White Paper

Securing Protected Health Information

David LaBrosse, NetApp

Monty Zarrouk, NetApp

March 2016 | WP-7222

Abstract

Clinical data is critical to providing excellence in patient care. If this data falls into the wrong hands, healthcare organizations might be subject to legal liabilities and financial penalties for failing to comply with data security regulations. These organizations also might suffer from negative impacts on the healthcare brand. The HITECH Act mandates that breaches of 500 records (or more) of protected health information (PHI) must be reported to the Office of Civil Rights (OCR) under the Department of Health and Human Services (HHS). With the surge in security breaches of healthcare information, it has never been more important to embrace security as a key aspect of every healthcare organization's strategic plan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Healthcare Security Challenges

Having the ability to protect and store critical data is a major focus of today's organizations. To guard against advanced threats in a complex and evolving climate of virtualization, cloud services, and mobility, healthcare organizations must increasingly take a data-centric approach to safeguarding their sensitive information.

Security is top of mind for healthcare leaders, with regulations mandating the confidentiality, integrity, and availability of health information. The healthcare industry represents a significant target for unauthorized access to protected health information (PHI). Patient records now sell for more money than a credit card on the black market—stolen health credentials can go for $10 each, about 10 or 20 times the value of a U.S. credit card number.[1] With this information, hackers use stolen data for insurance fraud schemes, unauthorized use of credit cards, and, in some cases, security breaches that can lead to other issues, including patient safety.

Figure 1) Confirmed security incidents in 2014.

Source: 2015 Verizon Data Breach Investigations Report

Largest Healthcare Data Breaches in 2015

In 2015, 185 providers reported PHI breaches that affected over 6 million patient records. According to the Redspin 2015 Breach Report, a total of 1,437 large breaches of PHI affecting 154,368,781 patients were reported since HITECH went into effect in 2009. Although insurers bore the brunt of hacking attacks, healthcare providers were victimized as well. Of the PHI breaches, hackers factored in six of the eight largest incidents of the records reported breached.[2]

Table 1) Top healthcare security breaches in 2015.

Provider	Records Reported	Type of Breach	Information Breached
Anthem	78,000,000	Hacking / IT incident	Stolen network credentials
Premera Blue Cross	11,000,000	Hacking / IT incident	Stolen network credentials

[1] Source: Don Jackson, Director of Threat Intelligence at PhishLabs
[2] Redspin 2015 Breach Report: "Protected Health Information," February 2016

Provider	Records Reported	Type of Breach	Information Breached
Excellus Health Plan	10,000,000	Hacking / IT incident	Network server
UCLA Health	4,500,000	Hacking / IT incident	Network server
Beacon Health Systems	306,789	Hacking / IT incident	E-mail
Empi Inc. and DJO	160,000	Theft	Laptop
Advantage Consolidated LLC	151,626	Hacking / IT incident	Other
Jacobi Medical Center	90,060	Unauthorized access	E-mail

Source: Redspin 2015 Breach Report: "Protected Health Information," February 2016

2 Cybersecurity Regulations and Business Drivers

2.1 Healthcare Regulations

With the significant number of PHI records breached during 2015, the federal government increasingly focuses on working with the healthcare industry to improve its track record in protecting patient information. On December 18, 2015, the Cybersecurity Act of 2015 was signed into law to provide the healthcare industry with clearer guidance for protecting against cybersecurity threats.[3] The bill requires the Department of Health and Human Services (HHS) to:

- Report to multiple congressional committees on the healthcare industry's preparedness for cybersecurity threat responses.
- Select a leader to head cybersecurity initiatives and detail methods for addressing threats across its health divisions.

Making cybersecurity a higher priority for the HHS is a good first step, but healthcare organizations also need to escalate their focus on protecting PHI.

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 sets national standards to protect the privacy of PHI, with requirements embedded in the Medicare and Medicaid EHR Incentive Programs. Under HIPAA, covered entities[4] must:

- Put in place safeguards to protect patients' health information.
- Reasonably limit uses and sharing of PHI to the minimum necessary to accomplish the intended purpose.
- Have agreements in place with any service providers they use to perform functions or activities on their behalf. These agreements are to ensure that these service providers (referred to as "business associates") use and disclose patients' health information properly and safeguard it appropriately.
- Have procedures in place to limit who can access their patients' health information as well as implement training programs for themselves and their employees about how to protect their patients' health information.

