http://www.apani.com

Health Insurance Portability and Accountability Act (HIPAA) and Its Impact on IT Security

Regulatory Compliance Series 3 of 6
May 12, 2005

This white paper looks at the Health Insurance Portability and Accountability Act (HIPAA), and its impact on IT security.

The HIPAA Security Rule contains three measures that must be addressed in order to protect and assure the confidentiality of electronic protected health information: Administrative Safeguards, Physical Safeguards and Technical Safeguards.

This paper focuses on the Technical Safeguards, policies and procedures that protect and monitor information access and prevent unauthorized access to data transmitted over a network, and how Apani Networks EpiForce can help organizations achieve and maintain compliance with the technology guidelines set forth in this provision.

www.apani.com

3230 E. Imperial Highway | Suite 201 | Brea, CA 92821

Email | compliance@apani.com Toll Free | +1 866.638.5625

Introduction

The Health Insurance Portability and Accountability Act (HIPAA), signed into law by President Clinton on August 21, 1996, was established to improve the overall efficiency and effectiveness of the healthcare system by ensuring continued healthcare coverage for individual workers and their families in the event that they change employment. The law includes additional provisions for healthcare systems which address the management of health information, the simplification of administrative aspects of healthcare, as well as rulings which address the privacy and the security of health information.

This paper will focus on the standards placed on the security of health information, as described in the HIPAA Security Rule, and how Apani Networks' EpiForce security system can help organizations achieve and maintain compliance with the technology guidelines set forth in this provision.

What is HIPAA?

The HIPAA Security Rule was proposed in August of 1998 by the Department of Health and Human Services (DHHS) as a result of increasing concerns over the security of computerized healthcare information. Its purpose is to ensure the portability, privacy and security of an individual's medical records and mandates that the healthcare industry place standards surrounding the maintenance and transmission of patient information that is stored in digital form. The Final Security Rule which adopted these standards was published in the Federal Register in February of 2003.

HIPAA impacts all organizations within the healthcare industry, as well as those who process or use any of the related information, including the DHHS Medicare Program itself, other Federal and State agencies operating health plans or providing healthcare, private health plans, healthcare providers, any organization that processes healthcare information and healthcare clearinghouses.

The general rules surrounding security standards require impacted entities to:

- Ensure the confidentiality, integrity and availability of all electronic protected health information that is created, received, maintained or transmitted.
- Protect against any anticipated threats or vulnerabilities to the security or integrity of health information.
- Protect against any unauthorized use or disclosure of the health information.
- Ensure that all staff members comply with these safeguards.

All covered entities except for small health plans must be in compliance with the Security Rule requirements by April 21, 2005. Small health plans must comply by April 21, 2006.

Key Sections That Pertain to System Security

HIPAA security regulations are intentionally vendor and technology neutral, and consequently are both broad and open to interpretation based on the individual circumstances of the healthcare entity. The Security Rule contains three measures that must be addressed in order to protect and assure the confidentiality of electronic protected health information:

- **Administrative Safeguards:** Implement and maintain policies and procedures to prevent, detect, contain and correct security violations.

- **Physical Safeguards:** Implement and maintain policies and procedures to limit physical access to computer systems and their facilities, while ensuring that properly authorized access is allowed.

- **Technical Safeguards:** Implement and maintain policies and procedures that protect and monitor information access and prevent unauthorized access to data transmitted over a network.

Administrative Safeguards

Herein lies the core HIPAA requirement: the implementation and administration of policies and procedures to detect and prevent a security breach avoiding unauthorized access of sensitive patient information. In a paper-based world, this process is straight-forward; keep the files under lock and key, allowing access only to those approved individuals or entities. A paper trail logging system easily provides the necessary audit trail to investigate potential security breaches.

Healthcare information today is ubiquitous, with patients demanding online access, frequent changes of healthcare providers and a growing community of specialists, each requiring background healthcare information. Consequently, the task of assembling, securing and maintaining electronic healthcare data requires a holistic approach which is flexible and adaptable to the constantly changing electronic era we live in. Just as a storage system must be designed to collect and administer this information, the security behind that system is just as important and must be equally comprehensive.

To ensure HIPAA compliance, a security system must prevent unauthorized access from external and internal threats. Perimeter-based defense systems have proliferated as a means to control external threats, including VPNs, firewalls and intrusion detection / prevention programs designed to thwart an attack aimed at compromising sensitive patient data. It is also recognized as an industry standard to implement authentication standards (1-3 levels, such as user name, password and a token) as part of any information depository user interface.

www.apani.com
3230 E. Imperial Highway | Suite 201 | Brea, CA 92821
Email | compliance@apani.com Toll Free | +1 866.638.5625

These industry accepted administrative security standards provide a minimum level of protection to achieve HIPAA compliance. A vulnerability, however, exists which, until now, has not been universally recognized as a threat, yet each healthcare provider and ancillary business partner is at risk to this potential security breach—the insider attack, specifically with regards to capturing data-in-transit while still within the 'trusted' environment of the inner network behind the firewall. This threat will be discussed further within this paper.

