ABSTRACT

Compliance with federal regulations governing privacy and security of health information is mandatory and yet, many healthcare organizations are far from meeting all requirements. This white paper presents the challenges imposed by evolving HIPAA and ARRA HITECH rules, along with best practices for addressing those requirements with trusted IT solutions. The paper also includes information on EMC solutions that meet the latest regulatory specifications for security, data protection, and availability. This important guidance will help healthcare providers optimize quality and safety of patient care while minimizing risk of non-compliance and associated financial penalties.

January, 2014
TABLE OF CONTENTS

EXECUTIVE SUMMARY .................................................................................................................. 3

INTRODUCTION ............................................................................................................................. 4

EMC CAPABILITIES FOR DELIVERING TRUSTED IT .................................................................. 5

ADVANCED SECURITY ..................................................................................................................... 6
  Encryption ..................................................................................................................................... 6
  Enterprise-wide Security Management ......................................................................................... 7
    Identity and Access Management ............................................................................................ 8
    Information Rights Management ............................................................................................. 8
  Secure Software and Hardware Development .......................................................................... 9

CONTINUOUS AVAILABILITY ......................................................................................................... 10
  Active-Active Data Centers ...................................................................................................... 10
  Continuous Data Protection ...................................................................................................... 11

INTEGRATED BACKUP AND RECOVERY ..................................................................................... 12
  Enterprise-wide Backup and Recovery ...................................................................................... 13
  Backup Security ........................................................................................................................ 13
  Application Integration ............................................................................................................. 13
  Archiving .................................................................................................................................. 14

HEALTHCARE IT PROFESSIONAL SERVICES .......................................................................... 15
  Security Services ........................................................................................................................ 15
  Data Erasure Services .............................................................................................................. 15
  Continuous Availability Advisory Services ............................................................................. 15
  Assessment Services ................................................................................................................. 15

TRUSTED IT BEST PRACTICES ................................................................................................... 16

CONCLUSION ............................................................................................................................... 17
EXECUTIVE SUMMARY

HIPAA rules pertaining to privacy and security of health information are being enforced more stringently than ever before. In addition, healthcare organizations striving to attest to the EMR meaningful use provisions of HITECH are running out of time to qualify for federal funding and could risk being fined for failure to comply. To fully meet the requirements of HIPAA and ARRA HITECH, healthcare organizations must abide by the Final Rule, which specifies requirements for security, data protection, and availability of protected health information (PHI) and electronic PHI (ePHI).

To adequately comply with the final rules of the meaningful use guidelines, healthcare organizations need to deploy trusted IT solutions as part of a comprehensive IT transformation that includes virtualization, cloud computing, and IT-as-a-Service business models. EMC has extensive subject matter expertise and experience in designing and deploying trusted IT infrastructures specifically for the healthcare industry.

This white paper presents the challenges healthcare organizations often face in complying with the final rules. It also provides information on trusted IT solutions from EMC that specifically address HIPAA and HITECH requirements for security capabilities such as encryption, integrated backup and recovery, and continuous availability of vital medical and patient information.

In addition, the paper includes best practices for choosing and deploying trusted IT solutions that ensure compliance while maximizing operational efficiency and reducing costs.

By following the guidance offered in this paper, healthcare organizations will have the information and insights needed to meet the requirements of the final rules with a trusted IT infrastructure that supports optimal safety and quality of patient care.
INTRODUCTION

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) introduced rules governing privacy and security of all protected health information (PHI) and electronic protected health information (ePHI). While some HIPAA rules have been enforced more vigorously than others, the ARRA Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 has specified significantly more stringent requirements.

In addition to requiring meaningful use of health information technology, such as electronic medical records (EMR), HITECH contains provisions that strengthen the civil and criminal enforcement of HIPAA rules. Time is running out for healthcare providers to comply with these rules and avoid serious financial penalties.

