# A Brief on HIPAA for the IT Auditor

Annie Brauitigam

November 2001

This paper was written assuming that the IT Auditor is aware of the Health Insurance Portability Act of 1996 (HIPAA) yet would like further advice on what this means for their role in the healthcare industry.

## What is HIPAA?

The U.S. Department of Health and Human Services (HHS) have released the first standards governing the privacy of Americans' health information to protect medical records maintained by a covered entity. President Clinton and Congress enacted HIPAA in 1996 with the objective to reduce healthcare fraud and abuse, ensure security and privacy of health information, ensure portability, and enforce health information standards.

## Must my organization comply with HIPAA?

Covered entities as well as any organizations that transmit information from a covered entity or to a covered entity must comply with the standard. A covered entity includes all health plans, health care clearinghouses, employee groups that are self insured with over 50 employees, and health care providers who transmit any health information in electronic form in connection with a standard transaction.

HIPAA does not distinguish between what a covered entity may do on-line vs. off-line but there may be a gray area where consumers may not be aware if their information is protected under HIPAA. According to a recent article in the HIPAA Advisory, HIPAA will not provide much protection to Internet users. Although websites hosted by covered entities must adhere to these regulations, they do not apply to non-covered entities such as websites selling non-prescription drugs, mental health websites that accept credit cards, pharmaceutical company websites, and general health advice websites including foodfit.com and medigenious.com.

## What steps must my organization take to become HIPAA compliant?

1. Designate a HIPAA Security Officer and develop a HIPAA group consisting of key members of management and areas of the organization to act as the leaders of HIPAA in the organization. These individuals should regularly meet to discuss the implications of HIPAA, the benefits that may be gained, the status of HIPAA compliance, and issues that arise that may implicate the organization's compliance with HIPAA.
2. Research the HIPAA regulation and keep informed of progress of the standard as well as your organization's progress for compliance.
3. Have an independent assessment performed to determine where the organization stands regarding compliance. This assessment should include a gap analysis outlining the regulation, what the organization is currently doing and what the organization needs to do in addition for compliance with the regulation. The thoughts and ideas in the establishment of HIPAA may not be new for your organization and your organization may already be taking the necessary steps to ensure patient information is protected. Many organizations may find some of the HIPAA regulations to build on the prior

regulations set forth by the Centers for Medicare & Medicaid Services (CMS) formerly known as the Health Care Financing Administration (HCFA) or state laws.

4. Review recommendations from the gap analysis performed.
5. Identify alternative solutions and decide on the most effective and practical solution. Keeping in mind that the benefits should outweigh the costs, HIPAA specifically left the standard broad enough for interpretation. This interpretation allows technology to expand as well as not forcing small organizations to undergo extreme and unnecessary changes.
6. Develop an action plan based on the items identified in the gap analysis. This action plan should take into account criticality and an order in which items must be performed. This action plan should include reasonable deadlines as well as the responsible party for carrying out the task. A large portion of this action plan should address the training of employees regarding HIPAA as it relates to their job duties and providing access to the HIPAA group regarding questions and concerns.
7. Develop Chain of Trust agreements with business associates with whom protected information is shared.
8. The action plan should be continually reviewed and revised to ensure that all items have been remedied by the final compliance date.
9. The HIPAA Compliance group or Internal Audit should perform reviews of the organization and employees to ensure compliance and understanding. Additionally the information systems and networks may need to be independently reviewed and certified as necessary. This will be determined by contracts with business associates and corporate standards.

**Who can help my organization become and maintain HIPAA compliant?**
Many consulting firms specialize in HIPAA and can assist your organization to become HIPAA compliant. These may include specialty-consulting firms as well the “Big 5” accounting firms. Although these groups do not actually determine if you are HIPAA compliant, they will prove to be very useful in providing guidance in determining the courses of action to take. The Internal Audit department of the organization should also be utilized in the beginning stages of organization becoming HIPAA compliant as well as ensuring that compliance is maintained.

**Who is the regulatory oversight agency in charge of ensuring organizations are compliant?**

The HHS Office for Civil Rights will enforce the regulations.

**How will the oversight agencies determine compliance?**
Oversight agencies will be responsible for determining whether the covered entities are performing their responsibilities and obligations for protecting and securing patients’ protected health information. The burden of proof that an entity is complying with HIPAA is the responsibility of the entity. These responsibilities include 1) keeping records and submitting compliance reports containing the information required by the Secretary in a timely manner determined by the Secretary, 2) cooperating with the Secretary regarding complaint investigations and compliance reviews of the policies, procedures, or practices of a covered entity to determine compliance with regulations, and 3) permit access to requested information to the Secretary during normal business hours.

