GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Enforcement of the Health Insurance Portability and Accountability Act

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b
Option 1
February 24, 2004

Hema Vadodaria, CISSP

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

February 20, 2003 marked a significant day for healthcare providers, clearinghouses, health plans, and employers as it denoted the adoption of the security standards of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. These standards were developed as a reaction to the trend towards a paperless society. Additionally, the law was enacted to enable the electronic exchange of protected health information (PHI) while ensuring its confidentiality, integrity, and availability. As the date for compliance with the security rules approaches, many healthcare organizations are struggling to interpret the regulations and prevent any disclosures of patient information. This document attempts to provide a brief introduction of the final HIPAA security regulations. The enforcing authorities, the manner in which penalties are addressed, and the rights of individuals and covered entities will also be presented. Legal implications of not complying with HIPAA regulations may result in civil or criminal penalties, the details of which are explained below. Finally, this document details the steps that covered entities may take to remain compliant and avoid any unwanted disclosures. It is typically the case that those who are made well aware of the enforcement process are better equipped to abide by the rules. This document intends to provide that level of knowledge.

HIPAA – The Law

The Department of Health and Human Services recognized the trend that healthcare organizations were moving towards a more electronic environment. With this technology, came the increased risk of unauthorized individuals viewing or obtaining patient related information. One purpose of HIPAA requirements "is to improve efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information." HIPAA also strives to set the standards for unique health identifiers for health plans, clearinghouses, and providers. In order to protect the confidentiality, availability, and integrity of individually identifiable health information, the HIPAA Security rules were proposed.

HIPAA Privacy regulations went into effect on April 13, 2003 with an extension of one year for small health plans. October 16, 2003 is approaching quickly as the compliance deadline for the HIPAA Transactions and Code Sets rules. The HIPAA Security regulations were published on February 20, 2003, were finalized on April 21, 2003, and require covered entities to be in compliance on April 21, 2005. Small health plans are allowed an extension of one year and must be in compliance by April 21, 2006[1].

[1] Federal Register, Vol. 68, No. 74 / 45 CFR Part 160 Civil Money Penalties: Procedures for Investigations, Imposition of Penalties, and Hearings; Interim Final Rule, URL: http://www.hhs.gov/ocr/moneypenalties.pdf (April 17, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

One may ask the question, "Do I need to comply with HIPAA?". The answer is not a straightforward one and begs another question, "Do you store or process patient information?". As defined in the HIPAA regulations, the following entities are expected to abide by the standards, requirements, and implementation specifications:

- a health plan;
- a health care clearinghouse;
- a health care provider who transmits any health information in electronic form; or
- a business associate of another covered entity who might create or receive protected health information.[2]

The HIPAA Security Regulations were designed to address three aspects of information security: Administrative, Physical, and Technical. These requirements are components of an all encompassing information security framework. From external access to the facility to the individual passwords entered on kiosk stations, HIPAA establishes requirements so as to minimize the likelihood of an intruder gaining access to protected health information. The Department of Health and Human Services (DHHS) realizes that not every covered entity has the means to implement all of the regulations as a result of various factors: size of covered entity, cost of security mitigations, network architecture constraints, and probability of risk. To accommodate differing environments, HIPAA Security regulations have been labeled as "Required" or "Addressable". A "Required" implementation specification must be implemented. If a standard is "Addressable", the covered entity must determine whether it is feasible to implement it. If not, the entity must thoroughly document why the standard is not reasonable and implement an alternative mitigation strategy.

Administrative

The Administrative safeguards deal with risk management, access management, security awareness and training, incident response, a contingency plan, and third party agreements. These topics have a wide range and have been grouped together as those areas that are the foundation of information security. Security awareness, for example, must be conducted on a routine basis to continuously remind and educate information users of the need to preserve patient information. This would also be the opportunity to train users on the various processes that have been implemented to support the HIPAA regulations. Risk management which includes the classification of data, routine vulnerability assessments, and business continuity planning is vital to the operation of a healthcare organization where patient lives may be at stake.