Healthcare organizations have until June 30, 2015 to comply with these rules or sacrifice significant federal funding available for stage 2 meaningful use (MU2). In addition, failure to meet MU1 requirements by 2015 will result in a penalty on Centers for Medicare & Medicaid Services (CMS) reimbursements, starting at 1 percent and rising annually.

On September 23, 2013, all healthcare organizations were required to adhere to the Final Rule of HITECH. This rule contains detailed requirements for

- encrypting all PHI data on storage devices,
- protecting PHI data with backup and recovery, and
- ensuring availability of PHI within a reasonable amount of time following a disaster or site outage—reasonable being considered hours as opposed to days.

Enforcement is expected to be stringent. After June 30, 2014, the Office of the National Coordinator for Health Information Technology (ONC) will conduct random audits on up to 10 percent of healthcare organizations attesting to MU1. Those failing the audit could be forced to return all federal funds received for meaningful use, ranging between $2 million and $7.5 million per hospital. In addition, healthcare organizations that suffer a security breach, lose PHI data, or fail to recover quickly enough following a disaster may be investigated by the Office of Civil Rights (OCR) and could face fines of up to $1.5 million1.

Meeting the final rule requirements is not optional. These latest regulatory developments underscore the urgent need for trusted IT solutions that provide necessary levels of security, data protection, and availability for any application or infrastructure handling PHI.

In addition, healthcare providers should deploy trusted IT solutions as part of a larger IT transformation based on extensive virtualization and adoption of IT-as-a-Service (ITaaS) to achieve increased performance, efficiency and agility of their overall infrastructures.

---

EMC® can help healthcare organizations close gaps in their IT infrastructure and achieve compliance with the final rules. EMC offers decades of healthcare industry experience and a dedicated staff of healthcare IT experts steeped in the latest federal regulations governing management and protection of PHI and ePHI.

In addition, EMC offers a comprehensive portfolio of trusted IT solutions spanning advanced security, integrated backup and recovery, and continuous availability. EMC invests millions of dollars annually in certifying EMC technologies with major healthcare clinical and business applications. EMC has staff working with application development teams at healthcare vendors—including Cerner, Epic, and MEDITECH—to ensure optimal performance and interoperability.

EMC also applies industry best practices for security, data protection, and availability to every aspect of hardware and software design. The result is a suite of trusted IT solutions that directly address the requirements of HIPAA and HITECH, including:

- **Advanced Security** – encryption from the infrastructure to the end-user device, integrated governance and compliance management, identity and access management, and security analytics
- **Continuous Availability** – active/active architectures, integrated disaster tolerance, and point-in-time recovery
- **Integrated Backup and Recovery** – enterprise-wide data protection solutions, backup-as-a-service, backup monitoring and analytics, archiving, and direct integration with healthcare applications

A broad range of EMC professional services are available to assist healthcare providers in planning, designing, and deploying these solutions to not only achieve meaningful use, but also facilitate IT transformation and enable ITaaS.
ADVANCED SECURITY

The world of data security has changed dramatically, rendering many traditional techniques ineffective and posing tough challenges for healthcare providers to prevent exposure of PHI. Simply building firewalls around the perimeter of the enterprise network is no defense against stealthy, new forms of attacks. Persistent identity thieves can almost always enter and often move through systems gathering information for weeks before detection. Once discovered, the next challenge is responding fast enough to avoid loss of PHI.

Some state regulations require prompt notification of security breaches. California, for example, now requires discovery of breaches within five days. Ideally, the response should be within a few hours at most. Unfortunately, organizations usually discover security attacks too late, respond too slowly, and capture too little information for effective resolution.

Virtualized clouds with dynamic pools of resources shared across multiple applications and devices demand more sophisticated security strategies. For example, today’s clinicians increasingly use their own mobile devices to access the EMR, extending the reach of security solutions well outside traditional data center boundaries.

With tightening HIPAA and HITECH requirements, healthcare organizations must move beyond traditional security methods to advanced security solutions that enable a more strategic, proactive stance against intrusion (Figure 1).

