trust Alliance, March 3, 2008).

Not only is the number of data thefts and losses due to security breaches continuing to grow at an alarming rate, the resulting monetary impact of these losses is also skyrocketing. So-called 'enterprise data loss' cost businesses and other organizations nearly \$105 billion last year, according to U.S. government estimates. Insider data breaches alone cost an average of \$3.4 million per company each year, according to the Ponemon Institute. And industry analyst firm Gartner Group estimates that the cost of recovery can reach \$150 per breached record – a number that does not factor in the monetary impact of regaining customer loyalty and rebuilding brand value, potential fines, and legal representation fees.

* Association of American Physicians and Surgeons, 2007

Contents

I. Best Practices for Preventing PHI Data Loss	page 2
II. Best Practice #1: Understand which clinical and business data is most sensitive to your patients, clinicians and the healthcare enterprise.	page 2
III. Best Practice #2: Know where your sensitive clinical data resides.	page 3
IV. Best Practice #3: Understand the origin and nature of your risks.	page 4
V. Best Practice #4: Select the appropriate controls based on policy, risk and where sensitive data resides.	page 4
VI. Best Practice #5: Manage security centrally.	page 6
VII. Best Practice #6: Audit security to constantly improve.	page 7
VIII. Developing a Strategy to Protect Enterprise Data Loss	page 8
Conclusion	page 10

At the same time that data breaches and losses are growing, healthcare systems of all sizes are embracing information technology, and collecting even greater volumes of patient and business data to optimize patient care delivery. Growth in electronic and online patient information translates to a wider distribution of that data across an increasing number of clinical and business information systems throughout the healthcare enterprise, and a diverse set of users. The result – an increased risk of compromising sensitive clinical data as more users – both inside and outside the healthcare organization – are provided with information access to collaborate on patient care decision making.

Traditional security infrastructures were primarily designed to protect against external threats. Yet today, the more imminent threats to security come from inside the organization. While the black market for information used for identity theft, fraud, and other financial gain remains robust, the focus on security has shifted to insiders with broad access to sensitive data – they know where the systems are, how they interact with each other, and what data resides on which systems. In the 19th Annual HIMSS 2008 Leadership Survey of Healthcare CIOs, 97% of CIOs admitted that they are concerned about the security of data within their healthcare organization, and 51% reported that an internal security breach is their top security concern.

This mismatch between current threats and traditional security infrastructures is leading to more healthcare data breaches, increased regulation, and higher operational costs. In turn, critical workflow processes can be negatively impacted – providing the very opposite effect that was intended by the information age and greater movement and availability of patient information

So, how can healthcare organizations protect themselves, and their patients, from a data loss catastrophe?

In order to protect the confidentiality, integrity and security of protected healthcare information (PHI), healthcare organizations must first understand where that PHI exists – whether in clinical applications, databases, storage infrastructure, patient portals, etc. – put in place policies and controls (e.g. data, access and compliance controls) to protect it from security risks as it travels throughout the infrastructure, and ensure that the whole lifecycle of the PHI is auditable.

Healthcare organizations should look to implementing an information risk management strategy, a framework based on security and health industry best practices and guidelines (such as ISO 27799 for Information Security Management, Health Informatics in the Health Sector), to ensure policies and controls for securing PHI are managed consistently across the healthcare environment.

This paper outlines six best practices for healthcare organizations seeking to prevent enterprise data loss in order to protect patient privacy and security, the health system's revenue cycle, and meet government and industry regulatory requirements.

Today, the more imminent threats to security come from inside the organization.

The HIMSS 2008 leadership survey found that nearly one in four healthcare CIOs reported a security breach in the last year.

I. Best Practices for Preventing PHI Data Loss

The HIMSS 2008 leadership survey cited that security is a top priority for healthcare CIOs, as nearly one in four reported a security breach in the last year. Identity management and security technologies were two of the top three technologies which respondents said they planned to implement for the first time in the next two years.

Healthcare organizations can leverage the strong experience of RSA and EMC for implementing the best practices that can help protect patient care data. By following these best practices, healthcare organizations can continue to acquire information technologies to improve patient care and clinical workflow, and meet internal and external compliance challenges with confidence that they can protect the security, privacy and confidentiality of sensitive patient data throughout its lifecycle. This paper outlines the Six Best Practices that can help protect patient data and move your organization's security efforts forward.

