White Paper

Achieving HIPAA Compliance through Security Information Management

netForensics®

Contents

netForensics®

Executive Summary

Enacted by the U.S. Congress in 1996, the Health Insurance Portability and Accountability Act (HIPAA) was established for two main reasons: 1) to improve health insurance accessibility for individuals changing employers or leaving the workforce; and 2) to encourage and protect the electronic transmission of health-related data.

In a statement by U.S. Department of Health and Human Services (DHHS) Secretary Tommy G. Thompson, on approving the Patient Privacy Rule in 2001, he said:

"This rule makes sure that private health information doesn't fall victim to the progress of the information and technology age, where an array of data is readily available in computer systems and too often is just a keystroke away from being accessed. We are giving patients peace of mind in knowing that their medical records are indeed confidential and their privacy is not vulnerable to intrusion." [1]

By encouraging the widespread use of electronic data exchange in the U.S. healthcare system, HIPAA strives to improve the system's efficiency and effectiveness. Yet the rule poses tough information security challenges for healthcare organizations. The burden of change rests on the organizations themselves, who must abide by the new standards for the use and dissemination of healthcare information—or face strict penalties for noncompliance.

To meet HIPAA compliance, healthcare organizations and related entities must implement comprehensive and effective security solutions that will protect their valuable information assets. IT organizations need an approach to HIPAA compliance that involves establishing an agency-wide, risk-based, and cost-effective information-security program. Security information management (SIM) allows healthcare organizations to implement appropriate security procedures as measured by the HIPAA industry standard. In the event of a security breach, SIM provides healthcare organizations the tools to prove that they took all reasonable precautions to protect patient data.

Wheaton Franciscan Healthcare, a healthcare organization based in Wheaton, Illinois, implemented a security management solution to address their information security and compliance challenges. By deploying netForensics' nFX Open Security Platform (nFX OSP) for SIM, Wheaton is now equipped with the real-time monitoring, security incident response functionality, and advanced reporting tools to transform security-related information into actionable intelligence—and meet HIPAA compliance.

Properly implemented, a best-practices SIM solution empowers healthcare management with real-time visibility into information security-related risk and compliance data to not only align with HIPAA standards, but to support the agency's broader corporate governance objectives. SIM provides healthcare organizations the comprehensive insight into security posture to address complex security challenges, successfully manage risk, and meet today's compliance demands.

Introduction: Brief Overview of HIPAA

HIPAA, also known as the Kennedy-Kassebaum Act, was signed into law by the U.S. Congress in 1996 to establish health insurance reform and healthcare administrative simplification for various healthcare entities including: health plans, healthcare clearinghouses such as billing services and community health information systems, and healthcare providers that transmit healthcare data in a way that is regulated by HIPAA.

Governed by the DHHS, HIPAA Title I supports the continuation of health insurance coverage for workers and their families when they change or lose their jobs. Title II defines numerous offenses relating to healthcare and healthcare-related information and sets civil and criminal penalties for agencies that fail to abide by HIPAA standards.

The most significant provisions of Title II for IT organizations are its Administrative Simplification rules. Per the requirements of Title II, DHHS has established five rules regarding Administrative Simplification:

- Privacy Rule
- Transactions and Code Sets Rule
- Security Rule
- Unique Identifiers Rule
- Enforcement Rule

Various security standards apply to each of these rules, particularly for the Security Rule, which establishes three main security objectives: Administrative Safeguards, Physical Safeguards, and Technical Safeguards. Each safeguard area includes both required and addressable implementation specifications. Required specifications must be adopted and administered as dictated by the rule. Addressable specifications are more flexible. Yet according to the rules for both required and addressable specifications, how organizations satisfy individual security requirements and which technology they choose are left to the business decisions of each entity.

Healthcare organizations face fines for noncompliance with HIPAA regulations. Penalties include the following: general fines of up to $25,000 per incident, as well as up to $50,000, imprisonment for not more than one year, or both for wrongful disclosure of individually identifiable health information.

