



HIPAA Security Regulation – Practical Strategies for Compliance

Overview

The Health Insurance Portability and Accountability Act (HIPAA) mandates standards for the security of electronic protected health information (ePHI) and requires compliance with the final Security Regulations by April 21, 2005. While the deadline for the final Security Regulation is imminent, the current Privacy Regulation includes a “mini security rule” that requires compliance effective April 14, 2003. The “mini security rule” is found within the Privacy Regulation and requires administrative, physical and technical safeguards to protect the confidentiality of all protected health information (PHI). In short, the Privacy Regulation mandates a non-trivial level of security compliance effective April 14, 2003. Consequently, healthcare organizations must implement appropriate security safeguards in order to comply with the “mini security rule” as well as the Security Regulation. In addition, inappropriate uses and disclosures of PHI due to insufficient security safeguards will be enforced under the Privacy Regulation, including civil monetary penalties. To date several lawsuits have been initiated.

Compliance with the Security Regulation will be an on-going effort requiring covered entities to evaluate and effectively address critical security risks, while employing overall best security practices. This involves reviewing and refining policies and procedures, security practices, as well as technical mechanisms used to guard the confidentiality, integrity and availability of ePHI. As covered entities work toward Security Regulation compliance, they face the familiar challenge of evaluating and determining how best to apply resources, budgets and technology to address compliance gaps.

This paper provides an overview of the critical components identified within the HIPAA Security Regulation, including the need for a strong security foundation built upon reliable authentication processes. The Security Regulation calls for technical safeguards including access control, data integrity, authentication, audit controls and encryption (Sentillion’s core competencies), that can be used to mitigate risks and simplify compliance with the technical security requirements, while providing added convenience to clinicians.

Covered Entities

Health care providers, health plans and clearinghouses are covered by HIPAA Security Regulations. To be compliant with HIPAA, these covered entities must meet the requirements of the standards. As well, covered entities will need to ensure the security of PHI in electronic form.

The Department of Health and Human Services (HHS) explains that a covered entity’s “risk analysis and risk management measures... must be designed to lead to the implementation of security measures that will comply with [HIPAA].” As a result, the risk analysis will drive the prioritization and assignment of resources and technology to ensure compliance and protect against unauthorized uses or disclosures.

Overview of HIPAA Security Regulation

The Security Regulation provides a national standard for safeguarding ePHI and requires that covered entities comply with four key requirements.

- Maintain reasonable and appropriate administrative, physical and technical safeguards ensuring the integrity, and confidentiality of all ePHI created, received, maintained or transmitted by the covered entity.
- Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI.
- Protect against reasonably anticipated uses or disclosures of ePHI that are not permitted under the Privacy Regulation, such as unauthorized access to PHI.
- Ensure that employees and officers comply with the Rule.



Given the range of covered entity organization types, the Security Regulation was written with some flexibility in its application. The rule permits covered entities to consider a number of factors in compliance including their size, technical infrastructure and capabilities, as well as the cost, complexity and criticality of the security risks. With that said the Security Regulation provides a comprehensive and high standard for security since covered entities must “ensure” compliance and consider “reasonably anticipated” threats or unauthorized uses or disclosures. For this reason, covered entities should carefully identify high-risk areas and employ solutions that prevent unauthorized access, use or disclosure of ePHI. To meet these demands a covered entity must evaluate its IT setting including the data, networks, applications and use models and implement security practices that protect information in a manner that will meet HIPAA requirements and business needs. Determining the best security policies and practices and technologies varies from organization to organization, however, best security practices show that risk mitigation is best achieved with a strong security infrastructure and strategy built upon strong authentication.

HIPAA Security Strategy

To comply with HIPAA, covered entities must evaluate the risks they bear and then create a security strategy that addresses the administrative, physical and technical requirements. The rule outlines eighteen required standards and approximately forty corresponding implementation specifications. These specifications are either “Required” or “Addressable” and provide further detail regarding what to implement. Covered entities must implement “Required” specifications; but, may further evaluate and justify how they implement “Addressable” specifications. This paper will only highlight the key specifications, a detailed white paper can be found at <http://www.hhs.gov/ocr/combinedregtext.pdf>.

Risk Analysis

Covered entities must mitigate the risk of a security breach, unauthorized access or information disclosure. A risk analysis is an objective process to determine whether addressable implementation specifications are reasonable and appropriate given the infrastructure, risk and the related cost to implement the measures. In short, an analysis helps to prioritize the risks and to develop a security strategy for mitigating high-risk issues, while employing best security practices.

Security Strategy

Building a solid security strategy begins with a foundation of fundamental security principles. First, the organization must build accountability into a security program. This can be achieved by implementing a strong authentication process that includes some form of two-factor user authentication across the enterprise. Next, the covered entity should develop strong, yet practical access controls that limit information access to a need-to-know basis. Finally, fundamental security principles mandate a system to record events and audit user activities, including access that can be regularly checked and managed across all technology applications.