1. Understand which clinical and business data is most sensitive to your patients, clinicians, and the healthcare enterprise
2. Know where your sensitive clinical data resides
3. Realize the origin and nature of your risks
4. Select the appropriate controls based on policy, risk, and where sensitive clinical data resides
5. Manage security centrally
6. Audit security to continuous improvement

II. Best Practice #1: Understand which clinical and business data is most sensitive to your patients, clinicians and the healthcare enterprise.

Not all data is of equal importance from a security perspective. The first step in preventing enterprise data loss is to determine which patient care data is most sensitive and at highest risk. Then, you can prioritize your efforts and define appropriate policies. But how do you know which patient care data is most sensitive?

To answer this critical question, you need to understand your healthcare organizational structure, examine the various clinical departments and support departments across your organization, and identify both the regulatory and non-regulatory security drivers for each department.

For example, your healthcare finance department may need to comply with Sarbanes-Oxley and Gramm-Leach-Bliley Acts as well as SAS 70, while your clinical departments needs to focus on the Joint Commission Standards. International healthcare organizations must comply with the European Union's Data Protection Directives as well as a range of country-specific regulations, such as the Japan Privacy Act, Canada's PIPEDA, and the Australia Privacy Act – to name just a few.

Once the regulatory and corporate compliance universe is understood, you can prioritize your patient care data by grouping information into various 'classes'. For example, you might create three classes of information from the most restricted and sensitive (e.g., clinical patient care data) to the least sensitive (e.g., data pertaining to medical supplies and inventory rates).

The next step is to determine the data categories and users for each type of information. You may choose to classify certain healthcare data as 'restricted.' Then, you would determine which elements of the information are most critical and which department or business unit within the health system owns this data.

Finally, after you have classified your data, you must then define the policies – the rules for appropriate handling of the data – including which employees, clinicians, patients and other users and applications are authorized to access this data and how, when and from where they are allowed to access it. For example, you might allow all physicians to access the entire patient record at all times and from all locations, but other employees to access only specific lab data or selected clinical department data on a patient – and only during specific hours and from within the corporate firewall.

III. Best Practice #2: Know where your sensitive clinical data resides.

At first glance, the answer to the question, "Where does my healthcare organization's most sensitive data reside?" seems to be obvious. The most likely answer: "In databases, of course!" But databases are really just the tip of the iceberg, especially in today's mobile, highly collaborative healthcare organizations. HIPAA defines PHI as individually identifiable health information that is transmitted by or maintained in electronic media or any form or medium.

If data is stored in a database, then it is also stored on a disk, which is likely backed-up by other disks or tape media. Additionally, your data is likely accessed through a variety of clinical applications and from a wide array of devices, transformed on clinical workstations, physician laptops and wireless hand-helds, e-mailed to other users, and then stored on even more file servers or collaboration portals.

The answer to the question is not so obvious – yet it is critical to preventing organizational data loss. Most organizations do not take the time to conduct a thorough data discovery, leaving them with the following three choices (which are simply not viable):

- **Secure all data.** This would be enormously expensive and could only be accomplished with an unlimited security budget which is simply not realistic and would slow down patient care delivery.
- **Do not secure any data.** Government regulations mandate protection for healthcare organizations. Other risks include loss of revenue, decreased patient and provider loyalty and damage to the healthcare organization's reputation. The risks that accompany this strategy are ones that most organizations are not willing to accept.

- **Secure only a portion of your data.** This approach is often done in a haphazard manner, whereby organizations institute just enough measures to lull themselves into a false sense that patient care data is secure while ignoring significant risks.

To prevent the healthcare organization from data loss and strike the necessary balance between cost and risk, you must go beyond simply determining which databases house your critical data. Rather, you should undertake a comprehensive data discovery process which requires answers to some basic questions about your infrastructure, including:

- Do you have sensitive patient care data in databases? If so, in which database tables? In which columns or fields?
- Do you have sensitive data in file shares? If so, in which folders? In which files?
- Do you have high-risk data on clinical workstations or laptops? If so, on whose laptops?

Next, you will also need to answer data type and usage questions such as:

- Is your clinical research intellectual property unwittingly exposed through custom-built applications?
- Are your patients billing and insurance information being transferred from databases to insecure file servers so that users can create spreadsheets and reports?
- Are back-up tapes containing patient information guaranteed to arrive at their final location without interruption or tampering?