[3] http://hitconsultant.net/2015/10/29/senate-cybersecurity-bill-5-key-facts-healthcare-organizations/
[4] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

Additionally, the Breach Notification Rule[5] requires most healthcare organizations to notify patients when there is a breach of unsecured PHI. The Breach Notification Rule also requires these entities to promptly notify the Secretary of Health and Human Services of any breach of unsecured protected health information. In addition, the rule requires the entities to notify the media and the public if the breach affects more than 500 patients.

Health Information Technology for Economic and Clinical Health (HITECH)

The Health Information Technology for Economic and Clinical Health Act of 2009 provides privacy and security of patient health information. The HITECH Act extends HIPAA with new requirements that affect many more entities, businesses, and individuals. These requirements:

- Strengthen requirements for Business Associate Agreements—business subcontractors who perform activities involving the use or disclosure of individually identifiable health information.
- Establish new security breach notice requirements.
- Increase penalties from $50,000 per occurrence to $1.5M per occurrence.
- Give state Attorneys General more power.
- Link health IT practices to NIST standards for Safe Harbor[6] privacy provisions.

2.2 Business Drivers

Cybersecurity Trends in 2016

To avoid the negative impact of a privacy or security breach, there is increased pressure on healthcare executives to invest in security solutions in 2016. Multiple business and regulatory drivers are forcing healthcare organizations to implement more comprehensive security solutions, including:

- Invest in better security solutions and practices to **safeguard patient data** and demonstrate compliance with government regulations (HIPAA, HITECH, and so on).
- Create a "**comprehensive security**" model that includes physical, administrative, and technical security risk assessments to ensure that organizational security policies, procedures, and IT operations comply with HIPAA and HITECH guidelines.
- Purchase larger "**cybersecurity insurance**" policies to help with the high costs of recovering from attacks. The debate on whether healthcare organizations should invest in prevention or in recovery is ongoing. Because it might not be possible to stop every privacy or security breach, there are valuable arguments that both options should be implemented.
- Prepare for the increase in planned and unplanned federal **security audits**. Security experts advise that the best security practice is to conduct ongoing internal audits to prevent hospital resources from becoming complacent with security practices so that each hospital department complies with regulatory guidelines.
- Invest in **analytics software** that will help healthcare organizations (especially large insurance companies and big hospital groups) to identify unusual and unauthorized access to their patient data or PHI.

[5] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
[6] http://www.usinternet.com/company/safe-harbor-privacy-statement.htm

Areas of Focus

Cybersecurity will be a primary challenge as healthcare organizations increase use of mobile and cloud platforms. Because of the rapid adoption of electronic health records (EHRs), healthcare organizations might want to take the following steps to reduce the security risks:

- **Encryption of EHR Data**. As more mobile devices access EHRs, healthcare IT must investment in encryption solutions for PHI in transit and at rest. Patient data and images should be **"view only"** on mobile devices, and they should not be stored in the mobile device SSD or memory. EHR data at rest should be encrypted so that organizations can take advantage of Safe Harbor opportunities.
- **User Access Authorization**. Healthcare IT must enforce strict authorization for end-user access to PHI. The EHR system needs to monitor and manage user access by both local employees and networked users across the region. For example, a radiologist from a private clinic might require access to the hospital's EHR data to conduct MRI scans of a patient's injured knee and must have the proper system access authorization. In addition, the EHR system should monitor and log usage by the radiologist to ensure that patient privacy and security standards are supported.
- **Analyze Security Logs and User Access.** Another best practice for healthcare IT is to frequently monitor and review reports on user access patterns. Doing so might require investing in additional software tools that can identify unusual sign-on and systems utilization activities. Some software packages require additional "analytics" capabilities to identify intentional or unintentional privacy and security breaches. For example, a hacker might steal an authorized user's login and password. Because the credentials being utilized are authentic, the system will not know that the hacker is stealing patient data until an unusual usage pattern is identified in an analytics report.
- **EHR Applications in the Cloud.** The adoption of cloud computing continues to rise as healthcare organizations take advantage of cost savings and operational efficiencies. During contract negotiations with EHR cloud providers, healthcare organizations need to review and question how the cloud provider will support HIPAA, HITECH, and other regulatory compliance and business associate agreements. The contract should include language that stipulates how the cloud provider will maintain compliance, including sharing copies of audits.