![Figure 1 – Evolution to Advanced Security](image)

Healthcare organizations today require a multi-layered, trusted IT infrastructure embedded with advanced security capabilities that span encryption, risk management, data loss prevention, identity management, predictive analytics, and governance.

Encryption

To effectively protect PHI from the data center to mobile devices, data encryption must be an integral part of the healthcare IT environment. While organizations can comply with the final rules by documenting their intent, encryption is the only safe harbor from prosecution if a security breach occurs.

In the data center, EMC recommends deploying solutions with data at rest encryption (DARE). For example, EMC VMAX® enterprise storage offers D@RE, a hardware-based, on-array encryption solution that protects information from unauthorized access even when drives are removed from the system. RSA® Embedded Key Manager is built into D@RE to provide a unique digitally encrypted key for each drive in the array, including spare drives (Figure 2).
For Big Data requirements such as Picture Archiving and Communication System (PACS) images, healthcare providers may choose Isilon® scale-out storage, which uses Vormetric encryption to protect sensitive information. With this solution, individual departments can protect data with a unique encryption key, preventing anyone without that key from accessing the information.

In healthcare organizations with unencrypted storage arrays, RSA Data Protection Manager (DPM) secures sensitive data at the point of capture with encryption or tokens. DPM enables users to manage policies and lifecycles of keys and tokens across the healthcare enterprise.

For protection in the cloud, EMC Atmos® object-based cloud storage with optional GeoDrive software provides built-in encryption for secure access to files.

As another option for the cloud, AFORE offers software-defined storage encryption and application encryption solutions. AFORE’s CloudLink virtualized security appliance features enterprise-controlled encryption with flexible key management for virtual machines. AFORE’s CypherX solution extends security beyond traditional perimeters by placing applications in secure virtual containers and encrypting all data to protect PHI from cyberattacks or malicious internal activity.

**Enterprise-wide Security Management**

Healthcare organizations must take a holistic view of security management by adopting an integrated approach to governance, risk, and compliance (GRC). To align appropriate security activities for maximum protection across the enterprise, EMC developed a security management framework comprised of:

- **Business governance** – embedding security into all organizational structures and processes while taking into account regulatory requirements (HIPAA, HITECH) and internal policies
- **Security risk management** – identifying and classifying information risks and tracking risk mitigation
- **Operations management** – implementing security processes and controls in line with security policy to prevent risks from developing into security incidents
- **Incident management** – detecting, analyzing, resolving, and reporting security incidents to minimize their impact
To make this framework a reality, healthcare organizations need a tightly integrated portfolio of security management solutions. The RSA Archer™ eGRC Suite manages every element of an enterprise GRC program—policy, risk, compliance, enterprise, incident, vendor, threat, business continuity, and audit—from a centralized screen. The RSA Archer eGRC Suite also enables healthcare organizations to build a registry of risks, map them to business processes and structures, pair known threats with identified vulnerability issues, and report on risks and threats in real time.

By integrating the RSA Archer eGRC Suite with RSA Data Loss Prevention (DLP) Suite, healthcare organizations can extend these capabilities even further. RSA DLP Suite finds, classifies, and protects PHI at every point in typical daily usage—on application servers or end-user devices, in transit over networks, and at rest in storage media.

These capabilities are further enhanced with RSA Security Analytics, which offers security monitoring, incident investigation, long termarchiving and analytics, malware analytics, and compliance reporting via a unified, browser-based interface. Unlike traditional perimeter security solutions, Security Analytics captures and analyzes large amounts of log data alongside full network sessions and other data to identify threats, policy violations and suspicious behavior across the healthcare enterprise.

Identity and Access Management

Healthcare organizations need a business-driven Identity and Access Management (IAM) solution to help securely manage access to sensitive patient information, deliver access in a timely manner, and ensure appropriate levels of access. To fully comply with healthcare compliance regulations such as HIPAA, healthcare organizations must have a unified view of users and their access privileges. HIPAA requires that organizations are able to regulate and enforce user access. Since this is nearly impossible in fragmented environments, EMC recommends a formal IAM program.