Through the data discovery process, your healthcare organization can create a map of its critical and sensitive data, which serves as a foundation for your security policy and control strategy. But in order to be effective, data discovery must be embraced as a continuous process, not just a one-time event, as neither your organization's data nor your use of it is static.

Data discovery must be embraced as a continuous process – not as a one-time event.

IV. Best Practice #3: Understand the origin and nature of your risks.

In addition to knowing where important or sensitive clinical data resides and how it is being used, you also need to understand your risks. How can your patients' data be compromised or stolen? By whom? And how much risk would your organization assume with exposure of this data?

The answers to these questions can be found both inside and outside of your healthcare environment. Lapses in processes and innocent mistakes on the part of clinical users are actually more common than a malicious attack from outside your organization. To support this, a recent study by the Ponemon Institute shows that insider threats – from negligent or malicious employees, partners and contractors and from process breakdowns – were the number one cause of data breaches in 2006. While the severity of each of these threats will vary by healthcare organization, defining that severity is essential to determining risk. The answers to all of these questions are critical in the development of your risk model.

Some of the more common risks have had their share of headlines over the last 24 months, including:

- **Lost or stolen media.** Back-up tapes or disk drives are frequently lost or stolen from data centers or en route to remote archival locations. These tapes contain confidential patient or employee information with personal information that can lead to criminal activity such as identity theft.
- **Privileged user breach.** Privileged users have been found selling sensitive patient medical records for medical identity theft, or accessing a patient record which they do not have permission to view.
- **Unintentional distribution.** Sensitive data is sent out via public e-mail, exposed on public portals or otherwise distributed to unauthorized users – which will become a greater concern as use of patient health records (PHR) expands.
- **Application hack.** A hacker (often an insider) breaches application authorization controls to access highly sensitive data through accounting applications, human resources applications and other critical business applications. For example, application developers often take production data to test new applications, violating numerous regulations and creating enormous risk.

- **Physical theft or loss.** A laptop, USB drive or other portable device containing sensitive patient data is stolen or lost, along with critical patient data stored on it.

According to a recent study conducted by Forrester Consulting on behalf of RSA, greater demands for mobile employee data access, collaboration and partner data exchange present the biggest challenges to data security today and in the foreseeable future.

Creating a risk model that takes into account all the potential ways your data might be compromised or stolen provides the context you need to implement an appropriate control strategy that outlines both the types of control mechanisms (i.e., *how* to secure the data) as well as the points of control (i.e., *where* to secure the data).

V. Best Practice #4: Select the appropriate controls based on policy, risk and where sensitive data resides.

Once you understand your policies, where your sensitive data resides and the risks at those locations in your infrastructure, you can develop an appropriate control strategy. That strategy will likely include both processes and technology.

The physical control strategy is comprised of two components: the control mechanisms (i.e., the types of controls) and control points (i.e., where in the infrastructure they are placed – at the storage, database, file server, application, network or end point). A comprehensive control strategy will include a combination of controls from all three categories described below, implemented at various layers in the IT stack:

- **Access controls control both authentication (i.e., is the user who he or she claims to be?) and authorization (i.e., what can the user do once he or she gains access?).** A wide range of products are covered in this category, including web access management, two-factor authentication and knowledge-based authentication. For example, the HIPAA Access Control 164.312(a)(1) requirement states that healthcare organizations should restrict access to information resources and allow access only to privileged entities. Healthcare providers need to limit access to health information to only those employees who have a business need to access it. The Joint Commission also recommends that existing

Where to Encrypt?

A variety of different encryption solutions are available today to help comply with requirements such as the HIPAA Encryption 164.312(a)(1) requirement which mandates the use of encryption to protect PHI from unauthorized disclosure. These solutions help enable the encryption of data at virtually any level in the IT stack: storage, database and file server, application, end-point, and network layers. Encryption addresses different risks at each layer. For example, organizations commonly encrypt the storage media (e.g., tapes) and end-points (e.g., laptop computers). While encrypting at these levels is non-invasive to applications that run above them, it only addresses the physical theft or loss of the media itself – a small spectrum of the risk model.

An increasing number of organizations are implementing encryption at both the database and file server levels because it is still relatively non-invasive to applications and provides protection against a broader range of threats, including privileged user breaches (e.g., a DBA compromising data) and

unintentional distribution (e.g., a developer using production data to test a new application).