3 NetApp Security Solutions

The ability to protect and store critical data is a major focus of today's healthcare organizations. With the appropriate data security technologies installed, healthcare organizations can guard against potential malicious attacks and attempts to steal PHI.

NetApp Solutions

NetApp, working with partners, delivers a comprehensive portfolio of solutions to secure confidential data at rest across physical and virtual data centers, disaster recovery sites, and cloud infrastructures.

Table 2) NetApp security solutions.

NetApp Security Options	
NetApp Storage Encryption	Uses self-encrypting disk drives for full disk encryption (FDE) of data with the NetApp® Data ONTAP® operating system.
NetApp AltaVault®	Delivers enterprise-class data protection and storage at up to 90% less cost than that of on-premises solutions. Securely backs up data, reduces risk, and speeds recovery with encrypted backup data to any cloud. AltaVault can also be securely integrated with IBM SoftLayer cloud solutions.

NetApp Security Options	
E-Series	NetApp SANtricity® software FDE combines local key management with full disk encryption or FDE-capable drives, protecting data from unauthorized access or modification resulting from theft, loss, or repurposing of the disk drives.
Gemalto SafeNet KeySecure	Provides high availability across the infrastructure with clustered appliances, instantly replicating configuration information to dramatically improve failover capabilities and fault resiliency for geographically dispersed data center deployments. (Supports NSE, AltaVault, NetApp Cloud ONTAP® software, and other Key Management Interoperability Protocol encryption solutions.)
Gemalto SafeNet Virtual KeySecure	Provides customers with a virtual appliance that manages and securely stores a maximum of 25,000 keys, supporting up to100 concurrent clients.
Gemalto SafeNet Virtual KeySecure for Cloud ONTAP for AWS	Maintains data confidentiality on NetApp Cloud ONTAP through efficient centralized key management and by enforcing customized security policies surrounding data access using Amazon Web Services (AWS).
Splunk	Splunk real-time analysis of security logs is one of the most common methods of real-time security analysis. Operational intelligence software enables healthcare to monitor, report on, and analyze live streaming and historical machine-generated data. Splunk helps users distill, sift, and understand machine data to improve service levels, reduce IT operations costs, mitigate security risks, enable compliance, and create new product and service offerings. Splunk also provides a quick, cost-effective System Information and Event Management (SIEM) tool to help healthcare customers pass security audits. Gartner ranks Splunk in the top-right quadrant for SIEM solution providers. Splunk competes against IBM, Intel, and other large vendors.

3.1 Encryption Is a Good Start

Encryption has become more mainstream because it secures data from unauthorized access or theft. This technology guards sensitive data, even if files are copied or disk drives are stolen. Although there are many different security mechanisms to choose from, data encryption is the most effective in protecting confidential information. And, with centralized key management and a hardened root of trust, healthcare organizations can protect their master keys and secure their data. Although HIPAA and HITECH do not require using encryption for compliance, healthcare organizations benefit from Safe Harbor provisions when utilizing encryption technologies.

With encryption, organizations have peace of mind that their data can't be read by unauthorized users and external attackers.

- **Protect data from evolving threats**. Sharing data is a standard way of doing business. With the growing sophistication of attacks on the enterprise network, it is critical to not only protect against breaches but also have processes in place to recover from loss. With encryption, data can't be read by anyone except authorized users.
- **Demonstrate compliance**. Regulatory mandates dictate that organizations comply with data privacy requirements. With tracking and reporting capabilities, organizations have the tools to provide the required auditing reports.
- **Safeguard data in the cloud**. As organizations move to cloud-based services, storage network encryption protects data used in cloud-based applications without impacting user productivity.

The use of encryption is a critical component in protecting sensitive data across the organization. Whether it's hardware or software based, encryption is not only secure, but also fast and easy to use. Security measures are effective only if confidential data is protected.