**What are the areas of concern regarding HIPAA?**
Although HIPAA deals with privacy, security, and transaction code sets, I will discuss the security standards for HIPAA since it may be of the most concern for IT auditors. A HIPAA Security Matrix has been developed to outline the administrative, physical safeguards, and technical procedures and mechanisms to guard against data integrity, confidentiality, and availability as well as the use of electronic signatures.

**Administrative Procedures to Guard Data Integrity, Confidentiality and Availability**

Certification
Organizations will be required either to evaluate their information systems and networks internally or externally to ensure that appropriate security has been implemented and maintained.

Chain of Trust Partner Agreement
When a covered entity is transmitting protected health information to another party, a Chain of Trust Partner Agreement must be entered into. This would be a contract between the two parties to maintain the same level of security to ensure the integrity and confidentiality of the information transmitted.

Contingency Plan
A contingency plan must first provide for the backup of data in the event that equipment malfunctions or a disaster was to occur. Data needs to be frequently backed up and stored at a remote off-site location. This off-site location needs to be far enough away that it would not be affected by a disaster at the primary location yet near enough that it can be quickly accessed in the event of an emergency. Next, a criticality analysis of the data and applications needs to be performed for an effective startup of operations. A disaster recovery plan as well as a business continuity or emergency mode operation plans needs to be documented. While a disaster recovery plan is more concerned about the immediate disaster and recovering, a business continuity plan is more concerned about how to keep the business running until the organization has recovered from the disaster. Most importantly, these plans need to be tested and kept up to date to ensure that they cover all critical aspects of operations and can sustain a disaster.

Information Access Control
Access to the organizations' information systems must be controlled through proper authorization, establishment and modifications to access.

Internal Audit
It is required that there is ongoing internal review of the records of the system activity to ensure that compliance is maintained and remedy any security violations that may occur.

Personnel Security
Personnel security needs to start with hiring trustworthy employees and performing background checks on all employees with logical or physical access to protected health information. Records of access authorizations need to be maintained. All system users including maintenance personnel need to be trained in security and provided with policies and procedures for handling security situations. Physical and logical access needs to be proper and appropriately maintained

as job duties and the organization change. It should be ensured that an authorized, knowledgeable person supervises maintenance personnel.

Security Configuration Management
The organization is required to implement procedures to ensure routine hardware and software updates and changes do not create security weaknesses. These procedures include documentation, hardware/software installation testing and maintenance review and testing for security features, inventory procedures, security testing, and virus checking.

Security Incident Procedures
Formal documented procedures for reporting security breaches need to be established to include reporting and response procedures.

Security Management Process
A formal security management process will need to be in place to address a wide range of security issues including risk analysis, risk management, a sanction policy and a security policy.

Termination Procedures
Termination procedures are necessary to provide clearly defined steps to be taken for the ending of an employee's employment or internal/external user's access. These mandatory implementation features include changing combination locks, removal from access lists, removal of user account(s), and the return of all keys, tokens or cards that allow access.

Training
Training will be required for all employees for understanding of the vulnerabilities of the protected heath information and the procedures that must be followed to ensure the security and privacy of such information. The training implementation procedures necessary to be implemented include 1) Awareness training for all personnel, including management, 2) periodic security reminders, 3) user education concerning virus protection, 4) user education in monitoring login success/failure and how to report discrepancies and 5) user education in password management.

**Physical Safeguards to Guard Data Integrity, Confidentiality and Availability**

Assigned Security Responsibility
One individual or department must be responsible for security and their responsibilities and obligations documented. This forces the responsible party to take charge of security and ensure that security of information systems and networks is maintained.

Media Controls
Documented policies and procedures are necessary for the receipt and removal of hardware/software in/out of the organization. Necessary media controls would include controlling access to the media to only necessary individuals and ensuring accountability of all transactions. Procedures must also be documented and followed for backup, storage and retention of data.

Physical Access Controls
Formal documented policies and procedures limiting access to an entity as well as ensuring the appropriate access for the individuals with access would be necessary. Controlling physical access to the organization must also be documented in the disaster recovery plan, business resumption plan, control of equipment procedures, the facility security plan, security procedures for those on a need-to-know basis, sign-in for visitors and an escort, if appropriate, as well the testing and revision of these procedures as necessary.

Policy/Guideline on Workstation Use
Organizations must have a policy on workstation use to enhance security. Some items to include in the policy would be a sign-off when leaving the computer unattended as well as having employees sign this policy upon employment. Employees should revisit this policy at least annually to ensure that employees understand their responsibilities and obligations to the security of the organization.