Encrypting data at the application layer gives organizations much broader protection, securing data throughout its lifecycle as it moves from the user and end point to the application, then to the database, and finally to the underlying storage and backup infrastructure. However, this added level of protection does not come without a cost. Application encryption requires that organizations add calls to encryption systems from within the application code. While advances in these solutions have greatly simplified this process, it is still invasive. Applications that process highly sensitive or highly regulated data, such as point-of-sale systems, are prime candidates for this type of control.

The right answer to the question, "Where should I encrypt my data?" will almost always be "At a combination of these control points." And the exact mix will depend on the nature of data and infrastructure processing that data.

technology should set levels of authorization for access to patient data according to the role the user plays in a patient's care.

- **Data controls control the data itself.** Data controls include products and technologies such as encryption and key management, data loss prevention (DLP) and information rights management (IRM).
- **Audit controls provide the feedback mechanisms to ensure the policies and controls are in fact working as they should.** Often called security information and event management (SIEM), audit control products provide the means to prove compliance as well as refine policies and controls.

Over the last several years more organizations are focusing on implementing data controls, especially encryption

solutions and DLP systems (which are also sometimes referred to as "information leak protection" systems) due to the increasing number of data breaches and growing regulatory scrutiny of data privacy and integrity issues. Why? Because both encryption and DLP systems are highly effective in collaborative environments where data is mobile, shared and transformed. These two types of data controls exemplify the notion of 'self-defending data'. That is, they enable your data to defend itself.

For example, even if an individual is able to circumvent your access controls and steal encrypted data, the data is useless to them. Likewise, if highly sensitive data subject to privacy regulations is transformed and e-mailed out of an organization, a DLP system can react and protect that data. In today's highly mobile collaborative environments, these controls are indispensable.

Over the last several years more organizations are focusing on implementing data controls, especially encryption solutions.

VI. Best Practice #5: Manage security centrally.

More than any other factor, the management of control mechanisms has a greater impact on both the effectiveness of controls and their total cost of ownership. Healthcare organizations are encouraged to take an enterprise wide approach to most effectively meet required security safeguards in 3 categories:

- **Administrative safeguards** – internal policies and procedures related to data protection
- **Physical safeguards** – protection of electronic information systems, buildings and equipment
- **Technical safeguards** – processes preventing unauthorized access to data

Organizations often make the mistake of managing each control mechanism separately, which results in policy misalignment, high management costs, and a lack of business process continuity.

A more efficient approach is to manage security policies and control mechanisms centrally. Centralizing the administration of security policies ensures that control points consistently enforce security rules and makes proactive monitoring of activity that could result in a security violation easier to automate. In addition, centralization helps ensure that users consistently follow appropriate usage rules for sensitive data to avoid unintentional leakage.

The second piece of centralized security management involves encryption keys. With centralized key management, encryption controls can be effectively and consistently implemented across all control mechanisms, protecting the organization from data breaches due to human error, lost keys, or incompatible and conflicting encryption policies. For example, while all encryption products come with some form of management console, these consoles often lack higher-level, policy-based capabilities. And because each encryption product comes with a separate console, it can be nearly impossible to align the configuration and operation of these systems with the business' underlying security policies. Furthermore, different employees, often non-security staff, are tasked with managing the various encryption products, increasing management costs.

Without centralized management of both security policies and encryption keys, processes can be irrevocably broken.

Finally, when encrypted data needs to be shared between applications, groups, or infrastructures, the lack of centralized management for key sharing means either the data needs to be decrypted before sending it from one point to another and re-encrypted on the other end, causing increased overhead and vulnerabilities. Without centralized management of both security policies and encryption keys, processes can be irrevocably broken, leading to patient care and business disruption.

Organizations that do not manage security centrally encounter three significant problems:

1. **Misaligned policies.** Managing these mechanisms individually makes it difficult – if not impossible – to ensure that the organization's security policies are uniformly and consistently implemented across all control mechanisms.
2. **High management costs.** The cost of ownership is multiplied several-fold when managing these mechanisms individually, because many employees (often non-security personnel) must manage a myriad of management consoles from different vendors. Typically, these consoles are rudimentary tools packaged with the control mechanism and lack any significant policy-based management capabilities, thereby forcing users to interact with systems at a highly technical, low-level manner. This incurs significant management, training, and other overhead expenses.
3. **Lack of business process continuity.** To make a safer patient care diagnosis, healthcare organizations typically rely on the sharing of data across applications, users, infrastructure, and sometimes organizations to gain a comprehensive view of patient information. The security mechanisms in place should facilitate, not hinder, these processes, but the lack of centralized management often creates barriers between these components and can even break processes completely.

