Hewlett Packard Enterprise

Business white paper

Building Blocks of a Sound ePHI Security Program

Beyond HIPAA Compliance

Table of contents

Executive Summary

IT professionals in today's healthcare organizations have to contend with urgent operational demands, critical cyber threats, and heightened regulatory scrutiny. To meet all these challenges, IT organizations need to take a holistic, long-term, and comprehensive approach to data security. This paper looks in detail at the changing market dynamics and demands in play, and it offers a set of best practices that healthcare organizations can employ in order to establish an effective security program to fully protect sensitive patient data.

Introduction: Security Challenges in Healthcare, and Increasing Urgency to Address Them

Today's healthcare organizations are grappling with unprecedented changes, and unprecedented challenges. Following are a few of the demands these organizations are confronted with:

- **Growing regulatory pressure.** Since the Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996, a lot has changed. Since then, additional rules came in the form of the Health Information Technology for Economic and Clinical Health (HITECH) Act. Then, in 2013, the final HIPAA Omnibus Rule was instituted to significantly enhance patient privacy protections and strengthen the ability of the government to enforce compliance with the law. The result is that healthcare organizations have more rules to adhere to, and face bigger penalties if they fail to comply. In fact, two organizations were fined a total of $4.8 million for a privacy violation.[1]
- **Increasing threats.** Healthcare data represents an increasingly valuable asset to identity thieves and other cyber criminals, and is increasingly being targeted as a result. Given the value of the data they manage, healthcare organizations are contending with security threats that are more sophisticated and more frequent. Since 2010, attacks in the healthcare industry have increased 125%, and 91% of organizations have experienced at least one breach in the past two years.[2] The theft of this data can be devastating. While consumers can change a credit card number if there's a breach, they can't change their medical histories and other personal details, which leaves them exposed. For healthcare organizations, these breaches are extremely costly. In fact, security incidents are now estimated to be costing U.S. hospitals up to $6 billion annually.[3] Further, it is important to stress that the costs of breaches go well beyond finances. The fines and other direct costs can pull resources from strategic initiatives that could have otherwise ultimately served the organization's core mission for care and service improvements. Similarly, the efforts and distraction of breaches—including remediation, forensics, and so on—distract staff from their core responsibilities. Breaches can also inflict significant damage to an institution's reputation, which can have long-term, and far-reaching consequences.

[1] NPR, "Fines Remain Rare Even As Health Data Breaches Multiply", Charles Ornstein, February 27, 2015. **http://npr.org/blogs/health/2015/02/27/389328345/fines-remain-rare-even-as-health-data-breaches-multiply**.

[2] Security Week, "Healthcare Organizations Face Spike in Data Breaches From Criminal Attacks", Brian Prince, May 07, 2015.

[3] Security Week, "Healthcare Organizations Face Spike in Data Breaches From Criminal Attacks", Brian Prince, May 07, 2015.

- **Shifting IT landscape.** For IT security teams tasked with guarding against breaches, the battleground continues to shift in fundamental ways, which can introduce new risks or exacerbate existing ones. For example, the adoption of cloud-based services raises the potential of exposure given many traditional controls can't be applied in these environments. Plus, there is often a lack of clarity between the customer and provider in terms of respective security responsibilities and roles. In just a few years, mobile devices and applications have fundamentally altered the landscape. Now, 88% of healthcare organizations permit employees and medical staff to use their own mobile devices to connect to the organization's networks.[4] Further, medical devices have also grown increasingly networked and mobile. Big data is being employed with growing regularity, resulting in the increasing aggregation—and potential exposure—of sensitive records and assets. All this change creates increasing pressures for security teams to adapt and expand their security controls. These groups can't simply keep data behind a firewall and expect data to be protected. In fact, the very notion of a secure perimeter continues to erode.
- **Changing business and operational requirements.** In recent years, healthcare IT organizations have been tasked with supporting such initiatives as Medicare and Medicaid EHR (electronic health record) Incentive Programs and the exchanges instituted in conjunction with the Affordable Care Act (ACA). These initiatives, and the pace at which they've had to be enacted, have created a host of new risks in many organizations.

