# Global Information Assurance Certification Paper

Miles Edmundson

GSEC Practical
Version v.1.4b

March 15, 2003

# HIPAA Final Rule Overview and Sample Case Study

ABSTRACT:

In 1996, the US Congress passed one of the most sweeping laws pertaining to the health industry in our nation's history. The Health Insurance Portability and Accountability Act (HIPAA) deals with two primary areas. Title 1 addresses the issue of health insurance coverage and portability (continuity of health insurance for individuals as they change jobs) and rules for handling pre-existing conditions.[1] Title 2, Preventing Health Care Fraud and Abuse, Administration Simplification and Medical Liability Reform section, addresses the issues of accountability, waste and fraud reduction. The US General Accounting Office has estimated that 11% of health care dollars are spent fraudulently.[2] Clearly, the government is hoping, through standardization of coding and procedures, as well as through accountability standards, to greatly reduce waste and fraud within the health care industry. This is especially significant in lieu of the billions of tax dollars funneling through Medicare and Medicaid.

Another objective of HIPAA is to establish standards for the maintenance and transmission of patient health information (PHI).[3] The act points out that currently, there are no standards to protect PHI during electronic storage and transfer. The purpose of this paper is to examine the details of Title 2 (specifically subpart C of Part 164: PHI data privacy and security) and then consider how the act applies in a common medical scenario. This is a very relevant topic because the HIPAA final rule was just released February 20th, 2003. The final rule will become effective on April 21, 2003. And, most health care organizations have until April 21, 2005 to comply. The next two years will be a challenge for those organizations that are not prepared to address PHI confidentiality, integrity, and security.

Over the last few years as HIPAA was being formed, there has been great concern over the costs and technical requirements. But surprisingly, there is nothing unusual or shocking in the Act from a technology perspective. The Act doesn't mandate any specific technology (for example, encryption) and sets only best practices that, for the most part, have been in use by many businesses and industries for some time. In fact, the Act clearly states that the specific technology used by each entity is a specific business decision.[4] This is not unlike other regulated industries. The banking industry is perhaps the best example. Banks

and credit unions have enacted and practiced many of the Acts general requirements for years.

An excellent summary of this section can be found in the following tables. The right-most column specifies whether the item is required (R) or is addressable (A), meaning that the health care entity has some leeway as to whether or not it needs to implement the specific line item. However, the health care entity MUST document why it is not taking an action on an addressable event.

Let's briefly examine the significant points of each section.

## ADMINISTRATIVE SAFEGUARDS

| Standards | Sections | Implementation Specifications (R)= Required, (A)=Addressable | |
|---|---|---|---|
| Security Management Process | 164.308(a)(1) | Risk Analysis | (R) |
| | | Risk Management | (R) |
| | | Sanction Policy | (R) |
| | | Information System Activity Review | (R) |
| Assigned Security Responsibility | 164.308(a)(2) | | (R) |
| Workforce Security | 164.308(a)(3) | Authorization and/or Supervision | (A) |
| | | Workforce Clearance Procedure | (A) |
| | | Termination Procedures | (A) |
| Information Access Management | 164.308(a)(4) | Isolating Health care Clearinghouse Function | (R) |
| | | Access Authorization | (A) |
| | | Access Establishment and Modification | (A) |
| Security Awareness and Training | 164.308(a)(5) | Security Reminders | (A) |
| | | Protection from Malicious Software | (A) |
| | | Log-in Monitoring | (A) |
| | | Password Management | (A) |
| Security Incident Procedures | 164.308(a)(6) | Response and Reporting | (R) |
| Contingency Plan | 164.308(a)(7) | Data Backup Plan | (R) |
| | | Disaster Recovery Plan | (R) |
| | | Emergency Mode Operation Plan | (R) |
| | | Testing and Revision Procedure | (A) |
| | | Applications and Data Criticality Analysis | (A) |
| Evaluation | 164.308(a)(8) | | (R) |
| Business Associate Contracts and Other Arrangement | 164.308(b)(1) | Written Contract or Other Arrangement | (R) |

## 287 PHYSICAL SAFEGUARDS

| Standards | Sections | Implementation Specifications (R)= Required, (A)=Addressable | |
|---|---|---|---|
| Facility Access Controls | 164.310(a)(1) | Contingency Operations | (A) |
| | | Facility Security Plan | (A) |
| | | Access Control and Validation Procedures | (A) |
| | | Maintenance Records | (A) |
| Workstation Use | 164.310(b) | | (R) |
| Workstation Security | 164.310(c) | | (R) |
| Device and Media Controls | 164.310(d)(1) | Disposal | (R) |
| | | Media Re-use | (R) |
| | | Accountability | (A) |
| | | Data Backup and Storage | (A) |