VII. Best Practice #6: Audit security to constantly improve.

As with any corporate process, a security program should have a feedback mechanism that enables the organization to assess its compliance with policy and provide feedback on the effectiveness of data controls. Because of the very nature of patient care delivery 24 x 7, and regulatory mandates such as HIPAA, Joint Commission and EU Data Directives, healthcare organizations need real-time tracking and correlation of security events in order to respond quickly to change.

SIEM (Security Information and Event Management) systems enable you to analyze and report on security logs and real-time events throughout your enterprise. To enable proper auditing of your data security infrastructure, you need an SIEM system that automatically collects, manages and analyzes the event logs produced by each of the security systems, networking devices, operating systems, applications, and storage platforms deployed throughout your enterprise. These logs monitor your systems and keep a record of security events, information access, and user activities both in real-time and for forensic analysis.

By correlating events in your data control systems – such as encryption and loss prevention – in real-time, you can quickly respond to incidents as they occur, remediating any potential losses. Such proactive log management provides the foundation for a comprehensive auditing strategy. An SIEM system enables you to regularly review your security infrastructure for:

- Incident investigation and forensics
- Incident response and remediation
- Compliance to regulations and standards
- Evidence for legal cases
- Auditing and enforcing data security policy

By establishing auditing best practices and implementing an effective SIEM system, you can reduce the cost and increase the efficiency of compliance, risk management, and forensics. Equally important, auditing provides an opportunity for continuous improvement. Security should always be viewed as a process rather than an event.

Healthcare organizations also need to conduct ongoing security training for all staff members regarding the vulnerabilities of the health information in an organization's possession and the procedures that must be followed to ensure the protection of that information. Staff members need to clearly understand "What is PHI? Am I allowed to possess PHI? How do I protect PHI? What do I do if I observe PHI being compromised or at risk of being compromised?"

A lack of centralized management of data across applications, users, infrastructure – and sometimes organizations – often creates barriers between these components and can even break processes completely.

VIII. Developing a Strategy to Protect Enterprise Data Loss

Now that you have an understanding of industry best practices to prevent enterprise data loss, how do you begin implementing them? RSA and EMC provide comprehensive solutions to help healthcare organizations through all PHI stages including contingency plans for business continuity and disaster recovery, risk assessment to control strategy to implementation.

Healthcare organizations can leverage a combination of hardware, software and services to address the best practices outlined in this paper as follows:

Best Practices #1 and 2: Determine what data is most sensitive and where it resides

Once you have classified your information, you can pinpoint all instances of the data across the network (e.g., in file systems, on desktops, and on PDAs) and when crossing network boundaries (e.g. when sent in an email).

Data discovery and classification is the first step toward securing your data, but the fact that sensitive data exists in different forms (e.g., database records, email messages, and unstructured files) and different contexts (e.g., at rest in data center storage, in motion through the network, and in use on laptops, mobile devices, and portable storage) complicates the process.

RSA® Data Loss Prevention Datacenter enables you to perform enterprise-wide classification and discovery so you can rapidly identify where the sensitive data resides in file shares, SAN/NAS, and other data repositories in your information infrastructure so that you can identify the areas where your data is at most risk. It helps you manage your sensitive data so that you can maintain compliance with industry and government regulations and protect valuable intellectual property, business strategy, and operations information. EMC Consulting Services for Security are also available to assist you with defining your data classification policy and using RSA® Data Loss Prevention Suite tools effectively.

Best Practice #3: Understand the origin and nature of your risks

The RSA® Data Loss Prevention RiskAdvisor Service provides risk assessment services to help you accurately assess the relevant risks and threats to your information, and identify the relevant policies, procedures, and controls to address those risks. The RiskAdvisor service leverages the RSA Data Loss Prevention Suite data discovery feature for finding sensitive information within the enterprise and provides a snapshot of potential exposure and a level of risk associated with it. The result of the Suite data discovery is the rapid identification of sensitive data on large data repositories, e.g., storage and file server infrastructures, desktop and laptop environments and data in transit on healthcare networks. The Risk Advisor service also encompasses a high-level mapping of business functions to sensitive data on scanned systems to help determine how sensitive information wound up in places where it should not reside.