For all these reasons, enhanced security safeguards are coming to be an increasingly urgent and critical mandate, one that is gaining intensified focus for CIOs, CSOs, and other executives at the highest levels of the organization. For the healthcare leadership responsible for addressing today's security requirements, the following sections offer a series of best-practice considerations and approaches.

Step #1: Focus on Security, Compliance will Follow

As healthcare organizations seek to mitigate risks of breaches and non-compliance, they need to embark on their initiatives with a clear understanding that compliance does not equal security. It is important to focus on instituting a holistic, comprehensive, long-term, and sound security program, rather than taking a tactical approach that's focused on checking the boxes associated with specific compliance requirements. Quite simply, the chief objective needs to be implementing effective safeguards that protect against evolving threats and mitigate the risk of devastating breaches.

Further security should be considered across virtually all IT and business initiatives—and the sooner the better. By involving security teams in initiatives early rather than later, they can avoid having to retrofit implementations to address security requirements, and avoid the delays and extra costs these last-minute efforts can introduce.

[4] Information Week, "Obamacare Vs. Patient Data Security: Ponemon Research," Alison Diana, March 13, 2014.

IT leadership will also be well served by identifying risks and addressing security gaps. In this effort, it is important to leverage frameworks that provide proven, sound guidance in terms of the security elements and processes that should be in place. Today's leadership teams can choose among a range of frameworks, including National Institute of Standards and Technology (NIST) standards 800-66 and 800-53, International Standards Organization (ISO) 27001/27002, Unified Control Framework, and myCSF. NIST 800-53 in particular represents an excellent source of guidance for implementing security in an organization.

Step #2: Do Effective Risk Analysis and Risk Management

To secure sensitive assets, you need to start by identifying where they are. While at a high level, this sounds like a basic, obvious concept, it is not at all straightforward for security teams. Administrators need to understand and document the ePHI data flow in the organization, including where it is created, received, maintained, stored, and transmitted. For the areas in which ePHI data resides, it is also vital to assess what the environments are like and how they are configured. As part of this effort, IT teams need to define:

- Which systems and elements contain ePHI, including specific applications, databases, file servers, SANs, and so on.
- The network architecture, including all ingress and egress points.
- Business processes that may be in place for accessing, updating, or copying ePHI.

It is important to stress that this documentation should be established for any location the organization's ePHI data resides, including any cloud providers, hosting providers, technology partners, or any other external entities. This is important because, even if a breach occurs at the third-party's site, the healthcare organization whose data is breached can still suffer from significant brand damage and other penalties.

Finally, once this documentation has been established, there has to be a consistent interval for reviewing these factors over time to ensure documentation stays current and accurate. Not only is this documentation a critical first step, it can be a way to establish credibility with any third-party auditors that the healthcare provider may work with.

Once you know where ePHI resides, you can then effectively map it to the controls in place. However, while it is important to establish controls, it isn't enough. These controls need to be informed by a thorough risk analysis. Going through a rigorous risk assessment and risk management effort are two of the top requirements of HIPAA. In these efforts, it is important to leverage guidance from the Department of Health and Human Services' Office for Civil Rights (OCR) as well as security frameworks like NIST 800-30.

Step #3: Identify Where Existing Security Technologies are Leaving Gaps

In today's healthcare organizations, a sound security program requires range of technologies, including the following:

- Encryption solutions
- User authentication
- Anti-virus
- Security information and event management (SIEM)
- Federated identity management (FIM)
- Data loss prevention (DLP)

However, many of these traditional security technologies are leaving a gap in defenses. Many are not capable of mitigating insider threats. Firewalls, anti-virus, and other defenses are routinely being bypassed by external attacks. Within organizations, traditional approaches to data-at-rest security don't offer any protection against advanced threats. For example, if an attacker leveraging Advanced Persistent Threat (APT) techniques gains access to an application, database encryption won't prevent the attacker from getting access to data.

