Donna M. Morgan, BS, CMA
GSEC Practical Assignment
Version 1.4 Option 1
A Journey towards HIPAA Security Compliance

Introduction.

No matter where you go in healthcare today, what healthcare magazine you pick up or what healthcare seminar you see advertised, the most widely reviewed topic being presented is HIPAA. But exactly how does a small rural hospital become compliant with the HIPAA Standards? What types of blocks are these organizations dealing with along the way to compliance? Where should they begin?

This report does not focus on the actual HIPAA regulation but rather takes a closer look at the reality of what is now happening inside the healthcare industry with regard to the Proposed HIPAA Security Standard. It takes a walk-through the possible steps and blocks of a fictional small rural hospital, which for the purpose of this report shall be called " Mercy Hospital". Because the entire HIPAA Regulation is well beyond the scope of this report, the focus will be on the Proposed Security Standard, which was first published as a NPRM (Notice of Proposed Rule Making) in the Federal Register on August 12, 1998 and has yet to be finalized. What security changes might a small rural hospital make to become HIPAA compliant? By breaking down the HIPAA Proposed Security Standard, felt by some to be overwhelming, organization can make the process manageable. We in the healthcare industry have no choice but to change our way of practice.

In a perfect world, consultants or technical vendors would come to the rescue of these small entities; however, the healthcare industry in some areas is facing devastating financial problems. Mergers, buyouts and closures are becoming common. How do you secure a small rural hospital with a negative cash flow?

At the beginning…Congress said, let there be HIPAA, and a new age was born!

What is the Health Insurance Portability and Accountability Act?

Over the past few years, members of the healthcare industry in the United States have become familiar with the Health Insurance Portability and Accountability Act of 1996, also known as HIPAA. The most famous section of this law is the Administrative Simplification, known as Title II - Subtitle F.

The Administrative Simplification is divided into several standards. The three which are causing the most concern at this time are the:

Transaction Code Set Standard - This is the regulated format to be used when submitting all electronic transactions. The deadline for this standard is October 16, 2002. Due to the complexity of meeting this standard, the Department of Health and Human Services (HHS) has agreed to extend the deadline by one year to healthcare providers who request an extension by the original deadline date.

Standards for Privacy of Individually Identifiable Health Information - Mandated guidelines of protecting the privacy of patient health information. The deadline of April 14, 2003 is fast approaching. However, in March of 2002, HHS published proposed changes to this standard, which as of the writing of this report has yet to be finalized.

Proposed Security and Electronic Signature Standards - The mandated guidelines for the security of Patient Identifiable Data whether in transit or stored. Although originally published in the Federal Register in 1998, these standards have not been finalized.

On May 31, 2002, the Department of Health and Human Services (HHS) published in the Federal Register, the Final Rule to adopt National Employer Identification Standard for use in healthcare transactions. The compliance deadline for this standard is July 30, 2004 for healthcare providers.

Proposed Security Standard

Why look at the Proposed Security regulation if it is not finalized?

The deadline date of April 14, 2003 for the HIPAA Standards for Privacy is quickly approaching, while it is very difficult to comply with mandated privacy regulations without implementing security procedures. Thomas Walsh, principal consultant at CTG HealthCare Solutions in Cincinnati put it nicely when he was quoted as saying, "You can have security without privacy, but you cannot have privacy without security."[4] Because of this reality, most healthcare providers are starting to implement security procedures within their organizations.

Where to begin??

"Mercy Hospital"

Shortly following the Y2K crisis, Mercy Hospital began its journey toward HIPAA compliance. Numerous members of the healthcare and administrative staff attended intense educational seminars, read white papers, articles, books and even did research on the Internet. They appointed a HIPAA Project Manager for the coordination of the project, a Privacy Officer (the Director of Medical Records) to oversee the privacy standards, and an Information Security Officer (the Director of the Information System Department) who would be responsible for developing the computer and information security program to be adopted by senior management.