The HIPAA Challenge: Protecting Patient Information

A fundamental benefit of HIPAA is that it encourages the wider use of electronic transactions, greatly simplifying healthcare administration and reducing administrative overhead costs. Yet with the computerization of patient medical records, healthcare organizations face an increased security risk from various sources, such as unauthorized internal access, intrusion attempts, and other security attacks. HIPAA therefore mandates security measures be taken to protect this sensitive data, ensuring that only patients and their healthcare providers have access to patient medical information. According to the Final Rule of the Act's Health Insurance Reform: Security Standards, the DHHS states:

"Section 1173(d) of the Act provides that covered entities that maintain or transmit health information are required to maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the integrity and confidentiality of the information and to protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized use or disclosure of the information. These safeguards must also otherwise ensure compliance with the statute by the officers and employees of the covered entities." [2]

To comply with HIPAA regulations and protect patient information, healthcare organizations are tasked with updating their legacy computer systems, ramping up their information security capabilities, and defining and implementing business processes that align with security objectives. According to the Title II Administrative Simplification

Security Rule, specific security issues must be addressed and solutions implemented as they relate to transmitting and storing patient data. Safeguard initiatives include the following:

Administrative Safeguards

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

Physical Safeguards

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Technical Safeguards

- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

The HIPAA Security Standards do not specify particular technology requirements, so each affected healthcare organization must assess its own risk and develop security measures accordingly. Organizations must then certify their security programs through self-certification or by a private accreditation entity. Therefore, to address the HIPAA Security Rule and ensure that Administrative, Physical, and Technical Safeguards are implemented that will lead to HIPAA compliance, a comprehensive and effective information security program is necessary.

Security Information Management: The Foundation that Enables HIPAA Compliance

A comprehensive and specific approach to meeting HIPAA requirements must start with leveraging the right security management solution—one that enables real-time monitoring and historical, on-the-fly reporting. But technology alone is not the answer. An in-depth approach that integrates existing assets—including people, processes, and policies—with technology is the most viable means to successfully attaining compliance.

A best-practice SIM solution provides healthcare organizations the ability to comply with the information security provisions of HIPAA. Assuming the following responsibilities to prove diligence in managing information security risk helps organizations meet HIPAA

requirements, as well as those of other privacy and security regulations:

- Define a policy-driven security management program that can be incorporated early on into business processes — Identify the people and technology controls needed to satisfy the organization's security mission and ensure HIPAA compliance. Also, ensure that security initiatives are integrated into business processes at their onset, rather than after the fact.
- Validate security controls — Provide for the monitoring and reporting of controls on human actions and decisions, process controls, and information technology controls.
- Implement a risk management approach to information security — Comprise active monitoring of risk as defined and measured by key control indicators (KCIs) and key risk indicators (KRIs), correlating the relative value of information assets, the threats to the confidentiality, integrity, and availability of the assets, and the vulnerability of the systems and architecture that store and carry the assets.
- Demonstrate due diligence in the application of internal controls — Create a link between the security infrastructure and policy by capturing all security events from all network hosts, devices, and assets in an auditable database.
- Develop and implement an effective security-incident management process — Demonstrate that the proper steps were taken to correct systems and adjust policy if a noncompliant situation is identified.
- Enable reporting that can help demonstrate compliance — Demonstrate the ongoing security of compliance-related assets over a period of time, recreating the organization's security posture if needed to obtain HIPAA certification, and enabling security performance management against metrics that can be leveraged for corporate governance initiatives.
- Establish capabilities for archiving and data preservation — Preserve near-term and long-term data in its purest form for forensics and evidentiary presentation.

By leveraging SIM to implement effective, comprehensive policies and procedures for establishing accountability and consistent reporting practices, healthcare organizations can successfully meet HIPAA regulatory compliance directives.

The Case for Security Information Management

Wheaton Franciscan Healthcare wanted to improve visibility into network security and enhance reporting capabilities to enable HIPAA compliance. The nonprofit healthcare organization based in Wheaton, Illinois, with 17 hospitals and more than 70 clinics in Colorado, Illinois, Iowa, and Wisconsin, was challenged by managing nearly 100 security devices, including firewalls, intrusion protection systems, virtual private network concentrators, and authentication services. The organization manually reviewed many of its security devices, though some were unmanageable due to the enormous volume of event log data. Wheaton turned to a SIM solution to bring its security initiatives under control.

After installing nFX OSP on its network servers, Wheaton reduced its monitoring workload and minimized downtime by leveraging its SIM tools to react more quickly to threats. With improved visibility into the network and the ability to assess its risk posture at any given point in time, Wheaton raised security and reporting to the level required for HIPAA compliance.