The program should include "segregation of duties" policies as required by HIPAA, so that users with authority to access PHI are kept separate from unauthorized users. Due to HITECH’s expanded scope, organizations must also ensure proper access control for any outsourced functions, such as payroll or collections.

The RSA Identity Management and Governance (IMG) solution addresses these needs by providing a business-driven approach to managing identities and governing access, which empowers clinical and business departments to determine access decisions. RSA's approach ensures that enterprise applications such as EMR and HIS are protected using granular controls and entitlements to define access based on individual roles and responsibilities within the healthcare system.

Information Rights Management

With information shared more broadly across providers, exchanges, insurers, and government agencies, information rights management has become an essential layer of protection. EMC Documentum® Information Rights Management (IRM) prevents unauthorized access to secured content so healthcare organizations can maintain control of sensitive information outside the firewall. This is particularly important for securing access from mobile devices by providing persistent protection of documents, messages, and attachments at rest, in transit, and upon delivery. Documentum IRM also provides a continuous audit trail to demonstrate proof of compliance with HIPAA, HITECH, and internal security policies.
Secure Software and Hardware Development

With trusted IT solutions, security is built in at the deepest levels to prevent intrusion and avoid data loss. EMC follows the development practices recommended by the Software Assurance Forum for Excellence in Code (SAFECODE), which are proven to strengthen security.

EMC has adopted these practices as part of a comprehensive, secure software engineering framework that spans policy, people, processes, and technology. For example, administrative controls for critical platforms such as EMC’s unified storage and scale-out storage incorporate security into the core product designs and not as add-on solutions. As a result, a broad range of EMC and RSA products have been awarded Common Criteria certification, an internationally recognized ISO standard for security.

In addition, EMC has built a set of software, standards, specifications, and designs for common software security elements such as authentication, authorization, audit and accountability, cryptography, and key management using RSA technology. By providing an open interface for these capabilities, EMC facilitates integration of its products with the broader security architectures of individual healthcare organizations.

EMC also works directly with leading healthcare application vendors that provide EMR, radiology, cardiology, and pathology solutions to integrate security between EMC’s products and their applications.
CONTINUOUS AVAILABILITY

Traditional approaches to data availability such as offsite tape storage and standby systems will no longer be adequate to meet the latest HIPAA and HITECH requirements. Retrieving tapes and manually starting up offsite systems could easily take days. To be compliant, healthcare organizations must be able to recover fully within hours.

Whether an outage is caused by natural disaster, widespread power loss, system failure, or human error, every minute of downtime affects quality and safety of patient care—and can incur hefty financial consequences. For example, in a large hospital with hundreds of physicians and thousands of other clinicians, just five minutes of downtime could equate to millions of dollars in lost productivity. Longer outages could add government penalties for regulatory violations, internal and external legal expenses, as well as the cost to recover lost data.

Ultimately, the goal for any healthcare organization should be continuous availability of systems, applications, and data (Figure 3). Virtualizing environments is a key enabler of continuous availability because it allows greater mobility of VMs and workloads from one physical system to another. This also underscores the importance of IT transformation and ITaaS as they decouple IT services from the underlying infrastructure.

![Figure 3 – Evolution to Continuous Availability](image)

Active-Active Data Centers

To move toward continuous availability, EMC recommends deploying an active-active infrastructure, which protects against technical faults and larger outages. A key solution for active-active operations is EMC VPLEX®, which enables data mobility and access across multiple data centers.