The problem is that these traditional technologies tend to protect silos, that is, a specific network ingress point or database, but they don't address sensitive data across its lifecycle. Further, many of these technologies are not equipped to offer security in cloud-based environments, or to contend with the implications of mobile devices or big data applications. Traditional technologies like database encryption can either present obstacles to strategic big data initiatives—for example by restricting aggregation and manipulation—or sensitive assets would need to be decrypted before they are imported into the big data environment, which would pose significant risks.

As your organization looks to embark on an initiative for better safeguarding ePHI, you should look to follow these high-level guiding principles:

- **Leverage automated rather than manual controls.** Instead of simply training employees about password complexity, institute automated directory controls that ensure that simple or default passwords aren't used. By enforcing policies in an automated fashion, your organization will be able to substantially reduce the instances of policy or compliance breaches.

- **Implement preventative rather than detective measures.** Look to establish controls that can prevent attacks, rather than implementing detective controls, that is, controls for helping with forensics after an attack.
- **Leverage data-centric security controls.** In the end, what matters most is the security of the data, the ePHI that represents a highly sought after target for malicious insiders and external attackers. To effectively address compliance objectives and risks, healthcare organizations must take a data-centric security approach. What is data-centric security? Step #4 reveals the unique characteristics and advantages of data-centric security solutions.

Step #4: Establish Data-Centric Security Controls

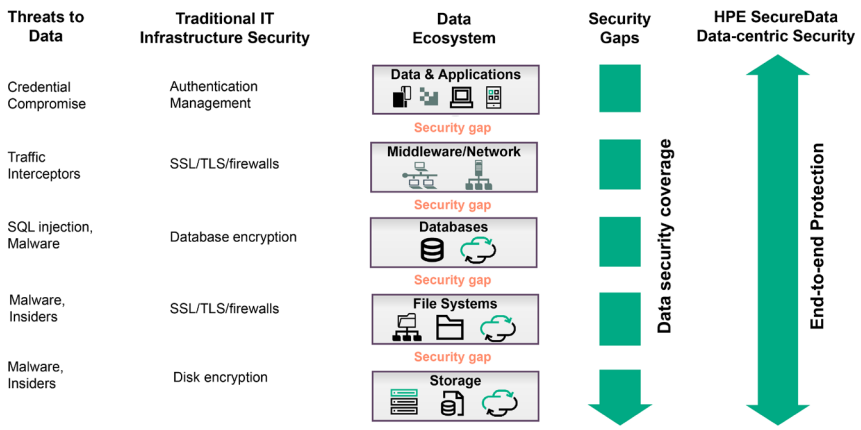
To address the limitations of traditional technologies and meet your security objectives, your healthcare organization needs to implement data-centric security. Through data-centric security, your organization can protect data at its point of creation or collection, and ensure it remains secured, no matter where it may be moved or saved. Toward this end, it is important to have data-centric security capabilities that are platform and system agnostic, so protections can be employed across a diverse set of environments, including legacy applications.

Through these capabilities, your organization can neutralize the danger of having sensitive data exposed. If unauthorized users somehow gain access to sensitive data, they wouldn't be able to decrypt or use it. In this way, organizations can qualify for Safe Harbor, and thus ensure that a breach won't require the costly and brand damaging exercise of public disclosure to comply with HIPAA and any other applicable privacy mandates.

Following are more details on the key advantages afforded by data-centric security solutions.

Comprehensive Security

With the right data-centric security solution, you can establish comprehensive safeguards that enable you to secure data across its lifecycle, wherever it is created, stored, or used.



Data-centric security solutions can secure data against a broad range of threats, including APT attacks, credential compromise, traffic interceptors, SQL injection, malware, malicious insiders, and more. A data-centric approach enables you to establish end-to-end protection, from the users' browser and beyond the SSL tunnel, wherever the data may be transmitted. Data is secured from the point of creation or capture, and through to when it is transmitted across a network, saved into applications and databases, or entered into short-or long-term storage. In short, data-centric security enables your organization to secure ePHI at all times, including at rest, in use, and in transit.