Physical Safeguards

The systems and processes required to physically secure data records are beyond the scope of this paper.

Technical Safeguards

These standards describe the technical processes of the systems which will be used to enforce the administrative standards. Stated differently, how will you execute your security plan, including the electronic creation, updating, managing and transmittal of the data? At a minimum, each of the following must be addressed:

- **Access Controls**
  Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.
- **Privacy Controls**
  Ensure that confidential data is secured in transit.
- **Audit Controls**
  Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
- **Integrity**
  Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
- **Person or Entity Authentication**
  Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Trusted environments are no longer secure

For the past 30 years, the primary IT security strategy has been a "Moat and Castle" approach; to create a strong perimeter around the "inner network" thereby creating a "trusted" environment and an "un-trusted" environment. Within the "trusted" environment, a perimeter-only strategy leaves internal data potentially exposed for internal attack, and access to IP devices unchecked and unprotected.

www.apani.com
3230 E. Imperial Highway | Suite 201 | Brea, CA 92821
Email | compliance@apani.com Toll Free | +1 866.638.5625

For example, the 2004 CSI/FBI computer security survey notes that more than 50% of network attacks originated internally, with an additional 34% of the attacks coming from an indeterminate location. Attacks in the survey ranged from inappropriate use of information — employees accessing records for non-work related concerns — to sabotage and corporate espionage.

Often, these intrusions were predicated by "probing" attacks where internal networks were searched for operating systems with known holes or vulnerabilities — personal information (social security numbers, credit cards, patient records, etc.) databases — to be stolen immediately or used for later attacks.

Computer Economics reports that the attacks have grown more dangerous with greater than 50% of the attacks in 2004 targeted at specific companies, rather than the more traditional broadcast viruses and other indirect attacks.

Today's security administrators must face a changed paradigm: attacks can come from anywhere, at any time. There's no well-defined perimeter, and it's often difficult to tell who should be granted access to the trusted network, and who should be kept out. An explosion in mobile computing and web-based applications has placed a premium on back office connectivity to anyone, from anywhere, with any device.

Five most common control weaknesses:

1. Improper account provisioning with segregation of duties
2. Insufficient controls for change management
3. A general lack of understanding around key system configurations
4. Audit logs not being reviewed (or that review itself not being logged)
5. Abnormal transactions not identified in a timely manner be considered abnormal or a violation of a security policy within the network.

Defenses focusing on stronger fences are ill equipped to handle the stealth, intelligence gathering and deception that plays increasingly critical role in enterprise security from diverse attack profiles.

Perimeter-based security fails because the network edge is no longer clearly defined. Wireless networks, remote users, web services, corporate spies, disgruntled employees, bribed administrators and socially engineered victims have seen to that. Hackers set up rogue Wi-Fi access points near hotspots to trick users into logging onto their networks. Once a malicious user has control of a computer, they can plant a key logger that can steal passwords, which may then be used as needed to access the corporate network.

Employees and consultants open still more holes. Employees connect their personal machines to your network, despite the fact that those PCs are connected to home networks, or unsecured wireless LANs. Consultants, business partners or remote employees may try to access sites within the trusted network, comprising the network with unprotected communications. Over time, firewalls are starting to resemble Swiss cheese, as more and more ports must be opened, and unnecessary ports often remain open long after they're needed; worse yet, your “trusted environment” becomes connected directly to Internet through a home use, partner link or unapproved wireless device. Perimeter defense is a lost battle!

IT managers have had to rethink security to reduce the risks of these attacks on the trusted network to insure they don’t violate privacy laws, exposing the corporation to legal and civil penalties. As today’s business environment extends the definition of “internal” beyond the perimeter, opening internal assets to more and more people and businesses, administrators must be aware that the “trusted” network can no longer be trusted, and must be secured. Putting trust back into the trusted network by addressing both external and internal security threats is now a requirement to achieving and maintaining.

The following is a “best practices” approach to securing the “inner” network from internal threats, thereby achieving regulatory compliance. These steps, coupled with an adequate external perimeter defense, will establish and maintain a secure “trusted” internal network environment.

Best practices approach to secure the inner network:

1. Define which security relationships are needed.
2. Segregate the network into security zones to facilitate easier management.
3. Enforce the established security relationships within and across the security zones.
4. Perform regular network audits to ensure security relationships are enforced.
5. Update security relationships as business needs or compliance issues dictate.
6. Provide an audit trail and reporting to satisfy regulatory compliance audits.

Apani Networks’ EpiForce accomplishes the above tasks through an operating system agnostic software solution that protects sensitive data by automatically and dynamically enforcing network security relationships, and encrypting all data-in-motion within a network perimeter. This provides access control, data flow security and the audit trail necessary for HIPAA compliance.