[2] Federal Register, Vol. 68, No. 74 / 45 CFR Part 160, URL: http://www.hhs.gov/ocr/moneypenalties.pdf (April 17, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Physical

Physical safeguards such as building access controls, hardware and media controls, backup and storage of data and the positioning of display screens are described in depth to ensure that PHI is not vulnerable to the wandering visitor. A commonly overlooked necessity of information security is the shredding of confidential patient related information. Documents simply thrown in a trash can or recycle bin can be easily obtained by the occasional passerby. In spite of all the technical controls implemented within the network, information can still become vulnerable to unauthorized access if the appropriate physical barriers are not in place.

Technical

The Technical safeguards delve deeper into the technical implementations of integrity controls such as encryption and unique user identification. Auditing is specified in more detail for all information systems that contain or use electronic protected health information. An example of a technical safeguard is securing electronic PHI that may be transmitted via e-mail across an unsecured network such as the Internet.

Enforcement

As soon as the HIPAA Security regulations were published, covered entities struggled to understand how non-compliance would be handled. The issue was a result of the vague nature of the implementation specifications. Many organizations were concerned that their inconsistent understanding of the rules may leave them in a position of non-compliance.

A slightly different angle was taken by DHHS with regards to the manner in which compliance would be imposed. The emphasis was placed on a cooperative approach – one that would focus on educating the covered entities, "providing technical assistance, and seeking informal means to resolve disputes"[3]. DHHS is encouraging voluntary compliance from covered entities and is willing to provide guidance with an abundance of documentation that will enable an entity to form corrective action. The Centers for Medicare and Medicaid Services (CMS) and the Office of Civil Rights (OCR) view the HIPAA Enforcement Rule as a chance to secure the manner in which patient information is transmitted or stored electronically rather than as a means of imposing punishments.

HIPAA Privacy rules will be imposed by the OCR while the Centers for Medicare and Medicaid Services (CMS) have been tasked with enforcing the Transaction

[3] Bentivoglio, John T., "HIPAA – Compliance and Enforcement Issues" URL: http://www.ehcca.com/presentations/HIPAA/bentivoglio-mon.pdf (October 2000)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

and Code Sets and Security standards. The OCR and CMS, working under the Department of Health and Human Services, will enforce Civil Penalties. Criminal Penalties, however, will be enforced by the U.S. Department of Justice. The first installment of the Enforcement Rule (Federal Register Volume 68, Number 74), which went into effect on September 16, 2003 addresses procedural aspects related to the administration of penalties. An electronic version of this rule is available at http://www.hhs.gov/ocr/moneypenalties.pdf.

The enforcement process will be initiated primarily by complaints from individuals or organizations. Health and Human Services (HHS) simply does not have the capability to conduct routine audits of all covered entities[4]. Complaints must be filed within 180 days from the date of the incident. Once a complaint has been filed, CMS works with the covered entity to develop a plan that will allow the entity to reach compliance.

Only covered entities are subject to the HIPAA regulations. Therefore, only covered entities can be liable for any penalties. If a complaint is made either online https://www.cms.hhs.gov/hipaa/hipaa2/support/correspondence/complaint/default.asp or via a written statement, CMS will send a letter of notification to the covered entity stating the fine and the reason the entity is in non-compliance. Upon receipt of the notice, the entity has 60 days to request a hearing in writing. If a hearing is not requested, the penalty is made final and the right to appeal it is forfeited.

The request for a hearing must state whether the covered entity admits or repudiates the violation in question. In the latter case, an explanation of the basis for opposing the penalty must also be presented. An Administrative Law Judge who presides over the hearing is required to hold a prehearing conference in order the isolate the issue and expedite the formal hearing process. Soon after, the formal hearing is held with the Secretary and final decisions are made as to the severity of the offense, the state of mind of the covered entity, and the corrective plan of action.

Throughout the judicial process, it is important to understand that the individuals who issue complaints and the covered entities who are accused of non-compliance have certain rights as listed below.

Individuals who have submitted complaints about healthcare organizations are protected in the following manner:

1. Possess the right to file complaints with HHS;
2. Follow the same procedures that are established for civil rights complaints;

[4] Youngstrom, Nina, "HIPAA Compliance Strategies" *Report on Medicare Compliance*, URL: http://www.aishealth.com/Compliance/Hipaa/RMCCarrotandstick.html (April 17, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3. Protected from intimidation, threats, coercion, discrimination, or any other retaliatory action as addressed in the "whistleblower" procedures for the filing of a complaint[5].