Secure Workstation Location
Organizations have the obligation to place workstations in secure locations. When they are not able to place workstations in secure locations, mitigating controls should be in place using increased security. Some example of possible mitigating controls include increased use of user IDs and passwords and logging the user off when the terminal has been inactive for a period of time.

Security Awareness Training
All employees, agents and contractors would be required to have security awareness training in regards to physical safeguards. For more information on what this training might entail, please refer to the Training discussed in Administrative Procedures to Guard Data Integrity, Confidentiality, and Availability.

**Technical Security Services to Guard Data Integrity, Confidentiality, and Availability**

Access Control
Organizations are required to restrict access on a need basis. Access control should also allow for procedures for emergency access regarding disasters and other immediate issues such as the DBA taking a vacation. Access must also be based on one the following three access methods; context-based access, role-based access or user-based access. Encryption is also recommended to ensure access control although it is not required at this time.

Audit Controls
Organizations are required to record system activity and review suspicious activity to identify and react to unauthorized access on a timely basis.

Authorization Control
Organizations must have a mechanism in place for obtaining consent from the patient for the release of their health information. Organizations must ensure that only authorized individuals have access to protected health information to oversee this activity. An organization may use the

various types of access control mentioned above such as using role-based or user-based access to accomplish this task.

Data Authentication
Organizations must be able to prove that data has not been altered or destroyed while in their possession. Some possible methods of proof mentioned in the standard include checksums, double keying, a message authentication code, or the use of digital signatures.

Entity Authentication
Organizations will be required to implement entity authentication to ensure that a party is who they claim to be. Organizations must uniquely identify each user as well requiring an automatic logoff after a period of inactivity. This period of inactivity should be shortened for workstations in non-secure areas. Additionally the standard requires one the following to be implemented; a biometric identification system, a password system, a personal identification number (PIN), telephone callback, or a token system that uses a physical device for user authentication. It is up to the organization to decide which of these methods would not only be the most efficient in their organization but also must be effective for the situation.

### Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted over a Communications Network

Organizations that use a communications network to transmit data must protect communication transmitting protected health information to ensure that only the intended recipient receives the data. To protect communications, organizations must implement integrity controls and message authentication. These will ensure that the data was not altered in anyway from the time the message was sent and that the message came from the party who claims they sent it. Either access controls or encryption must also be used when protected health information travels over a communications network. Lastly, the standard requires that the following four mechanisms must also be used when transmitting data over a communications network; an alarm, an audit trail, entity authentication, and event reporting which must be reviewed and followed up on.

### Electronic Signature

Although HIPAA does not require the use of electronic signatures, the standard does require that digital signature technology be used as well as following certain criteria if electronic signatures are used. These features include message integrity, non-repudiation, and user authentication. Non-repudiation is described as the claimed sender cannot later deny generating and sending the message. Other features suggested in the standard to look out for when deciding on a product but are not required include; ability to add attributes, continuity of signature capability, countersignatures capability, independent verifiability, interoperability, multiple signatures, and transportability.

### References

Arthur Andersen "HIPAA Resource Center" URL: **http://www.arthurandersen.com/website.nsf/content/IndustriesHealthcareResourcesHIPAAResourceCtr?OpenDocument**

Beacon Partners "HIPAAcomply" URL: **http://www.hipaacomply.com/**

HIPAA Compliance Beyond Health Care Organizations – A Primer, Koso Peter, May 24, 2001. SANS Institute. URL: **http://www.sans.org/infosecFAQlegal/HIPAA.htm**

HIPAA: What it Means for Privacy and Security, Stanton Meyer, March 3, 2001. SANS Institute. **http://www.sans.org/infosecFAQlegal/HIPAA.htm**

"Report Says HIPAA Privacy Reg Doesn't Offer Much to Internet Users", Ms. Janlori Goldman, Director, Health Privacy Project, Georgetown University. **http://www.hipaadvisory.com/news/2001/1120hpp.htm**

Security and Electronic Signature Standards: Proposed Rule Federal Register, Vol. 63. No. 155 Wednesday August 12, 1998

Standards for Privacy of Individually Identifiable Health Information: Proposed Rule Federal Register, Vol. 64. No. 212, Wednesday, November 3, 1998

The Centers for Medicare & Medicaid Services (CMS) **http://www.hcfa.gov/hipaa/hipaahm.htm**

The National Committee on Vital and Health Statistics Web Site **http://ncvhs.hhs.gov**