Through distributed federation of physical resources, VPLEX enables two separate data centers to act as one, so that VMs, applications, and data are accessible from either site simultaneously. If services are lost at one data center, they automatically continue to run from the other data center with no disruption to applications or clinical services. VPLEX also provides the flexibility to relocate workloads from one site to another and minimize planned downtime for maintenance or upgrades. During normal operating conditions, VPLEX allows transparent load sharing to maximize efficiency and performance. Different VPLEX products are available to handle mobility across local, metropolitan, and geographically separated distances (Figure 4).
While VPLEX virtualizes storage in this active-active configuration, it also works with VMware Site Recovery Manager to achieve seamless mobility of VMs across the two sites. This is facilitated through tight integration across EMC storage platforms, including VMAX and VNX®, and VMware vSphere Storage APIs for Array Integration (VAAI). In addition, the EMC Virtual Storage Integrator (VSI) plugin for VMware vCenter greatly simplifies mapping of VMs to the virtualized storage. With this integrated, virtualized, and geographically distributed data center environment, healthcare organizations can achieve a recovery time objective (RTO) of zero, which brings them well within compliance of HIPAA requirements.

**Continuous Data Protection**

Adding EMC RecoverPoint® to the VPLEX environment addresses another important requirement for data availability—point-in-time recovery (Figure 5). RecoverPoint provides continuous data protection (CDP) by capturing data so it can be played back to a specific point in time in a similar fashion to a digital video recorder (DVR).
INTEGRATED BACKUP AND RECOVERY

With data growing at an average of 40 percent annually, healthcare organizations are finding it increasingly difficult to complete backups within an appropriate timeframe. Some organizations are backing up databases as large as 30 terabytes, which can slow performance of EMR and other critical applications, potentially affecting quality and efficiency of patient care. In addition, backups can often fail for various reasons including application time out, network issues, or simple media failures, which create risk of data loss. Many organizations struggle with creating offsite copies or replicating backup data to a remote facility, which is a requirement of HIPAA and HITECH. Failure to achieve appropriate levels of data protection and maintain a disaster recovery plan can result in hefty fines for non-compliance with HIPAA and HITECH rules.

Backup scenarios also are becoming more complex as mergers and acquisitions result in multiple backup systems across an enterprise. As data grows in size and complexity, some healthcare providers struggle with interpreting the rules for governance and compliance. Several HIPAA mandates and state laws require long-term retention of data, such as medical images. Questions arise regarding a reasonable timeframe for retaining backups. Recovery time also is a more pressing requirement now that tighter controls dictate recovery in hours versus days. But how many hours for recovery are acceptable, especially when patient safety is at stake?

To accelerate backups and recovery, healthcare organizations are moving away from tape—which has a history of poor reliability, high cost, and intensive administrative requirements—to disk-based backup. For greater assurance of meeting regulatory requirements and achieving increased control, healthcare organizations should also centralize backup operations. In addition, providers need to adopt processes and technology for archiving data according to long-term-retention requirements consistent with federal and state guidelines.

As IT departments at healthcare providers transform their organizations to support ITaaS, another logical option is backup-as-a-service, particularly for multi-hospital health systems. With this approach, multiple hospitals share a common backup resource that is securely segmented to provide each participant with dedicated backup. In addition to this multi-tenant scenario, individual hospitals may choose to simply consolidate all backups to the cloud or back up to a common local target and replicate to the cloud. This same process also is available for long-term data archiving.

Regardless of whether a healthcare organization uses a multi-tenant or centralized cloud solution, EMC recommends an integrated approach to backup and recovery (Figure 6). This ensures that backup software and hardware communicate seamlessly and enable single-step recovery.

EMC backup and recovery solutions address three key objectives that every healthcare organization need to ensure compliance: 1) achieve complete, reliable backups of all data, 2) integrate to healthcare applications and clinical workloads, and 3) scale efficiently to handle continuing growth in data.
Enterprise-wide Backup and Recovery

In addition to the sheer volume of data in today’s clinical environments, backups are further complicated as healthcare providers transition to a virtualized infrastructure. Virtual machines (VMs) tend to proliferate rapidly, and since each VM represents a unique backup job, this can result in overrunning backup windows. According to IDC, only 75 percent of all data created is copy data and 25 percent of data is unique. That means, healthcare IT is backing up the same data over and over again.