Once organizations have a better idea of where sensitive information is located and how it got there, remediation recommendations – encompassing redesigned business workflow and other security controls – provide practical and immediate steps for the protection of sensitive information while also serving as an excellent baseline for developing a more comprehensive and ongoing data protection security program.

Best Practice #4: Select the appropriate controls based on policy, risk, and where sensitive data resides

EMC Consulting Services for Security can also help you develop an appropriate control strategy to address your risks balancing the need for physician access with adequate controls. In addition, RSA provides a range of products to enforce your security policy and control access, usage and distribution of your data throughout your infrastructure:

- RSA® Data Loss Prevention Network and RSA® Data Loss Endpoint detect sensitive data in motion across your network and in use on your laptops and desktops to help remediate incidents of violated policies. The product automatically monitors and blocks transmissions containing sensitive content to minimize required intervention and maintain compliance with regulations and corporate policy. For example, by automatically routing emails containing sensitive content to an encryption server to secure messages and attachments on-the-fly or blocking sensitive data from being copied to USB drives in accordance with content protection policies, Network and Endpoint provide enforcement of your enterprise data policies.

- RSA® File Security Manager manages encryption on both Windows® and Linux® file servers, transparently enforcing security for both the users and administrators of those file servers. RSA File Security Manager enables encryption in the file share, folder, and file levels, protecting against unauthorized use and distribution of sensitive data.
- RSA® Key Manager with Application Encryption provides application encryption and centralized key management capabilities. RSA Key Manager currently supports key lifecycle management for EMC Powerpath®, EMC Connectrix®, Oracle® Transparent Data Encryption, Native Tape with IBM® TS1120 tape drives and RSA File Security Manager.
- RSA® Access Manager centralizes access controls from a single administrative console, enabling organizations to manage "who has access to what" with the ability to delegate specific privileges to groups or departments. It provides a centralized authorization and authentication engine delivering end user convenience while significantly enhancing security and privacy controls.
- RSA SecurID® two-factor authentication is based on something you know (a PIN or password) and something you have (an authenticator). The authenticator generates a new one-time password code every 60 seconds, making it difficult for anyone other than the genuine user to input the correct token code at any given time. To access resources protected by the RSA SecurID system, users simply combine their secret personal identification number (PIN) with the unique one-time token code that appears on their authenticator display at that particular time. RSA SecurID authentication offers a wide array of one-time password authentication form factors – available in both hardware and software formats depending on business and employee needs.

Best Practice #5: Manage security centrally

RSA Key Manager provides centralized provisioning and key lifecycle management for encryption keys and other security objects throughout the enterprise. These reduce the complexity in the deployment and ongoing management of encryption controls. Key Manager application encryption and key management capabilities can also be easily integrated into specialized applications such as retail point-of-sale terminals and financial accounting systems. Key Manager can also provide a policy-driven solution for key management for encryption solutions from RSA, EMC and third parties. The RSA Data Loss Prevention Suite also provides centralized management for data discovery, classification, reporting, auditing and leak prevention capabilities.

Best Practice #6: Audit security to constantly improve

RSA enVision® technology is an information management platform for comprehensive and efficient transformation of event data into actionable compliance and security intelligence. RSA is a pioneer in security information and event management (SIEM) which has become a necessity for any company with operation-critical IT infrastructure and accountability to compliance standards. The most accurate analysis and verifiable compliance requires thorough data gathering. The RSA enVision platform has been proven to efficiently collect and protect *All the Data™* from any IP device, in computing environments of any size, without filtering and without the need to deploy agents.

RSA and EMC provide comprehensive solutions to help healthcare organizations through all PHI best practices implementation stages.

Conclusion

Protecting your health information from enterprise data loss is both a strategic necessity and regulatory requirement. The risks, including damage to patient and physician confidence and institutional reputation, are far too great to ignore. Healthcare organizations can adopt a multi-phased approach to leverage six best practices based on significant, long-term experience protecting sensitive data for thousands of organizations across the globe. By following these best practices, you can improve your ability to secure sensitive patient data, protect revenue and meet government regulations.

About RSA

RSA, The Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com/healthcare.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

SecurID, enVision, *All the Data*, RSA, the RSA logo and RSA Security are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2008 RSA Security Inc. All rights reserved.

PHIBP WP 0708