Its centralized management and auto-configuration facilitate an expeditious installation and ease of use, thereby reducing the cost and complexity of securing inside the perimeter, a necessary task to achieve regulatory compliance. This is performed by authenticating, protecting and managing communications to and from every network device through an automated system which has the ability to control security relationships at a granular level.

www.apani.com
3230 E. Imperial Highway | Suite 201 | Brea, CA 92821
Email | compliance@apani.com Toll Free | +1 866.638.5625

HIPAA Compliance: Putting trust back into the "trusted" network

The HIPAA Security Rule has been widely interpreted as ensuring the integrity and security of IT systems relating to protecting patient health information that is collected, maintained, used or transmitted, and the environment in which they operate. As part of this process, the security relationship of nodes within a given environment should be established and implemented according to a stated policy and regularly audited for compliance with this policy.

The ability to define, implement and manage these security relationships between systems that house protected patient health information and the applications and devices that access them demonstrate that healthcare entities are taking steps towards HIPAA compliance. As part of this process, it is critical that the security infrastructure selected to perform this functionality has built in reporting capable of addressing HIPAA reporting and auditing requirements. Apani Networks' EpiForce system can accomplish this requirement, and can provide a history demonstrating remediation for items which were out of compliance.

To prevent unauthorized access, both desktops and servers need to be securely locked down so as to only be accessed by authorized systems. Apani Networks' EpiForce facilitates machine level access control for each workstation and server in the network, and will prepare healthcare organizations for audit scrutiny by fully automating the implementation of the organizations security relationships and by providing a rigorous audit trail.

Conclusion

HIPAA was established to ensure that patient healthcare records could be accessed, retrieved and re-located effectively and securely, and to enforce strong penalties when this confidence has been breached. It requires any organization coming in contact with this data to prepare appropriate internal controls to maintain this privacy. A critical element in achieving compliance is demonstrating that the healthcare data is secure, that the systems accessing the data are secure and that access to this controlled information is closely monitored, preventing unauthorized access.

Based on the research of the FBI and other crime investigating organizations, at least half of the security threats to an organization are a direct result of internal threats, such as a rogue devices, employees or business partners. In order to adequately secure IT systems, maintain data security and achieve HIPAA compliance, organizations must recognize that the "trusted" network is a notion of the past—safeguards must be enacted to protect from the inside attack—and that all data traveling within the network perimeter must be secure.

About Apani Networks' EpiForce

Apani Networks' EpiForce is a centralized security management system designed to secure inside the perimeter providing network access control, dynamic enforcement of security relationships and network wide point-to-point connectivity and encryption. It is a compliance security tool that automatically enforces and audits network security relationships, providing dynamic access control, data flow security and centralized management for an enterprise.

Using the highest levels of encrypted data protection and through the ability to logically segment the network, security managers can control access to critical information and mitigate the impact of security breaches. EpiForce uses a central management system for policy provisioning to consistently apply security policies across the corporate network and reduce the cost and complexity of security and compliance management. Detailed reporting of security associations and security alerts for unexpected network events enables the preparation of internal control reports necessary for regulatory compliance.

The following specific requirements, as referenced within the Information Access Management and Security Awareness and Training sections of the Administrative Safeguards category in the Act, are addressed with Apani's EpiForce:

- Log-In Monitoring
- Access Authorization
- Security Reminders

EpiForce Protects Against Internal Security Threats, Enabling HIPAA Compliance:

- Automatically implements and enforces the network security relationships needed to comply with the latest requirements of HIPAA.
- Divides a network into logical security zones to enforce the security relationships between the nodes through a central management console, thereby simplifying administration and reducing management costs.
- Enables a secure point-to-point encryption system that protects all data-in-motion, preventing unauthorized access to the sensitive data that is carried across your network.
- Provides an audit trail for security relationships including what they are, when they were established, how they have been modified and a guarantee they are enforced.
- Provides reports and alerts on network activity that are critical for enforcing security policies. These reports are vital for day to day management of the network, and are required to prove that your are in compliance with HIPAA.

www.apani.com
3230 E. Imperial Highway | Suite 201 | Brea, CA 92821
Email | compliance@apani.com Toll Free | +1 866.638.5625

About Apani Networks

Apani Networks is a leader in Enterprise IT network security, providing protection for critical network data and securing the evolving edge of corporate networks. Established in 2003, Apani Networks puts the trust back into trusted networks by providing centrally managed IT Security Compliance solutions that automatically and dynamically implement and report on network wide security relationships. Apani's encryption-based security solutions allow corporate IT managers to quickly, automatically and cost effectively lock down their trusted networks, while providing the audit trail necessary to demonstrate compliance to the wide range of regulations that affect enterprises today.

Visit our website **http://www.apani.com** to download White Papers focused on the different compliance regulations, and how they might impact your organization.

Free regulatory compliance IT security cost / benefit calculator: **http://www.apani.com/calculator**

This confidential calculator allows you to:

1. Establish potential security cost savings for any security initiative.
2. Create and compare "what if" scenarios for planning purposes.
3. Print out customized reports

3230 E. Imperial Highway | Suite 201 | Brea, CA 92821
Email | compliance@apani.com Toll Free | +1 866.638.5625