EMC solves this problem with solutions like EMC Avamar® deduplication software and system, which performs deduplication of physical systems and VMs at the client so far less data is backed up. Avamar is a turnkey appliance, eliminating the need for separate backup servers. It supports large data center backups, as well as backups from smaller physician offices or clinics, including individual laptops and mobile devices, all with one centralized solution.

For VMware environments, EMC embeds Avamar in VMware ESX Server, as well as the VMware vStorage API for Data Protection (VADP) toolset. This enables VMware users to easily perform guest- or image-level backups within the VMware environment.

Avamar integrates with EMC Data Domain to extend the capability and backup use cases found in healthcare IT departments. EMC Data Domain® deduplication storage system deduplicates data during the backup and archive process, achieving a 10-30 times reduction in backup storage required. Its architecture is designed for secure, reliable backup and recovery, and Data Domain Replicator software provides safe offsite storage that eliminates the need for tape. Data Domain systems also can scale extensively by simply adding appliances.

Deduplication is critical to ensuring cost-effective data protection. For example, using deduplication for backup allows IT departments to efficiently replicate data across great distances to ensure proper disaster recovery. Because EMC employs global deduplication, only unique blocks of data are moved between sites, which can reduce network traffic during replication by as much as 99 percent. EMC uses variable block deduplication to maximize deduplication rates, which reduces application resources and data center floor space.

EMC NetWorker® is a unified backup and recovery software solution that provides enterprise-class data protection across multiple platforms, including integration with Avamar and Data Domain to maximize opportunities for deduplication. NetWorker centralizes backup management for the entire healthcare system and supports a broad range of environments, from small remote clinics to large health system campuses. EMC NetWorker is integrated with EMC storage technologies to make it easier to execute and manage snapshots and CDP technologies built into EMC VNX and EMC VMAX storage arrays.

Finally, EMC Data Protection Advisor is an essential tool for real-time monitoring and reporting on the entire data protection environment, regardless of the technology in use. DPA collects and analyzes information from physical or virtual backup servers, backup storage, and replication environments to help IT make informed decisions about modifying the backup environment, promptly resolve issues, and continuously measure service levels to maintain compliance.

Backup Security

As with primary data sources, ensuring data security in the backup environment is essential. EMC recommends using industry-standard RSA BSAFE FIPS 140-2 validated cryptographic libraries, which are integrated in both Avamar and Data Domain.

With Avamar and Data Domain encryption software, backup data can be secured in transit and at rest on target backup storage. Centralized encryption key lifecycle management also can be integrated into the data protection environment with RSA DPM.

Application Integration

EMC Data Protection Solutions also work together to help healthcare providers evolve from using isolated backup solutions to a backup and recovery infrastructure that is directly integrated with clinical and enterprise applications.

For example, Data Domain offers Data Domain Boost software that extends the deduplication process to the data source while using a high performing IP protocol. When deployed with Oracle RMAN, Data Domain Boost increases backup performance and efficiency of Oracle-based application backup. In this way, Oracle database administrators directly manage their backup and recovery processes, greatly reducing time and effort typically required in traditional data protection environments. Similar direct integration is also available for other enterprise databases and applications, including Microsoft SQL, SharePoint, Exchange, SAP, Sybase, and IBM DB2.

Another example of application integration is Data Domain’s VMWare Instant Recovery function. With this feature, administrators can run a live VM directly on Data Domain from data that was backed up by Data Domain. Users can then recover files that they need directly from the live VM and then vMotion the application back into production for instant recovery.

In addition, EMC is working with major EMR and EHR partners to enable integrated backup and recovery that fully complies with the final rules. For example, EMC has developed a backup module specifically for MEDITECH—NetWorker Module for MEDITECH (NMMDI)—to streamline backups of the MEDITECH database environment directly to Data Domain. This approach provides a single, integrated solution that often reduces backups to as little as one hour with equally rapid recovery.