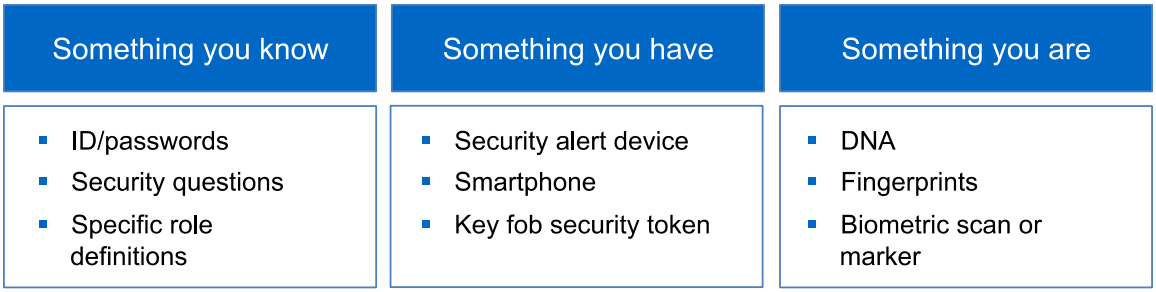
NetApp, working with partners, delivers a comprehensive portfolio of encryption solutions to secure confidential data at rest. NetApp does so while centralizing and simplifying encryption key management across physical and virtual data centers, disaster recovery sites, and cloud infrastructures. By integrating the SafeNet KeySecure products by Gemalto with NetApp disk encryption technologies and NetApp storage solutions, organizations can secure important information from unauthorized access or theft. Organizations can also meet data security and compliance initiatives and preserve their company's reputation by avoiding publicized loss of data.

3.2 Prevent Unauthorized Access to PHI with Multifactor Authentication

Stolen login information or identity credentials are the cause of many breaches. If the system thinks a user is authorized (because the user has the correct ID and password), then hackers can exploit that weakness and steal patient data. That is why it is important to have "multifactor" authentication.

NetApp solutions support several of the multifactor tools used today. The typical multifactor model requires the end user to have all, or a combination of, the following verifications and authorizations before being granted access to data.

Figure 2) Examples of multifactor authentication.



Gemalto SafeNet MobilePASS

Gemalto provides an outstanding multifactor authentication tool called SafeNet MobilePASS. NetApp works closely with Gemalto on encryption and key management solutions and can help facilitate a discussion on multifactor authentication.

MobliePASS requires end users to not only have a secure password ("something they know") but also to enter a randomly generated six-digit number ("something they have") when they log into a system. This second form of authentication ensures that only the individual in possession of the smartphone can enter the six-digit code. This requirement makes it more difficult for external or remote hackers to break into a system.

Another good security practice is for system users to create a PIN access code for their smartphones. Doing so makes it difficult for a criminal to use the SafeNet MobilePASS security feature when a smartphone is lost or stolen. Although it might be irritating to have to reenter a PIN code or pattern on a smartphone, doing so provides an additional layer of protection.

3.3 Recovery Plans Are Equally Important

NetApp AltaVault cloud-integrated storage enables customers to securely back up data to any cloud at up to 90% less cost compared to that of on-premises solutions. This feature allows healthcare organizations to include the public and private cloud as part of backup and recovery strategies for cost-effective data protection. Healthcare organizations achieve faster recovery, reduced data loss, ironclad security, and minimal management overhead.

Accrediting organizations such as The Joint Commission and DNV have traditionally focused much of their IT-specific survey efforts on organizational disaster recovery planning activities. With Medicare's evolving Conditions of Participation, these organizations are shifting their focus to demonstrable recovery capabilities within an organization. With AltaVault, recent backups are intelligently cached on local systems for rapid restores while older versions are vaulted to the cloud. Because backups are on quickly accessed disk technology versus traditional tapes, organizations can rapidly demonstrate the ability to restore data. This ability makes both the organization and the surveyor confident that data is not only being backed up but can be reliably and quickly restored.

With AltaVault, data is compressed, deduplicated, encrypted, and streamed to the cloud gateway appliance.

Customer Reference

"Our NetApp AltaVault and OpenStack–supported backup service makes it easy for customers to check off all those boxes for regulations compliance, such as encryption and off-site copies."

Frank Tollefson, Assistant Director of Network Services
INHS/Engage

The solution makes it possible to establish off-site data backup and retention for compliance purposes:

- Data is encrypted and secure at all times, in flight and at rest, using AES 256-bit encryption. Data also complies with FIPS 140-2 level 1 (certification in progress) and industry-standard SSL or TLS encryption.
- Encryption keys are managed locally by your security department.
- The solution provides role-based access controls and integration with TACACS and RADIUS.