Covered entities should develop security policies and procedures for authentication, access and audit controls and employ technology that reinforces these principles. By starting with a security foundation that provides strong user authentication and controlled access, a covered entity will not only mitigate the highest risk areas for compliance, but will also prevent unauthorized access, that leads to unauthorized uses and disclosures.

Sentillion Vergence[®] Product Suite **A Critical Component of HIPAA Security Strategies**

Sentillion's Vergence product suite enables authentication, controls and manages information access, protects privacy and information integrity and provides audit trails. Vergence is designed to deliver important security and privacy features that can be integrated into a covered entity's security program for ongoing compliance with HIPAA Privacy and Security Rules. Vergence provides a solid security



foundation for authenticating users and reliably sharing authentication between applications. Without strong authentication, the very basis of a security infrastructure is compromised. To address this challenge, leading healthcare organizations are leveraging Sentillion solutions to securely validate and communicate an authorized user to participating applications.

The following table on pages 4 and 5 lists the final HIPAA Security Rule's and Vergence's relative solutions to the regulations.

Conclusion

Different organizations have different needs. For some organizations employing an electronic information system is a daunting first step, others are further along in gaining electronic information system use and adoption. The reality is, however, that many covered entities are going to have to make changes to meet HIPAA Security Regulation and to comply with the mini security rule found in the current Privacy Regulation. To meet these demands covered entities and their IT organizations must evaluate their IT environment and implement security and privacy practices that protect the patient and health information across their enterprise. Determining the best security and privacy policies, procedures and practices requires methods for strong authentication, access control and auditing and a system that was built to meet the specific needs for healthcare. Sentillion's Vergence is such a product that was built for healthcare to meet its diverse user and regulatory requirements.



Security - Technical Safeguards

Sections	Standards	Implementation Specifications <i>(R)= Required, (A)=Addressable</i>		Sentillion Solution	HIPAA Benefit
164.308(a)(1)(ii)(D)	Security Management Process	Information System Activity Review	(R)	Vergence Privacy Auditor	Vergence Privacy Auditor identifies and records information system activity, such as security incidents, including attempted and successful accesses to ePHI. This data may be used to prevent, detect, contain, and correct security violations.
164.308(a)(4)	Information Access Management	Access Authorization	(A)	Identix Biometric Devices Vergence Authenticator	Vergence Authenticator and Identix Biometric devices (re-sold by Sentillion) provide authentication and access management to help enforce authentication policies.
		Access Establishment and Modification	(A)	Identix Biometric Devices Vergence Authenticator	Vergence Authenticator and Identix Biometric devices (re-sold by Sentillion) provide authentication and access management to help enforce authentication policies.
164.312(a)(1)	Access Controls	Unique User Identification	(R)	Vergence Authenticator Vergence SignOn Manager Vergence Launchpad	Vergence supports consistent use of Unique User ID across enterprise applications.
		Automatic Logoff	(A)	Vergence Authenticator Vergence SignOn Manager	Vergence enables automatic logoff or single sign off capabilities across all Vergence enabled applications. Vergence facilitates consistent enforcement of logoff, and enables customized timeouts based upon the clinical environment.
		Encryption and Decryption	(A)	All	Vergence encrypts sensitive login data when in transit and when stored.
164.312(b)	Audit Controls		(R)	Vergence Privacy Auditor	Vergence enables audit controls across all linked applications, recording user access to ePHI. Vergence provides logs that can be examined by a Privacy Officer or Security Officer to proactively monitor for security events, investigate suspected unauthorized accesses or attempts to access and audit access to ePHI.
164.312(c)(1)	Integrity Controls	Mechanism to Authenticate electronic information	(A)	All	Digital signatures on the Vergence network ensure traffic hasn't been tampered with and the system hasn't been compromised by a hacker's rogue application.



Sections	Standards	Implementation Specifications <i>(R)= Required, (A)=Addressable</i>	Sentillion Solution	HIPAA Benefit
164.312(d)	Person or Entity Authentication		(R) Identix Biometric Devices Vergence Authenticator	Vergence and Identix Biometric devices (re-sold by Sentillion) enables stronger and consistent authentication of users across enterprise systems. Supports strong password rules, as well as biometric and other devices. Leverages a single infrastructure that can adjust the level of authentication needed based upon the risk analysis.
164.312(e)(1)	Transmission Security	Integrity Controls	(A) All	Vergence supports digital signatures on the Vergence network and ensures that traffic hasn't been tampered with and the system hasn't been compromised by a hacker's rogue application.
		Encryption	(A) All	Vergence encrypts network traffic when sensitive data is being transmitted. User credentials are stored in the Vergence credential repository in encrypted form.