Through their comprehensive coverage, data-centric solutions can address a range of use cases, such as securing payment data, medical records, and assets used in big data analytics environments. These solutions enable you to establish effective control and visibility over sensitive data, whether it is being managed within the data center or in an external cloud.

Maximize data utility and value

At the same time, data-centric solutions don't compromise the value of data, or in any way impede your organization in fulfilling its business or medical charters. With these solutions, you can protect data in production applications, and consistently enforce policies so that data will be furnished only to authorized users for policy-sanctioned purposes.

With data-centric security solutions, you can protect structured data, while maintaining functional and analytic integrity. Your medical staff gets convenient access to the data they need to deliver quality patient care, and the administrative staff and customer service personnel get the information required to provide prompt, effective service to patients, partners, and other stakeholders—whether they're within the data center, using personal smart phones, or accessing cloud services.

A data-centric approach enables you to embrace the potential value of Hadoop and other big data technologies, while mitigating the risks posed by the large-scale aggregation of assets in big data environments.

Minimize Administrative Complexity, Disruption
While many encryption technologies have been around for quite some time, many traditional technologies introduced significant complications into an organization's operations, including complex, time consuming key management efforts, major recoding of applications, and significant changes to business processes. With data-centric security, organizations can avoid these drawbacks.

Data-Centric Security in Action

This section offers several examples of how healthcare organizations were able to leverage data-centric security to address some of their most pressing security and business objectives.

Regional Healthcare Network
- **Background:** A regional medical network was comprised of labs, mobile staff, clinicians, and administrative offices.
- **Challenge:** To more effectively fulfill its charter, the organization needed to provide authorized users with convenient, single sign-on (SSO) access to regulated data, including records being transmitted via email and stored in the cloud. At the same time, the IT organization needed to ensure proper security controls were in place, while scaling to support 35,000 users.
- **Solution:** The organization leveraged data-centric security to efficiently establish and retain controls over regulated data. By adopting a cloud-based delivery model, they were able to scale cost effectively.

Insurance and health network
- **Background:** A national insurance and health network was responsible for conducting HIPAA-regulated communications with a range of diverse groups—including patients, doctors, dentists, and labs.
- **Challenge:** The IT organization had to find a cost effective way to ensure compliance with state privacy and HIPAA requirements. To do so, they needed a mechanism for securing email communications, one that could scale to support millions of users.
- **Solution:** By employing data-centric security, the IT organization was able to establish the controls required, including message revocation, DLP integration, and message transfer agent (MTA) routing support.

Insurer

- **Background:** A US-based insurance company was tasked with managing very large data sets in mainframe systems and Oracle databases. These data sets included personally identifiable information (PII) and HIPAA-regulated identifiers. To optimize operational and cost efficiency, the organization relied on a third-party service provider to manage the IT infrastructure and handle application development.
- **Challenge:** The insurer's security team needed to track and demonstrate compliance for their PII and HIPAA-regulated data. This included retaining control over the access and usage of data that was managed in external third-party environments, as well as in a range of different computing platforms.
- **Solution:** By employing data-centric security, the organization's internal teams were able to establish demonstrable control over data in third-party environments. For example, they employed data de-identification so their contracted development organization couldn't access live data. As a result, they were able to capitalize on the benefits of an external development team, while ensuring only authorized users could access live data.

Pharmaceutical Industry Service Provider

- **Background:** A service provider that serves pharmaceutical firms offered a range of analytics solutions for marketing. The organization began leveraging big data platforms based on Hadoop to provide marketing analytic enrichment services, including enhanced loyalty card programs, promotions, and e-commerce optimization.
- **Challenge:** To deliver its services, the provider needed to aggregate customers' massive data sets, including repositories that contained HIPAA-regulated data. As a result, they needed to establish controls required to ensure sensitive patient data wasn't exposed.
- **Solution:** The service provider leveraged data-centric security to de-identify data before it was migrated into the Hadoop environment. By doing so, they could ensure that analytics were always run on de-identified data, so ePHI would not exposed in insecure Hadoop environments.