Information Security Officer
The ISO is responsible for advising on protective measures such as policies and procedures, measuring performance, and reporting to management. The ISO is also responsible for the confidentiality, integrity and availability of all Protected Health Information (PHI) at their hospital as regulated by the HIPAA standard. [5]

Exactly what type of information do they have to protect?

The Information Security Officer (ISO) needed to become familiar with the Proposed HIPAA Security Standards as published in the Federal Register and the restrictions placed on PHI at his institution.

Protected Health Information under the HIPAA regulation is defined as any information, whether oral or recorded in any form or medium, that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. [1]

During the course of an average patient's hospitalization, there could be hundreds of individuals working on the patient's care who would have been granted access to the patient's protected health information. Admitting personnel, physicians, nurses, technicians, and care managers, are just some of the individuals who may play a role in a patient's recovery.

How could they possibly secure PHI in this environment?

The Risk Assessment Process at Mercy Hospital

Following the appointment of an Information Security Officer, a HIPAA Steering Committee was developed, representing all areas of the hospital. The first assignment for the ISO was to assess the potential risks and vulnerabilities to PHI at Mercy Hospital as required in Sec 142.302 of the HIPAA Proposed Security Standard.

During this risk assessment and remediation initiative phase, it quickly became apparent there were no written security policies or an overall Information Security Program in place. A gap analysis was developed, which compared the risk assessment done at Mercy Hospital against the HIPAA Proposed Security Standards. This analysis revealed to the HIPAA Steering committee there were numerous vulnerabilities, a lack of policies and procedures along with a cultural change, which needed to be addressed before the hospital could become compliant.

There are four sections to the HIPAA Proposed Security Standard:

1. Administrative Procedures

2. Physical safeguards
3. Technical security
4. Technical security mechanisms[1]

Mercy Hospital examined each of these four sections in depth to determine the course of action needed. Especially noticed was the lack of policies and procedures, the need for house wide education, and hopefully a cultural change. Since the HIPAA Standards are technology neutral and scalable, it became important to develop a plan to meet the needs of Mercy Hospital along with being compliant. Mercy Hospital identified HIPAA as the instrument to develop a new way of doing business.

1. The Administrative Procedures

Administrative Procedures are documented formal practices, which are developed to manage the selection and execution of security measures to protect data and to manage the conduct of personnel in relation to the protection of data. [1]

Security Policy and Procedure Development

In a small rural hospital, it is not uncommon to find there are no formal written policies and procedures regarding the Risk Management of information security. Since an identified vulnerability was having no defined Security Program in place or any policies and procedures dedicated to information security, a subgroup of the Steering Committee was formed and given the task of developing draft policies or programs. These policies would be reviewed by the ISO and the entire HIPAA Steering committee. To begin the process, they used the Security NPRM, which lists Technical Practices and Procedures, to be addressed with formal written policies or by implementing technical procedures. [1]

1. Individual authentication of users – Refers to the verification that individuals are who they say they are. How would they accomplish this? Digital Signatures, perhaps?
2. Access controls – Refers to a method of restricting access to resources, allowing only privileged entities or individual access. They also needed to consider the types of access controls such as; mandatory access control, discretionary access controls, time-of-day access and classification of Mercy Hospital's data.
3. Audit trails – A chronological record of system activities, who went where…. when
4. Physical security and disaster recovery – refers to how Mercy Hospital would deal with the physical security of their data systems, such as locks, passwords or ID's, and the development of a Disaster Recovery plan.
5. Protection of remote access points – How would Mercy Hospital deal with remote access points such as clinics, physician offices, pharmacies, rehab centers that are owned by the hospital but which reside off campus. Also they needed to take a look at the number of employees who worked from home or were able to access the hospital network from a remote area. How would they secure this information? VPN perhaps? Strong Policies?