Archiving

In some data protection scenarios, backup is not practical due to volume or type of information. For example, PACS images are often extremely large and rarely updated. Rather than consume expensive production storage and repeatedly back up the same images, EMC recommends moving these files to a secure archive that keeps them readily accessible and guarantees that they can never be altered or deleted without authorization. Archives should also be replicated for disaster protection.

EMC offers a variety of archive solutions, which are driven by customer use case and application demands. In some cases, applications benefit from archiving to network-attached storage while object-based storage is a preferred archiving repository for other applications.

For example, EMC Centera is an object-based archiving solution based on a purpose built storage array that is highly available and tolerant of multiple points of failure. Centera uses an API or gateway to attach to a wide variety of EMR, PACS, VNA, and file archiving solutions.

EMC Isilon scale-out storage provides a highly scalable, secure, and efficient way to archive Big Data like PACS images while enabling rapid access. With Isilon, healthcare organizations can consolidate image data from each departmental PACS into a single, unified archive solution. This lays the foundation for adopting a Vendor Neutral Archive (VNA) to reduce costs and improve operational efficiency.

Often enterprise data such as email can become unwieldy for backup. An effective approach retains only 30 days of email data in the production environment and archives anything older. This strategy eliminates the need to repeatedly back up the same data while keeping important communication records secure to meet compliance requirements. EMC SourceOne allows IT organization to centralize archiving of email, file, and SharePoint data, as well as conduct advanced searches of massive repositories and legal holds of sensitive documents.
HEALTHCARE IT PROFESSIONAL SERVICES

EMC security, continuous availability, and integrated backup offerings are complemented by several Healthcare IT Professional Services to help ensure the success and compliance of transformational IT projects.

Security Services

HIPAA regulations require that healthcare organizations perform internal audits to verify compliance with EMR meaningful use, including security requirements. To provide a non-biased validation of such audits, EMC Consulting works with Redspin, a global leader in penetration testing services and IT security audits.

As part of an EMC Consulting engagement, Redspin will compare a healthcare organization’s security controls to those required by HIPAA to identify any gaps. The analysis also determines if implemented security controls match documented policies and procedures. Following the analysis, the EMC and Redspin team will report on any vulnerable areas and recommend corrective action to meet Final Rule requirements.

Data Erasure Services

Security must be maintained any time a system is decommissioned, whether returning it at the end of a lease, retiring it permanently at end-of-life, or repurposing assets for another use. If PHI resides on those systems, healthcare organizations must ensure that it remains secure even if there is no intention to reuse the systems.

EMC helps healthcare organizations protect information at every stage of the information lifecycle with EMC Data Erasure Services. Using proprietary techniques, these services thoroughly wipe all data from individual disks, as well as entire arrays. Once data has been erased, EMC provides a comprehensive report and certificate of completion to prove compliance. EMC’s Data Erasure Services also are validated by an external third party to ensure that erased data can never be recovered.

Continuous Availability Advisory Services

To help healthcare organizations efficiently plan, design, and build trusted IT infrastructures that maximize system, application, and data availability, EMC Global Services offers Continuous Availability Advisory Services. Drawing on EMC’s extensive subject matter expertise in healthcare and availability technologies, these services evaluate current capabilities, identify gaps, produce architecture designs aligned with specialized requirements, and perform a full cost-benefit analysis to justify the solution.

Following industry best practices and using proven technologies, EMC Global Services can help healthcare organizations quickly and efficiently deploy the availability solutions they need to meet HIPAA and HITECH requirements as important deadlines approach.

Assessment Services

Healthcare organizations also can use one of several EMC assessment tools at no cost to help them better understand their environment, including data types, data growth rates, and backup statistics.