Covered entities accused of disclosing protected health information have the following rights:

1. May not be imposed if the criminal penalty provision also applies to the infraction in question;
2. May not be imposed if the entity accused of the penalty was not aware, and by exercising the necessary precautions, may still not have known that the item could be in non-compliance;
3. May not be imposed if the entity liable for the penalty did not purposefully disclose the information. Disclosure of patient information due to a result of willful neglect will be taken into consideration.

The next two sections delve into the details of the various civil and criminal penalties that may be imposed. Regardless of the amount of a fine, covered entities must consider the residual effects of non-compliance such as legal costs or the time and resources necessary to achieve compliance or cooperate with law enforcement representatives. Possibly the most significant cost to an entity would be the negative publicity and potential loss of business.

Civil Penalties

HIPAA has both civil and criminal penalties that range in cost and severity of penalty depending on the violator's state of mind. Civil Money Penalties (CMP) are issued if it is determined that a covered entity or individual did not intentionally disclose protected health information.

If the information was revealed as a result of negligence by the covered entity or an individual offender, a penalty amount of $100 per infraction is incurred with a maximum of $25,000 per calendar year. Negligence, although the Enforcement Rule does not specifically define it, may be defined as not properly locking a shredder bin and accidentally allowing a visitor to recover patient related documents that were meant to be destroyed. If the covered entity or individual offender confesses that he or she was not aware of the violation, and by implementing the necessary precautions still may not have known, CMS may not impose a civil penalty. If the covered entity executed best efforts to implement and comply with HIPAA and an employee still disclosed PHI, the covered entity will not be imposed civil or criminal penalties. If the violation was not due to "willful neglect of the requirements", "the Secretary may reduce the amount of the

[5] Federal Register, Vol. 65, No. 250 / 45 CFR Part 160 Standards for Privacy of Individually Identifiable Health Information; Final Rule, URL: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/privacy/finalrule/PvcFR03.pdf (December 28, 2000)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

fine"[6]. The Secretary may dismiss the fine altogether if the covered entity brings the violation into compliance within thirty days of the notice. The thirty day deadline may be extended if the covered entity (or individual) states a valid case for needing additional time. The above mentioned civil penalties are summarized in the table below:

Circumstances of Violation	Penalty
Negligence	$100/violation not to exceed $25,000 per calendar year
Was not aware and with necessary precautions may still not have known	$0
Reasonable cause and not due to willful neglect	Potential for reduction of fine; Can be waived if violation corrected in 30 days

Criminal Penalties

Criminal penalties can be imposed upon health plans, providers, and health care clearinghouses that knowingly disclose or obtain Individually Identifiable Health Information (IIHI) under illegal circumstances. HIPAA imposes criminal penalties on those individuals who knowingly:

1. Use a unique health identifier for reasons other than direct patient care;
2. Obtain IIHI relating to an individual; or
3. Disclose IIHI to another person or entity.

If a covered entity or individual purposefully discloses protected health information, the penalty is up to $50,000 with a potential jail time of one year. If a covered entity or individual knowingly collects or divulges IIHI when he or she "is not authorized to receive or release such information, but has portrayed otherwise"[7], the penalty is up to $100,000 with a potential jail time of up to five years. If a covered entity intends on soliciting, transferring, or using IIHI for commercial advantage, personal gain, or malicious harm, the penalty is up to $250,000 with a potential jail time of up to ten years.

Whether or not a covered entity or individual had knowledge of the violation is determined by whether the violator had knowledge of the offense. The Department of Justice is only required to show that the entity or individual had knowledge that the violation took place, "not whether the act was wrongful or

[6] HIPAA Academy, "HIPAA Penalties" URL: http://www.hipaaacademy.net/hipaaPenalties.html (2003) (September 27, 2003)
[7] Columbus, Susan, "DHS Privacy Program Statement of Understanding DHS 2091" URL: http://www.dhs.state.or.us/admin/hipaa/doc_priv/docs/penalties.pdf (April 16, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

unlawful"[8]. The above mentioned criminal penalties are summarized in the following table:

