Global Information Assurance Certification Paper

Bringing Security to Health Care

Abstract

The Health Care industry is comprised of a wide variety of organizations ranging in size and scope from independent care providers to large-scale clearinghouses. Each of these organizations shares a common element; they all have access to patient information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was drafted to address the disparity in privacy safeguards between these organizations and assure that reasonable controls are in place to protect this information. Part II of HIPAA is referred to as the Security Standards Rule and defines requirements for physical, administrative, and technical safeguards. The organization is responsible for developing an approach to meet the business challenge of implementing these regulations.

Introduction

The HIPAA Security Rule defines standards for securing Patient Health Information (PHI). It is important to realize that securing the organization's infrastructure to protect the use and electronic transfer of PHI is fundamentally similar to securing information across many different industries. The components are part of a similar defense-in-depth strategy that would be consistent for enterprises desiring layered security and best-practice approaches.

HIPAA Perspective

The value of business information should be understood to establish strategic priorities, identify criticality, and allocate resources appropriately. The protection of key information is fundamental to business survival. PHI is similar to other forms of business information that warrant protection. Whether intellectual capital, internal knowledge, or personnel information, levels of protection, audit, and control are required to ensure Confidentiality, Integrity, and Availability (CIA).

The lack of common standards and security mechanisms across Health Care organizations is a significant driver behind HIPAA. The HIPAA regulations provide technical solutions through a combination of administrative, physical, and technical safeguards. These safeguards are identified by technology category or mechanism to provide flexibility in meeting the base requirements. The regulations do not identify specific products or vendors to provide for flexibility in establishing robust solutions.

From the business expense perspective, there are benefits associated with the compliance investment that can drive a strong Return on Investment (ROI). Implementing common data definitions, providing secure connectivity, and ensuring confidence in data integrity will be a catalyst for improved

interoperability, efficiencies, and customer satisfaction. "Recognizing the savings and cost potential of standardizing electronic claims processing and protecting privacy and security, the Congress provided in HIPAA 1996 that the overall financial impact of the HIPAA regulations reduce costs."[1]

Compliance Components

The HIPAA security regulations are structured to identify both mandatory and selectable components required for compliance. There is also discretion at the organizational level in adopting specific components. "Security should be appropriate and proportionate to the value and degree of reliance on the IT systems and to the severity, probability, and extent of potential harm."[2] The definition of implementation components within the regulations as 'addressable' supports this flexibility. A risk assessment can be used to address variability from the regulation while still maintaining overall compliance.

Administrative safeguards include policies, procedures, and planning. This standard establishes the foundation for internalizing security and disaster recovery into the daily business of the organization. This standard reinforces the requirement to have an assigned security officer. Organizations should assess the need and benefits of dedicated security, disaster recovery, and business continuity professionals. World events have shown the positive business impact of solid disaster recovery and business continuity planning.

A key component of the administrative standards is the end-user involvement, buy-in, and organizational benefit gained from security awareness and training. User security training provides an awareness of issues and vulnerabilities that allows the user to protect the company's systems and information. User awareness of issues such as password management, Internet and electronic mail usage, software licensing, and security risks such as social engineering, etc., helps to protect the organization while maximizing the utilization of company resources.

Physical Safeguards include facility and media controls. They provide basic standards for physical security for access and availability of systems and information. It is critical to implement physical controls as this is the often the easiest and most overlooked method to access information. The best security systems in the world can be easily circumvented with physical access to hardware, backup media, etc.

---

[1] "HHS Fact Sheet, Protecting the Privacy of Patients' Health Information: Summary of the Final Regulation."
[2] "Generally Accepted Principles and Practices for Securing Information Technology Systems," p.6.

Technical Safeguards include those security mechanisms that are facilitated by technology implementations. These safeguards include auditing, integrity, authentication, and access controls. Security principles such as unique user identification, logging, and encryption are addressed. A key benefit of these principles is non-repudiation - the user who accesses or transmits PHI can be held responsible and accountable. An example HIPAA-compliance implementation of public-key cryptography leveraging digital signatures and certificates supports non-repudiation; it also enhances confidentiality and integrity.

There are a wide range of products, technologies, and services that can address compliance with these standards including standalone, modular, and fully integrated systems. Many vendors have repackaged their product lines to emphasize HIPAA compliance.

Security Standards: Matrix[3]

ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)		(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedure	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement	(R)

[3] Tables from "Security Standards: Regulation Text."

PHYSICAL SAFEGUARDS

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)		(R)
Workstation Security	164.310(c)		(R)
Device and Media Controls	164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

TECHNICAL SAFEGUARDS

Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	164.312(b)		(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	164.312(d)		(R)
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

Compliance Approach

From an organizational perspective, the first step toward compliance is to appoint a Security Officer. The Security Officer has responsibility for assessing the environment, identifying issues, developing an action plan, and engaging the organization in pursuing compliance. It is critical to engage the organization and leadership for the Security Officer to be successful.