Conclusion

For today's healthcare organizations, it is absolutely vital to establish stronger safeguards over ePHI. With data-centric protection, your healthcare organization can maximize the security of ePHI, without making any compromises in your ability to achieve business or medical objectives. With this approach, you can leverage comprehensive controls that enable you to address compliance requirements, while reducing the effort associated with security administration. More importantly, you can establish the strong safeguards that effectively minimize your organization's exposure to data breaches, and their costly aftermath.

HPE Security—Data Security Data-Centric Technologies

HPE SecureData Enterprise
HPE SecureData Enterprise is the only comprehensive data protection framework that secures data as it is captured, processed, and stored across a variety of devices, operating systems, databases, and applications. With HPE SecureData Enterprise, healthcare organizations and service providers can gain the data-centric security capabilities they need to address many HIPAA-required controls, and most importantly, establish strong, persistent controls over ePHI and other sensitive data.

HPE SecureData Enterprise includes capabilities for format-preserving encryption, tokenization, data masking, and stateless key management. It offers healthcare organizations a unique, proven data-centric approach to protection, ensuring access policies travel with the data itself. The platform enables organizations to employ data encryption and tokenization without changes to data format or integrity, and it eliminates the cost and complexity of issuing and managing certificates and symmetric keys. The platform delivers:

- **Central policy management and control.** With the solution, encryption, tokenization, and key management policies are controlled centrally, enabling data privacy policy to be centrally defined, enforced, audited, and managed for structured and unstructured data protection.
- **Stateless key management.** HPE SecureData Enterprise dynamically derives keys on-the-fly after authorization, thus eliminating the need to store or manage keys. In addition, the platform seamlessly integrates with existing identity management and authorization systems to provide policy-based access to data.
- **Broad deployment capabilities.** With the solution, healthcare organizations get high performance Web services interfaces that support encryption and tokenization in a wide range of applications, middleware, databases, big data environments, and cloud services.

HPE SecureMail
HPE SecureMail is an end-to-end encrypted email solution that can scale to millions of users, while keeping PII and ePHI secure and private. The solution enables health care organizations to address their security policies and HIPAA requirements, without restricting the flow of information users require. The solution offers these capabilities:

- **Data-centric protection for email and attachments.** HPE SecureMail encrypts data and attachments so that if a security breach does occur, the encrypted content is of no value to the attacker. Attachments are stored on internal servers, not external third-party servers.
- **Stateless key management.** Using industry-based standard, HPE Identity-Based Encryption (IBE), secure messages can be sent to any recipient, without first requiring the recipient to take special action. Since there are no keys to manage or store, HPE SecureMail requires minimal administrative or infrastructure support and allows for scale across global enterprises.
- **Flexible deployment options.** HPE SecureMail supports on-premises, cloud, and hybrid deployments, as well as cloud email services such as Office 365. The solution also works seamlessly with Outlook, Exchange, Blackberry Enterprise Server (BES), mobile device management (MDM) platforms, business applications, and websites. HPE IBE offers a clean separation between encryption and authentication, meaning it can support a variety of authentication methods, including Active Directory, LDAP, portals, and Web access managers to name a few.

About Coalfire

Coalfire is a leading, independent information technology Governance, Risk and Compliance (IT GRC) firm that provides IT audit, risk assessment and compliance management solutions. Founded in 2001, Coalfire has offices in Dallas, Denver, Los Angeles, New York, San Francisco, Seattle, Washington D.C., and England and completes thousands of projects annually in retail, financial services, healthcare, government, and utilities. Coalfire's solutions are adapted to requirements under emerging data privacy legislation, the PCI DSS, GLBA, FFIEC, HIPAA/HITECH, HITRUST, NERC CIP, Sarbanes-Oxley, FISMA, and FedRAMP. **coalfirelabs.com**

About HPE Security—Data Security

HPE Security—Data Security is a leader in data-centric security safeguarding data throughout its entire lifecycle—at rest, in motion, in use—across the cloud, on-premise and mobile environments with continuous protection.

Learn more at
voltage.com
hpe.com/software/datasecurity

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-0702ENN, March 2016, Rev. 1