Offender's Frame of Mind	Penalty
Knowingly commits violation	up to $50,000 and/or imprisonment up to 1 year
Knowingly commits violation under false pretenses	up to $100,000 and/or imprisonment up to 5 years
Knowingly commits violation with intent to sell, transfer, or use IIHI	up to $250,000 and/or imprisonment up to 10 years[9]

How to Remain Compliant

The question most covered entities seem to be asking themselves is, "What can I do to make sure one of my employees does not accidentally reveal PHI?". The answer is not a clear cut one, but rather in the form of a process. From a Security standpoint, there are several steps that can be taken to achieve compliance over a period of time. A deadline of April 2005 seems far enough away but if steps are not taken today, it will be difficult to achieve compliance.

Before one can decide how to protect PHI, it is necessary to identify every application and system that it resides on. Although the HIPAA Security regulations only apply to electronic PHI, realize that this could even include voice mail systems. This process is part of a larger Risk Analysis in which critical data is identified, potential for loss and disclosure is determined, and necessary security precautions to protect it are agreed upon. Interaction from all areas of the organization is essential in order for this effort to be successful. Upper management should evaluate threats to all of the organization's assets, including "programmatic threats caused by staffing and budgeting shortfalls"[10]. This task may seem rather daunting once the initial phase of a risk analysis is conducted. The following checklist is a good way to begin the process:

1. What is your most valuable information? Where is it located?
2. If revealed or destroyed, what is the financial loss to your organization? Legal implications? Customer loss?
3. What are the potential threats that could compromise your assets (e.g., weather, hackers, power outages)?
4. What is the likelihood that the threats will occur?

[8] Bentivioglio, John T. "HIPAA – Compliance and Enforcement Issues"

[9] San Fernando Valley Community Mental Health Center, Inc., "Overview of HIPAA Compliance Program – April 2003" URL: http://www.sfvcmhc.org/HIPAA/hipaa.html (April 14, 2003)

[10] Hewitt, Clyde and Bill Miaoulis, "Key Security Questions for Healthcare Executives: What to Ask and Answer Before Implementing the HIPAA Security Rule" URL: http://www.hipaadvisory.com/action/security/0603keyques.htm (2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5. Combining the results of questions 1 – 4, what are some reasonable measures that can be taken to protect the information?

An organization wide risk analysis of this type should be conducted once a year as technology can rapidly change in an environment.

Delegate the responsibilities of HIPAA compliance to Privacy and Security Officers. It is essential that these individuals be given enough authority and the ability to dedicate their efforts towards developing a plan of action and ensuring that all areas of the regulations are either implemented or documented with an alternate strategy. The officers will need cooperation from all areas of the organization but they should be able to determine what form of action is required from each department.

Although it is a time consuming event, all covered entities should develop, at a minimum, policies and procedures which address the handling of PHI. Topics can range from auditing of PHI use to sanctions that may be imposed for failure to comply with policy. These policies and procedures should explain how to respond to requests for PHI use and disclosure to other entities, business associates, patients, family members, or unauthorized individuals[11]. It should be made clear within the policies that protected health information is to be accessed by only those individuals who have a need to know.

The weakest link in any organization is typically attributed to the end user. Unintentional disclosures range from not locking a workstation's screen to a physician accidentally sending an e-mail about a patient to the wrong e-mail address. Situations such as these can be addressed through simple awareness techniques. To begin with, all employees should be required to undergo HIPAA training that covers the bases with respect to Privacy, Transactions and Code Sets, and Security regulations. Depending on these employees' positions and responsibilities, they should then undergo training on the regulations as they pertain to their duties. For example, an individual in the Information Technology Department would need to understand that not everyone should have access to a patient management system but only those individuals who require access to do their job. Awareness about HIPAA regulations can also be communicated via posters, periodic quizzes with rewards, messages on the Intranet, or even brief e-mails. An annual training session on the HIPAA regulations is a good way to remind employees of responsibilities and commitment to protecting PHI. It is important that everyone understands what actions they are allowed with regards to patient information as well as the compliance penalties a covered entity or individual may be susceptible to.

