Global Information Assurance Certification Paper

Overview of HIPAA's Security Concepts

Marcia Branco

April 13, 2000

HIPAA is the Health Insurance Portability and Accountability Act. President Clinton signed this federal mandate into law during 1996. The main goals of HIPAA are 1) guarantee health insurance coverage of workers during job transitions 2) protect privacy of patient records 3) promote national, uniform security standards for the secure electronic transmission of health information. Complex HIPAA regulations govern various aspects of the healthcare industry. Numerous standards bodies and national agencies are involved in the development of HIPAA rules.

The DHHS, Department of Health and Human Services, is the governing body for the security requirements of HIPAA. The DHHS must follow a formal procedure for setting security standards. First, it must develop recommendations for standards to be adopted. Next, it must publish the proposed rules in the Federal Register. This is commonly known as an NPRM or Notice of Proposed Rule Making. Then there is a 60-day Comment Period where suggestions and recommendations specific to the NPRM are accepted. At the end of the Comment Period, comments and suggestions are analyzed and changes may be incorporated into the proposed regulations. Eventually, the Final Rule is published in the Federal Register. At this point, all health plans, health care providers and health care clearinghouses that electronically store, maintain or transmit in any format individually identifiable health care information must begin HIPAA security compliance procedures.

The NPRM for Security and Electronic Signature Standards was published in 1998. However, no Final Rule for these standards has been published yet. Many industry experts believe a Final Rule for Security Standards will be published before the end of this year. Large and medium sized organizations must be compliant with HIPAA security requirements 24 months after the Final Rule is published. Smaller companies have 36 months to become compliant. Penalties for known misuse of individually identifiable health information and failure to comply with HIPAA security requirements can result in fines up to $250,000.00 and/or up to 10 years imprisonment.

The path to HIPAA compliance can be arduous and costly. One of the first steps to HIPAA compliance is to create organizational awareness of HIPAA. One way to do this is to appoint a Security Officer to oversee the security requirements of HIPAA. HIPAA executive awareness presentations should be made to Senior Management. Creation of a HIPAA Security Team is key. Next, it is essential to perform an enterprise-wide assessment of the computing infrastructure. Remember, some of the Y2K documentation may be a good starting point for this assessment. Periodically, review the DHHS Security and Electronic Signature Standards NPRM (http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule.rule?user_id=&rule_id=62) for timetables and updates. This may be a good time to present a report to executive management that identifies gaps in the current infrastructure's HIPAA compliance, as well as, strategies to eliminate those gaps. At this point, you may be ready for the path to implementation. Training may be necessary for some implementation projects. Audits should be performed after implementation is final and also on an on-going basis.

DHHS security standards are technology-neutral and scalable. Security is a multi-step process of continual creation, implementation, monitoring, testing and managing using various products for each step. The HIPAA open security standards understands the complexity of security and permits each health related entity to determine what technology best satisfies HIPAA security requirements in its own unique environment. Also HIPAA security regulations allow for the effected businesses to factor the economic costs of HIPAA against potential security solutions, as well as take advantage of emerging technologies. Additionally, companies in the health care industry should maintain documentation outlining the development, implementation and maintenance of required security standards, including periodic review of this material and its related processes.

The DHHS has grouped security standards into four categories:

- **Administrative Procedures**
  documented general practices for establishing and enforcing security policies
- **Physical Safeguards**

documented processes for protecting physical computer systems and related buildings and equipment from natural and environmental hazards and intrusions

- **Technical Security Services**
  security services for protecting, controlling and monitoring access to data
- **Technical Security Mechanisms**
  mechanisms for protecting information and restricting access to data transmitted over a network

The outcome of the four security categories established by the DHHS is to guard the availability, confidentiality and integrity of data. A Security Policy should include those measures. Availability relates to how long data or a system is up and running versus the time it is down and unusable. One infamous threat to the availability to a system is a DDoS or distributed denial of service attack. This attack was perpetrated on the Yahoo web site. There are various security measures to reduce the vulnerability to availability attacks. Bandwidth management devices, commonly known as QoS - Quality of Service, control what type and percentage of traffic can enter or leave a network. Router access control lists may also determine what type of traffic is available on a network. Anti-virus software can additionally ensure system availability. An IDS or intrusion detection system can detect security breaches that may impact system availability, inhibit further intrusive activity and sound alarms for particular events. Disaster recovery planning can dramatically increase the availability of data during catastrophes. Physical security of data maintains the availability of data by ensuring that an unauthorized person does not have access to delete important data. Centralized logging, reporting functions and data backup help to sustain data availability.

