



OKENA — Helping Achieve the Goals of HIPAA

What is HIPAA and How is it Relevant to Security?

The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 in an effort to maximize the efficiency of our Health Care System. HIPAA contains provisions which specifically address the issues of information technology and security within the Health Care industry. These provisions are a set of *Privacy & Security Standards* which have been rewritten a number of times since 1996 in order to accommodate technological progress. On Dec. 28, 2000, the US Department of Health & Human Services (HHS) established final regulations of the *Privacy Standards* for health information. All businesses and institutions who are involved with the maintenance and transmission of health information are required to comply with the *Privacy Standards* by April 14, 2003. The final regulations of the *Security Standards* have not been established as of November 20, 2001, but the content is not expected to change much from what is contained in the 'Proposed Security Rule', which is available now.

Who is Affected by HIPAA?

Health plans, health care clearinghouses & providers, "or any business responsible for maintaining or transmitting health information," (HHS) are required to initiate and fulfill the mandates of HIPAA.

What do the *Privacy & Security Standards* Mandate?

The *Privacy & Security Standards* are designed to protect all electronic health information from improper access or alteration. The *Privacy Standards* are concerned with 'what' information is protected and the *Security Standards* are concerned with 'how' this information is to be protected.

"Health information must be protected during transmission and where maintained in electronic form," (HHS). Availability, confidentiality and integrity are three key aspects of securing electronic health information and these areas of security are reiterated numerous times throughout the *Privacy & Security Standards*. Availability refers to establishing protection against system downtime which causes health information to become unavailable. Confidentiality refers to establishing protection against an

undisclosed entity having access to private health information. Integrity refers to the protection against unauthorized changes of private health information. The Privacy Standards require that availability, confidentiality and integrity of health information are protected. “The proposed security standard consists of the requirements that a health care entity must address in order to safeguard the integrity, confidentiality, and availability of its electronic data,”(NPRM).

There are extensive security products from a myriad range of vendors, built to secure different aspects of an organizations electronic information. Therefore, HHS was posed with a dilemma: Do we provide standards which require the adoption of very specific technologies, products and vendors; or do we provide Health Care Organizations (HCOs) with a framework for protecting specific health information and let the HCO choose the technology, product and vendor?

The HHS has been generous by allowing Health Care Organizations the flexibility to satisfy their security requirements in their *own* way, allowing them the freedom of customizing security to their unique business environments. The solutions which HCOs choose are not limited to specific security products as long as the security standards are fulfilled. “There is no recognized standard that integrates all the components of security that must be in place to preserve health information confidentiality and privacy as defined in the law. We want to give providers/plans/ clearinghouses flexibility to choose their own technical solutions,” (NPRM). This allows enough leg room within the structure of the Privacy requirements, for HCOs to implement the latest and most technologically advanced security solutions.

However, the standards do mandate a set of *implementation features* which require all HCOs to build a structured security framework. This framework does not require *specific* technologies or vendors, but instead, creates a backbone of security support that all HCOs are required to erect. The implementation features are divided into recommendations for the ‘Proposed Security Rule.’ The following bullets constitute the categories of the *implementation features* within the ‘Proposed Security Rule.’

- Administrative procedures to guard data integrity, confidentiality, and availability – these are documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data.
- Physical safeguards to guard data integrity, confidentiality and availability e.g. from hazards such as fires etc. and against intrusions with locked facilities.
- Technical security services to guard against data integrity, confidentiality and availability – these include the processes that are put in place to protect and to control and monitor information access.
- Technical security mechanisms – these include the processes that are put in place to prevent unauthorized access to data that is transmitted over a communications network.

The fourth bullet category, ‘technical security mechanisms’, is the category which OKENA has to target when approaching a HIPAA related sale. Under this category, the following implementation features are mandatory for information systems which employee communications and networks:

- i. Access Controls
- ii. Alarm, event reporting, and audit trails
- iii. Audit trails
- iv. Encryption
- v. Entity Authentication
- vi. Event reporting
- vii. Integrity controls
- viii. Message Authentication

Adaptive Communications, LLC states that “the use of Firewalls, VPN’s, **Intrusion Detection Systems**, and PKI Solutions,”(HIPAA Info. Doc.) help with the implementation of the above features. OKENA has an advantageous play in the Intrusion Detection space which is often needed for implementations i., ii., iii., vi, and vii above.

Who Do We Contact?

The Privacy Standards require that HCOs designate a ‘Privacy Official’ who is responsible for handling the security requirements of HIPAA. While not all HCOs will have an individual completely allocated to this task, it is required, and the person designated as the ‘Privacy Official’ is the optimal contact for discussing security implementation.

How Does OKENA Help HCO’s Comply With the *Privacy Standards*?

“A large organization should base their approach on the policy, but will control and monitor with technical mechanisms. Access controls must be configurable at the location, workstation, user group, application and user level, with multiple types of control options. This will enable organizations to customize the access controls to their environment..... Security procedures must provide for monitoring and timely response. Organizations must establish procedures to monitor and respond to real or attempted breaches in security in a timely manner in proportion with the risk. The increasingly interconnected real-time and trans-border nature of information and the potential for damage to occur rapidly, requires that organizations act swiftly,”

(HIPAA Security Summit Guidelines).

OKENA’s application centric, intrusion prevention software, StormWatch, is designed to proactively protect the availability, confidentiality and integrity of health information residing on desktops *and* servers. Because StormWatch secures applications from operating outside of their legitimate boundaries, OKENA is able to secure sensitive health information systems against hacking, malicious activity and accidental disruption in real-time. Unlike intrusion detection products, StormWatch does not use signatures to

stop attacks and has the ability to prevent deleterious attacks instead of simply alerting administrators, often after valuable health information has been corrupted. Instead OKENA has developed a unique rules engine with the power to intercept and prevent both known and unknown attacks from damaging information resources. *We prevent intrusions from executing.*

Benefits:

- OKENA maintains the ***availability*** of health information:
 - Reduces downtime of network resources
 - Prevents against current – and future – innovative attacks and viruses
 - Prevents accidental and intentional disruption of security operations
 - Defends file and network resources
 - Is fully distributed and scalable

- OKENA protects the ***confidentiality*** of health information:
 - Sets parameters on what activities will and will not be allowed by applications
 - Identifies and secures against abnormal or unusual behavior
 - Fine-grained access control is enforceable on system resources
 - Enforces good behavior, protecting against any actions that violate your rules
 - Allows hierarchical, role-based management via the rules engine

- OKENA protects the ***integrity*** of health information:
 - Protection of sensitive health files in the face of new attacks or improper access
 - Out of the box system hardening, provides protection against common system compromises such as distributed port scans, network worms and Trojan horses
 - Default policies for IIS, Microsoft SQL Server, and Office provide 'out of the box' protection and establish a solid baseline from which to customize and develop environment specific security policies
 - Central correlation of events across many agents helps to prevent damage from distributed attacks
 - Health information stored in databases within SQL server is proactively protected against attacks with a comprehensive default policy

What are the Repercussions for Not Achieving Compliance?

The HHS' Office of Civil Rights is the agency responsible for enforcing the Privacy Standards. There are various consequences that range from \$100 dollar fines for small civil penalties, as well as greater "penalties for noncompliance ranging from \$50,000-\$250,000 in fines,"(IBM).

Matt McConnon
Research Marketing Specialist
OKENA
(781)209-3221
mmcconnon@okena.com