Time should be spent with one's attorney to ensure that Business Associate Agreements are well written. Make sure that any organization with whom patient

[11] Wainrib, Ronald E. & Associates, Inc, "New HIPAA Health Care Privacy Rules Pose Legal Traps for Contractor Workforce Management" URL: http://www.contingentlaw.com/new_hipaa_health_care_privacy_ru.htm (2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

information is processed, receives, signs, and abides by the agreement. This is a crucial step to making certain that a covered entity is not held liable for any non-compliance related activities conducted by the business associate.

Although it was mentioned earlier, documentation cannot be stressed enough! As a covered entity is reviewing those areas of non-compliance, it may be determined that HIPAA compliance cannot be achieved with specifications as stated in the regulations. In these cases, it is imperative that these entities document the reason they will not be able to comply, an alternate plan of action, and an expected timeframe as to when this will be accomplished.

Conclusion

The Enforcement Rules issued by Health and Human Services follows the process for civil complaints and, therefore, is nothing new. The second installment of the Enforcement Rule will be much more significant in that it will address substantive requirements for imposing civil penalties[12]. How violations will be determined as well as the methodology for calculating civil money penalties is to be included in the Enforcement Rule. The Privacy regulations are already in effect and the extension date for Transactions and Code Sets is fast approaching. After reading through this document, covered entities should be able to walk away feeling a little less anxious about the legal implications of HIPAA and a little more empowered to achieving compliance. As emphasized in the Enforcement Rule, the Department of Health and Human Services is focused on obtaining voluntary compliance with HIPAA and is not looking for an occasion to impose penalties. It is obvious that covered entities have several opportunities which, if taken, may result in a reduced fine or one that is completely dismissed. The bottom line for all covered entities is that a good faith effort will be recognized and goes a long way.

[12] Miller & Chevalier, "ERISA and Benefits Alert" URL: http://www.millerchevalier.com/db30/cgi-bin/pubs/Benefits%20Alert%20-%20April%202003%20[HIPAA%20Enforcement%20Regulations].pdf (April 17, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

1. Federal Register, Vol. 68, No. 74 / 45 CFR Part 160 Civil Money Penalties: Procedures for Investigations, Imposition of Penalties, and Hearings; Interim Final Rule, URL: http://www.hhs.gov/ocr/moneypenalties.pdf (April 17, 2003)

2. Bentivoglio, John T., "HIPAA – Compliance and Enforcement Issues" URL: http://www.ehcca.com/presentations/HIPAA/bentivoglio-mon.pdf (October 2000)

3. Youngstrom, Nina, "HIPAA Compliance Strategies" *Report on Medicare Compliance*, URL: http://www.aishealth.com/Compliance/Hipaa/RMCCarrotandstick.html (April 17, 2003)

4. Federal Register, Vol. 65, No. 250 / 45 CFR Part 160 Standards for Privacy of Individually Identifiable Health Information; Final Rule, URL: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/privacy/finalrule/PvcFR03.pdf (December 28, 2000)

5. HIPAA Academy, "HIPAA Penalties" URL: http://www.hipaaacademy.net/hipaaPenalties.html (September 27, 2003)

6. Columbus, Susan, "DHS Privacy Program Statement of Understanding DHS 2091" URL: http://www.dhs.state.or.us/admin/hipaa/doc_priv/docs/penalties.pdf (April 16, 2003)

7. San Fernando Valley Community Mental Health Center, Inc., "Overview of HIPAA Compliance Program – April 2003" URL: http://www.sfvcmhc.org/HIPAA/hipaa.html (April 14, 2003)

8. Hewitt, Clyde and Bill Miaoulis, "Key Security Questions for Healthcare Executives: What to Ask and Answer Before Implementing the HIPAA Security Rule" URL: http://www.hipaadvisory.com/action/security/0603keyques.htm (2003)

9. Wainrib, Ronald E. & Associates, Inc, "New HIPAA Health Care Privacy Rules Pose Legal Traps for Contractor Workforce Management" URL: http://www.contingentlaw.com/new_hipaa_health_care_privacy_ru.htm (2003)

10. Miller & Chevalier, "ERISA and Benefits Alert" URL: http://www.millerchevalier.com/db30/cgi-bin/pubs/Benefits%20Alert%20-%20April%202003%20[HIPAA%20Enforcement%20Regulations].pdf (April 17, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.