Confidentiality relates to protecting data from unauthorized access or keeping secrets secret. Packet sniffing clear text data across a network is a prime example of a confidentiality compromise. An IPSec VPN using 3DES encryption is one of today's best security solutions to preserve the confidentiality of data. An encrypted VPN solution will create a tunnel between two end-points over an insecure network and encrypt the data traversing it. 3DES is the strongest encryption algorithm available today. IPSec is the emerging standard for ensuring network layer encryption and authentication over IP networks. IPSec permits VPN connectivity in multi-vendor environments.

Data integrity is the assurance that data has not been altered. Spoofing is a common attack to data integrity. A secure network perimeter is a good start to protecting data integrity. Properly configured firewalls and routers can combat numerous attacks. Baselining systems and then performing periodic reviews against the baseline by using a product such as Tripwire preserves data integrity. Identity is closely related to data integrity. Features such as strong password filtering and two tier authentication schemes with the use of token cards provide proof of identity.

Electronic Signature Standards is another aspect of the HIPAA Security Regulations. Electronic signatures are not yet required. However, if electronic signatures are used, it is mandated that they be in the form of digital signatures performing the following three tasks: message integrity, non-repudiation and user authentication. Message integrity promises that the message has not been tampered with during transport from sender to receiver. Non-repudiation proves that the sender and only that sender sent the message. User authentication means that the user was authenticated in order to send the message. Digital signatures involve the following components: encryption algorithm (ex. 3DES), hashing algorithm (ex. MD5), a key pair and software such as PGP. The sender uses a hash algorithm to create a one way hash value of the message. This hash value is the message digest. Then the sender uses the sender's private key to encrypt the message digest into a digital signature that is attached to the original electronic message. The receiver uses the sender's public key to 1) determine whether the digital signature was created using the associated private key and 2) to create a new hash of the message that should match the original hash result. If both hashes match, the digital signature is verified. PKI, public key infrastructure, is another approach to implementing digital signatures. This can be a very complicated security feature to implement.

Security is a highly complex field that touches upon many aspects in the business world. Security in the health care industry is an even more elaborate discipline that is constantly evolving. HIPAA Security Regulations are trying to create some general security concepts for all health care related businesses to follow. By doing this, HIPAA is highlighting the importance of security by deeming it an operational

requirement. All health industry businesses, their partners and patients can benefit from HIPAA Security Regulations.

Sources

Department of Health and Human Services. Administrative Simplification. 12 April 2000.
URL: http://aspe.os.dhhs.gov/admnsimp/index.htm (10 April 2000).

Department of Health and Human Services. Notice of Proposed Rule Making for Security and Electronic Signature Standards.
URL: http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule.rule?user_id=&rule_id=62 (7 April 2000).

Cisco Systems. Security and Health Care Enterprise Networks: Balancing Technology and Culture. 10 April 2000.
URL: http://www.cisco.com/warp/public/cc/sol/mkt/ent/inds/hlth/shcen_wi.htm (6 April 2000).

3Com. HIPAA E-Source. 28 March 2000.
URL: http://www.healthcare.3com.com/securitynet/hipaa/indexl.html (5 April 2000).

Phoenix Health Systems. HIPAAdvisory.
URL: http://www.hipaadvisory.com (11 April 2000).

QuadraMed Corporation. QuadraMed's Internet Forum on HIPAA Preparedness. 23 March 2000.
URL: http://www.hippa-iq.com/default.htm (5 April 2000).