6. Protection of external electronic communications – How would Mercy Hospital deal with protecting electronic communications such as email between themselves and Business Associates such as lawyers, billing services and other facilities where they need to exchange PHI for the treatment or payment situations for the benefit of the patient?
7. Software discipline – What would Mercy Hospital decide would be the policy and procedure for handling software used within the hospital network?
8. System risk assessment – How would they perform an initial risk assessment and how often would they perform a follow up?

A second subcommittee was formed to examine the current Organizational Security Practices regarding Protected Health Information. Their task included the examination of:

1. Did Mercy Hospital have entity wide Security and confidentiality policies?
2. How would they deal with Security Education and Awareness Training programs for the entire staff regarding the HIPAA Security Standards and all policies and procedures developed by Mercy Hospital? How often would they review these policies and procedures and if changed how would they educate the staff?
3. The need to develop a Sanctions Policy for any violation of written policy and procedures, which would be addressed by the Steering Committee. Furthermore, Administration would need to back this policy with realistic ramifications.
4. The need to develop a Chain of Trust Partner Agreement to be signed by all entities not owned by Mercy Hospital needing access to PHI in order to do a function or service for Mercy Hospital.

A final sub committee worked on the additional requirements of the Administrative Procedures under the Proposed HIPAA Security Regulation[1], such as:

- Certification of the computer system or network. This is a technical evaluation performed as part of the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements.
- Developing a Contingency Plan for responding to a system emergency. This plan would include how Mercy Hospital would perform backups, and if they would prepare critical facilities or hot sites they could use to facilitate continuity of operations in the event of an emergency or disaster.
- Develop documented policies and procedures for the routine and non-routine receipt, manipulation, storage, dissemination, transmission, and/or disposal of Protected Health Information
- Develop Information access control policies, which would grant individuals different levels of access to Protected Health Information on a “need to know basis”.

- Develop and implement or purchase an Internal audit system, which would review hospital records of system activities such as logins, file accesses, and security incidents.
- Develop policies and procedure on Personnel security, which will insure that all personnel who have access to any PHI have the required authority and a "need to know".
- Develop Security Configuration Management Systems, which would include written security plans, rules and procedures concerning the components of an organizations security, hardware and software installation and maintenance review, inventory, security testing, and virus checking.
- Develop Security incident policies and procedures for the tracking of security breaches that would include report and response procedures.
- Develop Termination policy and procedures for the ending of an employee's employment. This policy needs to include changing of locks, removal of user accounts, turning in of keys, tokens, access cards, etc.
- Develop and implement a Security Training Program, which would educate all users concerning the vulnerabilities of the health information in an organization possession and ways to ensure the protection of that information. This includes awareness training, periodic security reminders and user education on the use and importance of virus protection.
- Also needed is a Security Management Process which would be responsible for the creation, administration and oversight of policies to ensure the prevention, detection, containment and correction of security breaches involving risk analysis and risk management. Included in this process is the establishment of accountability, management controls, policies and education, electronic controls physical security and penalties for the abuse and misuses of its assets both physical and electronic.

So what happens when all the policies and procedures are in place?

Education/Cultural Change

One of the most important parts of the HIPAA implementation plan is development of strong policies and procedures and the education of the organization's employees. An organization can develop strong policies and put in place highly technical security systems, but without the necessary education and needed cultural changes will succeed in doing nothing to prevent the security of their system.

The first line of defense at Mercy Hospital is the staff; the employee who interacts with the patient and patient’s family, employees who create, receive and has access to hundreds of pieces of PHI on a daily basis. If the staff of Mercy Hospital is unaware of, resistant to or takes lightly the potential risk of divulging PHI, they become the most frequent reason for failure of an organizational initiative to become HIPAA compliant.