The Security Officer must gain a strong understanding of the HIPAA requirements and security regulations. They also must understand the way PHI and other key information flows through the organization. The Security Officer will need to interact with all levels of the organization. They must be empowered to access information, research, assign and delegate as needed. They will have to engage outside organizations and service providers to understand information flow and associated risks. They may require the support of consultants, vendors, etc. Management should support recommendations from the Security Officer, assist with accepting and mitigating risks, and be supportive of financial commitments required to obtain compliance.

A solid approach to address the safeguards in the Rule is to leverage the matrix located in Appendix A of the Security Standards Rule. This matrix identifies the standards within each category, references the source section, and identifies the implementation specifications. This can be used as a checklist to ensure all applicable components have been addressed. A project management methodology should be used to provide accountability, reporting, and measurable goals.

Before initiating any change, the Security Officer will need to conduct an assessment of the current state of the administrative, physical, and technical environment. "The road to a secure computer environment starts with a blueprint on how to get there"[4]

To gain an understanding of the administrative elements, they may need to involve, disaster recovery, business continuity, security, management and training resources. They will need to conduct a review of formal and informal policies and agreements with service providers. To identify the physical environment, the Security Officer may need to involve facilities and network management staff. They should review Information Technology (IT) usage policies and retention guidelines. To address the technical safeguards, the Security Officer will need to engage the IT staff responsible for maintaining the network security architecture. Based on the size of the organization, responsibility for assessment of the different standards can be delegated.

Once the assessment phase has been completed, the next step is to identify the gaps. Those items in compliance can be identified as such and those out of compliance should be assessed and prioritized. The assessment should be broken up into component elements that can be addressed or delegated for additional research, white papers, policy development, etc.

A remediation strategy should be developed for each identified gap. The Security Officer should facilitate team activities, such as brainstorming and other idea generation tools, to maximize available knowledge while generating agreement and consensus. The recommended approach or solution for each compliance item should be evaluated for applicability and scope within the environment. Validation steps should be defined to ensure the gap has been addressed.

Technical solutions that are considered should be weighed objectively using unbiased approaches such as scoring, etc. Vendor solutions should be evaluated to ensure that they meet the stated objectives and provide appropriate levels of functionality and interoperability.

[4] Lovelace.

The remediation strategy should be consolidated into a cohesive action plan. The Security Officer should present this plan to management for approval. Factors such as risk management, expense, policies, etc. may drive reevaluation and reformulation of the plan. Once an action plan has been approved, the Security Officer should assign the responsibility to implement the plan to the appropriate staff.

Addressing the gaps is the key to achieving compliance with the HIPAA Security Rule. However, even after achieving initial compliance, the role of the Security Officer is not complete. "The mere installation of a network security device is not a substitute for maintaining and updating a network's defenses."[5] They continue to support the organization and a security culture by planning, designing, and evaluating security solutions. They maintain a leadership role within the organization and are a champion of security initiatives.

Conclusion

Health Care organizations can obtain compliance with the HIPAA Security Rule by leveraging a structured approach to assess, identify, and remediate the standards. The Security Officer will play a key role by providing leadership and guidance to the organization. This will lay a strong foundation for the ongoing management and incorporation of evolving technologies in the future. This is critical to become a leader as the pace of change continues to accelerate.

Many of the principles and practices outlined in the HIPAA Security Rule are the basis of a comprehensive information security approach. The required components are in-line with industry directions and best-practice recommendations. Health Care organizations that have shown a commitment to implementing best-practice tools and approaches to secure their infrastructure may have already met most of the requirements of the Security Rule.

[5] "The National Strategy to Secure Cyberspace," p.8.

References

Department of Health and Human Services. "Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160, 162, and 164. Health Insurance Reform: Security Standards; Final Rule." 20 Feb 2003. URL: http://aspe.hhs.gov/admnsimp/FINAL/FR03-8334.pdf (11 Aug 03).

Department of Health and Human Services. "HHS Fact Sheet: Protecting the Privacy of Patients' Health Information: Summary of the Final Regulation." 20 Dec 2000. URL: http://aspe.hhs.gov/admnsimp/final/pvcfact1.htm (13 Aug 03).

Swanson, Marianne, Guttman, Barbara. National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce. "Generally Accepted Principles and Practices for Securing Information Technology Systems." Sep 1996. URL: http://www.hipaadvisory.com/regs/finalsecurity/nist/800-14.pdf (13 Aug 03).

Phoenix Health Systems. "Security Standards: Regulation Text." HIPAAdvisory. URL: http://www.hipaadvisory.com/regs/finalsecurity/regulationtext.htm (13 Aug 03).

Lovelace, Herbert W., "Security: It's A Carefully Planned Race." Information Week. 1 Oct 2001. URL: http://www.informationweek.com/story/IWK20010927S0007 (18 Aug 03).

President's Critical Infrastructure Protection Board. "Cyberspace Threats and Vulnerabilities: A Case for Action." The National Strategy to Secure Cyberspace. Feb 2003. URL: http://www.whitehouse.gov/pcipb/case_for_action.pdf (18 Aug 03).