- **FSA/ESA/SSA** – Assesses file, email, and SharePoint environments with an in-depth analysis of unstructured and semi-structured data in use at a healthcare system.
- **Backup Assessment** – Provides a detailed look at the backup environment including performance, growth, and client data, with minimal effort
- **Oracle RMAN Assessment** – Organizes backup information by database for Oracle back-ended clinical applications
TRUSTED IT BEST PRACTICES

Based on decades of healthcare IT experience, combined with regulatory knowledge and technical expertise, EMC has developed a set of best practices to guide healthcare organizations on their journey to HIPAA and HITECH compliance.

Regulatory rules are complicated and subject to interpretation. Healthcare organizations often don't know where they stand or how to move forward. EMC recommends beginning with a detailed assessment of existing security measures, backup and recovery systems, and availability levels to identify gaps.

Once gaps are identified, healthcare providers should choose appropriate solutions to address specific requirements within each area requiring remediation.

For example, ensuring availability of an Epic EMR requires specialized understanding of that unique environment. The encryption approach used in a Cerner environment will not necessarily be the same for MEDITECH. And, backing up McKesson patient folders with millions of small files requires a substantially different approach compared to backing up Epic's gigabyte-sized databases. "Cookie cutter" solutions simply are not effective.

To address such specialized requirements, EMC runs a dedicated solutions lab to help certify, benchmark, and validate EMC solutions that are integrated with applications developed and marketed by its healthcare application partners. This investment allows EMC to accelerate time to market of the latest technologies and incorporate best practices with its healthcare application providers.

As healthcare organizations plan and design a trusted IT environment, it is important to embrace an enterprise-wide approach that integrates security, backup and recovery, and availability solutions. Integrated solutions ensure smooth interoperability for improved efficiency and stronger protection.

In addition, healthcare providers need solutions that have Common Criteria certification and follow industry best practices for secure software development, such as those prescribed by SAFECode.

Trusted IT solutions should also be an integral part of IT transformation and ITaaS initiatives to maximize opportunities for improving security, data protection, and availability while increasing overall infrastructure efficiency and agility. A major part of IT transformation must include virtualization. Virtual environments are more agile and enable greater data mobility for disaster recovery. Virtualized environments also can take advantage of hybrid clouds for faster, more efficient backup and recovery.

EMC recommends automating security, data protection, and disaster recovery procedures as much as possible. Automation avoids risk of human error, ensures consistency, and executes recovery processes often in minutes instead of hours or days typically required by manual methods.

Finally, healthcare organizations should verify and test their trusted IT environments often to ensure they comply with HIPAA and HITECH rules and meet RTO and RPO goals. This is the best way to avoid fines and, most importantly, verify that the systems and information required for efficient, quality patient care are properly protected.
CONCLUSION

Stringent rules for HIPAA and HITECH compliance are coming to bear in the near future. Understanding these rules and deploying trusted IT solutions to comply are essential for maximizing opportunities for acquisition of federal funds and avoiding hefty financial penalties.

Beyond meeting regulatory requirements, healthcare providers also stand to gain many strategic benefits by making trusted IT an integral part of a virtualized cloud infrastructure.

For example, virtualized infrastructures require less physical space and have lower power and cooling demands, reducing costs significantly. In addition, automation is an inherent characteristic of virtualization and cloud environments, which greatly eases administrative burdens on IT staff. This not only lowers operating costs even further, but also frees time and resources for innovation and strategic healthcare IT initiatives.

By ensuring security, protection, and availability in a virtualized cloud, healthcare providers minimize risk of data loss or inability to access vital PHI, thus ensuring optimal quality and safety in patient care. Medical information and patient health records can be securely accessed virtually anytime, anywhere—whether at the bedside or from a physician’s mobile device—also aiding in the efficiency and responsiveness of care.

As regulatory rules continue to evolve, virtualization offers greater flexibility to adapt trusted IT solutions to maintain compliance. In general, healthcare providers gain more agility to quickly deploy new services, respond to industry changes, and efficiently absorb mergers and acquisitions. With trusted IT solutions and a virtualized cloud, healthcare organizations have the best assurance of meeting their long-term patient quality and safety requirements, while reducing costs and exceeding operational objectives.