The Proposed Security Standards requires that all covered organizations develop, maintain, and educate their employees, trading partners, and/or contractors. [8] the mandatory education needs to consist of:

- Health Care Information Security
- Virus Protection
- Risk management
- Media management
- Chain of Trust
- Security Management
- Incident Reporting
- Configuration change Management
- Policies and procedures required to comply with the HIPAA standard
- Technical Infrastructure and Operation Required to Support the Security NPRM.[8]

D'Arcy Guerin Gue who wrote "The Step Child of HIPAA Compliance: Culture Change", coined a phrase and simple definition of the work "HIPAAtized". She stated a HIPAAtized culture might be "where compliant attitudes, behaviors and sensitivity to patient privacy and confidentiality become second nature and assumed throughout the workforce." [3] Easier said then done!

2. Physical safeguards

The Information Security Officer at Mercy Hospital performed a risk assessment on the physical safeguards throughout Mercy Hospital. Again, when he brought these findings to the HIPAA compliance Committee there were many vulnerabilities identified, which need to be examined.

One vulnerability was the need for written policies and procedures. The first identified was the need for Media control policies. These would provide a formal written procedure for how Mercy Hospital accepted the receipt and removal of hardware or software, such as diskettes and tapes into and out of the organization.

These policies needed to specify Access controls, such as

- Accountability – means that would ensure that the actions of an organization or individual could be traced uniquely to that organization or individual.
- Data backup or retrievable exact copy of information – How does Mercy Hospital want to deal with data backup? How often would there be backups? Where would it be stored?

- Data storage or the retention of PHI – Where will Mercy Hospital store PHI, how is it stored, how long will it be stored, etc.
- Disposal or final disposition of electronic data, or the hardware on which electronic data is stored. What method of disposing of electronic data or hardware will Mercy Hospital develop as its Disposal Standard Policy? Degauss? Who is responsible, where will this be documented?

The next big undertaking the HIPAA Compliance Committee and the Information Security Officer needed to embark on was to develop systems which would protect PHI by setting policies and standards regarding Physical Access Control.

Physical Access controls are the written policies and procedures that limit physical access to Mercy Hospital and/or PHI, which resides in the organization. However the policies and procedures must also allow for properly authorized access to be allowed without delay. In times of emergency in a hospital setting properly authorized personnel need to have immediate access to PHI. If not delays could become deadly.

In order to keep the hospital up and running at all times and in the wake of the lessons learned on September 11, 2001, a Disaster recovery plan needed to be developed by members of the Steering committee at Mercy Hospital. Because of the enormity of this task and the critical nature of this issue, the members of the HIPAA Steering Committee decided they would look to outsource Disaster recovery. They began the process of looking for the correct vendor by searching the Internet, setting up conferences, setting their goals and hiring an outside firm.

An emergency mode operation would need to be developed which would allow the organization to continue to operate in the event of fire, vandalism or system failure.

Of course in order to have a security system, Mercy Hospital needed to have control over bringing hardware and software into and out of the hospital. It also needed a way to maintain a record of that equipment which included marking, handling and disposal of hardware and storage media. Equipment Control policies and procedures would need to be developed for this reason.

Workstation policies and procedures needed to be developed. These policies would be the guidelines of what Mercy Hospital expected to be the proper functions to be performed, the manner in which those functions are to be performed and the physical attributes of the surroundings of the specific computer terminals site or type of site.

3. Technical security

What type of access should be developed?

One of the most important decisions Mercy Hospital needed to make was what type of access control it would use for the security program. The proposed HIPAA security standard mandates the use of one of the following Access controls:

- ◊ Context-based access
- ◊ Role-based access
- ◊ User-based access

Role-based access as described by David Ferraiolo and Richard Kuhn while writing for the National Institute of Standards and Technology explained role based access:

> "Once the transactions of a Role are established within a system, these transactions tend to remain relatively constant or change slowly over time. The administrative task consists of granting and revoking membership to the set of specified named roles within the system. When a new person enters the organization, the administrator simply grants membership to an existing role. When a person's function changes within the organization, the user membership to his existing roles can be easily deleted and new ones granted. Finally, when a person leaves the organization, all memberships to all Roles are deleted. For an organization that experiences a large turnover of personnel, a role-based security policy is the only logical choice." [7]

Of course all access would be required to have a unique user identifier for identifying and tracking individual user identities.