The netForensics Solution: Aligning with HIPAA Objectives

netForensics provides the SIM infrastructure to drive HIPAA compliance initiatives. nFX OSP provides healthcare organizations greater visibility, better intelligence, and more effective response. nFX OSP features a variety of tools and technologies to help organizations conquer complex HIPAA compliance and risk management challenges. The enterprise-class SIM technology from netForensics includes the following:

- Actionable Security Intelligence — With broad security intelligence, healthcare organizations have a foundation from which to maintain HIPAA compliant operations. Organizations can establish a continuous process of threat collection, identification, and remediation, protecting patient information and ensuring business continuity.
- Enterprise-Class Security Decision Support — Healthcare organizations can meet compliance requirements through automated threat identification, by reporting against controls, and via incident resolution management. Additionally, they can resolve incidents as they occur. Metrics enable performance measurement, with baselines for security and performance gauges at the analytical and executive dashboard levels.
- Scalable, Robust SIM Architecture — A scalable SIM architecture cost-effectively supports growth and reduces total cost of ownership in mid-size to large environments. The SIM architecture incorporates data from security and network devices, applications, scanners, and databases to deliver global visibility into all security-related activities, regardless of numbers.
- Correlation Technology and Processing Power — A comprehensive correlation technology goes beyond simply logging security information, and instead speeds threat identification and provides an accurate picture of risk. The nFX OSP technologies are architected to handle the massive volume of security information from network-related sources as well as server logs, applications, databases, and identity management systems, and pinpoint attacks from the inside and beyond based on a thorough understanding of network and user activity. The correlation technologies process large volumes of data from the perimeter down to the core to identify real-time threats and historical patterns.
- Visualization, Reporting, and Analytics — Healthcare organizations can visualize threats as well as the security information underlying the threats. Through the in-depth reporting functionality, key stakeholders and especially those performing HIPAA certification have ready access to comprehensive compliance data. The deep level of analytics enables institutions to measure compliance, risk, and operational performance so that security analysts, operators, and executives can determine the security posture and take any necessary steps to improve it.
- Incident Resolution Management Workflow and Embedded Security Knowledge — nFX OSP offers guidance through a repeatable incident response workflow, allowing healthcare organizations to effectively eradicate threats and prevent reoccurrences. Through actionable security intelligence, the incident remediation process is documented for security policy management and improvement purposes, as well as for regulatory compliance. The embedded knowledge base integrates third-party security information that includes a pre-populated database of incidents and how to resolve them.

- Application Security Monitoring —nFX OSP provides comprehensive security monitoring at the application layer. Flexible deployment options allow nFX OSP to be configured optimally to handle application events, while failover and redundancy guarantee the availability of events from identity management systems, server logs, and traditional network security devices. Dashboards and reports allow everyone involved in the process of enterprise security to understand the impact of an application-level incident on business continuity.

Using these tools and technologies, healthcare organizations can effectively manage information security risk, and consequently demonstrate HIPAA compliance.

Conclusion

The HIPAA Security Standards are making strides in protecting the confidentiality and integrity of health information. Yet HIPAA requirements have intensified the need for healthcare organizations to improve the security of IT systems, applications, and data. Healthcare IT organizations must establish and implement Administrative, Physical, and Technical Safeguards for protecting patient data. Healthcare establishments are turning to information-security best practices of risk and vulnerability measurement to ensure the integrity, confidentiality, and availability of patient systems and data.

A fully implemented SIM solution like nFX OSP, along with alignment of human, process, and information controls, enables healthcare organizations and related agencies to meet HIPAA objectives. Through SIM, organizations can leverage existing technology and tools to identify, assess, and report on security-related issues and events for patient data, and ultimately provide tangible evidence of their efforts.

References

1. Thompson, Tommy G., Secretary, U.S. Department of Health and Human Services, in Statement Regarding the Patient Privacy Rule,

http://www.hhs.gov/news/press/2001pres/20010412.html

2. Health Insurance Reform: Security Standards — Final Rule,

http://a257.g.akamaitech.net/7/257/2422/14mar%2020010800/edocket.access.gpo.gov/2003/pdf/03-3877.pdf

About netForensics

netForensics transforms all security related information into actionable intelligence, enabling more than 450 enterprises and government agencies to better respond to security threats, maintain compliant operations, and ensure the continuity of key business processes.

By harnessing the power of our award-winning Security Information Management platform that manages more security events at more organizations than any other product in the marketplace, we help customers deliver security management solutions that rely on the availability of timely and relevant information security information.

We facilitate these actionable security intelligence (ASI) solutions by rationalizing security information from strategic applications and critical compliance-related assets, as well as the perimeter devices that protect them. ASI solutions make this information available to technology domains and users within the security organization and beyond — by unifying network and security organizations, while supporting IT governance, enterprise compliance, and risk management initiatives.

200 Metroplex Drive • Edison, NJ 08817 • p 732.393.6000 • f 732.393.6090
www.netforensics.com • info@netforensics.com

netForensics®