3.4 Security Intelligence Is Key to Understanding Threats

NetApp helps healthcare organizations maximize time to value from clinical data with validated solutions for analytics, data warehouses, and business intelligence. Working with Splunk and NetApp, customers have the ability to aggregate machine data to detect, investigate, and report on security incidents on a validated platform. Below are advantages that customers can achieve when they invest in Splunk and NetApp together.

- Get enterprise-class reliability for big data analytics workloads.
- Achieve faster time to value—validated, optimized designs are ready to be deployed to quickly start analysis, data mining, and business intelligence processes.
- Scale healthcare IT infrastructure without losing performance and keep up with explosive data growth.

NetApp provides a storage infrastructure for Splunk deployments that delivers optimal and consistent performance with minimal maintenance and expense. Competitors frequently overarchitect and overcharge for Splunk infrastructure.

- The NetApp E-Series storage system provides improved performance, data availability, scalability, data protection, and single-interface storage management compared to that of Splunk workloads running on commodity servers with internal drives.
- The NetApp EF560 and the E-Series use the same chassis, which is employed in thousands of installations that demand high-performance, dense, cost-effective storage. Together, these storage systems have a proven record of five-9s reliability across deployed systems.

Together, these building blocks also are configured to support the Splunk hot, warm, cold, and frozen data tier model. Operations can effectively accelerate data indexing and searching with flash and minimize cost and space for colder data with high-capacity near-line SAS drives.

3.5 Physical Security Is Growing

Meet the Challenges of Video, Surveillance Data Throughput, Retention, and Retrieval

Concerns over security, crime, and terrorism have driven the creation of massive video surveillance infrastructures, increasing the demand for video storage. The NetApp Video Surveillance Storage solution offers superior storage to meet the advances in next-generation video and analytic surveillance technology.

The E-Series storage system uses a modular architecture for a true pay-as-you-grow solution to address growing data storage requirements. Leading intelligent video security, combined with E-Series storage, handles the bandwidth-intensive streaming environments of next-generation video surveillance infrastructures. With those two systems you get:

- Consistent, high-performance bandwidth for media-intensive video streaming environments
- Performance-tuned solutions that deliver high-availability access to media content
- Superior performance to and from network video recorders (NVRs) for greater camera support and fewer NVR instances
- The ability to leverage your investment in video cameras and networks and maintain productivity with high-availability storage

4 Summary

As government regulations and internal policies drive increasing demands on how PHI is protected, identifying storage solutions that keep sensitive information secure has become a high priority for healthcare IT. NetApp, working with partners, delivers a comprehensive portfolio of security solutions to guard clinical and business data from unauthorized access or theft. These solutions also meet data security and compliance initiatives and preserve healthcare organizations' reputations by avoiding publicized loss of data.

Appendix

U.S. Federal Agencies for Security Governance

The following table lists the different federal government agencies that are responsible for healthcare security governance. The area of responsibility and links to the websites are provided for quick reference.

Federal Office / Agency	Health IT–Related Responsibilities	Website
Centers for Medicare and Medicaid Services	• Oversees security and compliance	https://www.cms.gov
Office for Civil Rights	• Administers and enforces the HIPAA Privacy, Security, and Breach Notification Rules • Conducts HIPAA complaint investigations, compliance reviews, and audits	www.hhs.gov/ocr

Federal Office / Agency	Health IT–Related Responsibilities	Website
Office of the National Coordinator for Health Information Technology	• Provides support for the adoption and promotion of EHRs and health information exchange • Offers educational resources and tools to assist providers with keeping electronic health information private and secure	www.HealthIT.gov
National Institute of Standards and Technology, U.S. Department of Commerce	• Sets computer security standards for the federal government and publishes reports on topics related to information technology security	http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
State and Local Governments	• Some states have additional restrictions; for example, mental health data might have different rules for confidentiality	State specific

U.S. Accrediting Agencies

The following table lists the different federal government agencies that accredit healthcare organizations in the United States. The area of responsibility and links to the websites are provided for quick reference.

Accrediting Agency	Health IT–Related Responsibilities	Website
Centers for Medicare and Medicaid Services	• Oversees security and compliance	https://www.cms.gov
Joint Commission	• Accredits and certifies nearly 21,000 healthcare organizations and programs in the United States	http://www.jointcommission.org
DNV GL	• Provides quality-driven accreditation and clinical excellence certifications to America's hospitals	http://dnvglhealthcare.com

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.