Along with a unique user identifier, the Proposed Security Standards also requires at least one of the following implementation features:

- Biometric identification – such as fingerprint patters, iris scan, retinal scan voice prints, or hand written signature
- Password – which must be unique and follow a password policy developed by Mercy Hospital
- Personal identification number – or PIN number used to provide verification and identification
- A telephone callback procedure – a procedure used to authenticate the identity of the receiver and sender of PHI through a series of questions and answers.

It is important to remember when implementing access controls that employees who have authorized access commit most security breaches. According to an Information Week/ Price Waterhouse Study, authorized personnel commit 58% of all breaches, unauthorized employees commit 24% and former employees commit 13%. This accounts for an amazing 95% of all breaches come from within. [6]

4. Technical security mechanisms

The final section of the HIPAA Proposed Security Standards which Mercy Hospital needed to assess and implement, was the technical security mechanisms. If members of the healthcare staff at Mercy Hospital use the network as a means of communication of PHI, the following technical security mechanisms needed to be in place.

- Integrity controls – refers to a mechanism, which ensures that the information received has not been altered during transmission.[2] Mercy Hospital decided to look closer at using digital signature to achieve this requirement.
- Message authentication – the method used to provide a level of assurance through validation of a sender's message.[2] By assigning unique user ID's and passwords when using the network, Mercy Hospital took the first step toward providing message authentication.

In addition to Integrity controls and message authentication, Mercy Hospital needed to implement one of the following in order to be in compliance with the Proposed HIPAA Security Standards;

- Access controls
- Encryption
- Alarm
- Audit trail
- Entity authentication
- Event reporting

Summary.

The HIPAA Proposed Security Standards at first glance seem to be overwhelming. If these standards are taken individually most individuals who are responsible for the compliance of these standards will see they are good common sense and good common business practice. The hardest obstacle in implementing these regulations is the education and cultural change, which needs to take place within the entire healthcare industry.

References:

1. U.S. Department of Health and Human Services. "Notice of Proposed Rule Making for the Security and Electronic Signature Standards". 12 August 1998
URL: http://aspe.hhs.gov/admnsimp/nprm/seclist.htm (June 12,2002)

2. Romig, Tautra, " HIPAA Compliance: Cost-Effective Solutions for the Technical Security Regulation". SANS Institute, November 21, 2001,
URL http://rr.sans.org/legal/HIPAA_primer.php (July 1, 2002)

3. Guerin Gue, D'Arcy, "The Step Child of HIPAA Compliance: Culture Change", HIPAAdvisory, Phoenix Health Systems

URL: http://www.hipaadvisory.com/action/Compliance/culture.htm (June 15, 2002)

4. Health Data Management, "Tracking HIPAA Security Progress" 13 June 2002
URL:http://www.healthdatamanagement.com/html/hipaa/NewsStory.cfm?DID=8674
(June 27, 2002)

5. Peltier, Thomas R., "Information Security Policies, Procedures, and Standards",
Boca Raton, FL: Auerback Publications, 2002 , Pg 65

6. Place, MHA, Nancy, "HIPAA Security Implementation: Critical Success Factors", IBM HIPAA National Practice, Slide 7, 3 August 2002
URL: http://www.nhvship.org/download/NancyPlaceIBM.ppt , (June 28, 2002)

7. Ferraiolo, David and Kuhn, Richard" Role-Based Access Control (RBAC)", National Institute of Standards and Technology, 9 January 1995
URL: http://hissa.ncsl.nist.gov/rbac/paper/rbac1.html (June 20, 2002

8. WEDI Workgroup, "Awareness Training and Education", WEDI Strategic National Implementation Process (SNIP), Pg 4, December 2001
URL: http://snip.wedi.org/public/articles/awareness.pdf (June 25, 2002)