## TECHNICAL SAFEGUARDS (see § 164.312)

| Standards | Sections | Implementation Specifications (R)= Required, (A)=Addressable | |
|---|---|---|---|
| Access Control | 164.312(a)(1) | Unique User Identification | (R) |
| | | Emergency Access Procedure | (R) |
| | | Automatic Logoff | (A) |
| | | Encryption and Decryption | (A) |
| Audit Controls | 164.312(b) | | (R) |
| Integrity | 164.312(c)(1) | Mechanism to Authenticate Electronic Protected Health Information | (A) |
| Person or Entity Authentication | 164.312(d) | | (R) |
| Transmission Security | 164.312(e)(1) | Integrity Controls | (A) |
| | | Encryption | (A) |

5

ADMINISTRATIVE SAFEGUARDS: Section 164.308

Approximately 50% of the safeguards in the Act apply to management and administration responsibilities. The purpose of this section is to propose a formal, security management process to create, administrate, and oversee policies that cover the entire range of security issues as well as ensure prevention, detection, containment, and correction of security violations.[6] This is, in fact, the function of management.

As a foundation for all PHI safeguards, management must first authorize and conduct a Risk Analysis. The procedures to conduct a Risk Analysis are beyond the scope of this paper. There are a number of publications available to assist health care entities with this process. It is significant to note that entities have their choice in whether to conduct a quantitative or qualitative analysis. The National Institute of Standards and Technology has published an excellent nine step procedure for conducting a Risk Analysis.[7] Further, the CISSP courseware goes into detail with methodologies for conducting both a quantitative and qualitative analysis.[8] The objective of all of these methods is to identify the risks, within a given institution, to patient health information (PHI) and to form the foundation for protecting the confidentiality, integrity, and availability of that PHI.

Following the analysis, management must document the steps taken to transfer, mitigate, or assume each specific risk as well as provide a procedure detailing sanctions for employees that fail to follow PHI security policies, and provide a means for system activity review. [9] Again, there is nothing new to general management in this statute. It is a common practice of management to identify risk and then, seek to minimize it. The “means for system activity review” is new language in the Final Rule that replaced specific language about audits. There is no stipulation that this activity must be conducted by an independent third party. However, there is clear evidence that a thorough review of logs, file access, security incidences, and policies and procedures etc. must be maintained and

examined in a regular, scheduled process. Again, there is no surprise with this mandate. Both internal and external audits have been, and continue to be, a regular feature of business. The purpose of such audits (especially internal audits) is to make the organization stronger and less vulnerable to losses due to fraud, waste, and error. In this case, it also helps the organization better protect PHI and avoid potential civil action should PHI be compromised.

Also included in this section is a requirement to have a detailed plan and response to any security incidences, a data backup plan, disaster recovery plan, and an emergency mode operation plan. Once again, there is nothing shocking about these requirements. Clearly, for an industry as crucial to the well-being of a nation (not unlike the banking and finance industry), management should be prepared to ensure the confidentiality, integrity, and availability of PHI. If there are mistakes in how this information is handled, lives can be lost. There are numerous instances in the news today about medical mistakes that cost lives. Section 164.308 attempts to implement management controls to minimize the potential for errors with PHI.

While there are a number of addressable items in this section, two items standout as critical. First, the Act requires isolating health care clearinghouse functions from other parent and sister entities. This will necessarily involve electronic controls for access and authorization to PHI. Management should strongly consider formal, documented policies and procedures defining levels of access for all personnel who have access to PHI.

Second, the Act raises the issue of Security Awareness and Training for employees. This training would be required for all staff and management and would address ongoing issues pertinent for employees in that specific location. For example, security awareness training could involve security reminders, virus protection, password management, policies and procedures review, and even an examination of HIPAA history, rationale, and requirements. During the dialogue phase prior to the final rule, one commenter argued that security awareness training for all system users would be too difficult to do in a large organization. The response is telling,

> "We disagree with the commenter. Security awareness training is a critical activity, regardless of the organizations size. This feature would typically become part of an entity's overall training program, (which would include privacy and other information technology items as well). For example, the Government Information Systems Reform ACT (GISRA) of 2000 requires security awareness training as part of Federal agencies' information security programs, including Federal covered entities, such as the Medicare program. In addition, National Institute of Standards and Technology (NISP) SP 800-16, "Information Technology Security Training Requirements, A Role and Performance Base Model", April 1998,

provides an excellent source of information and guidance on this subject and is targeted at industry as well as government activities." [10]

Clearly, organizations should plan on providing some aspect of security continuing education to employees.

PHYSICAL SAFEGUARDS: Section 164.310

Physical safeguards include four mandatory and six addressable requirements. Two of the mandatory requirements will be encountered on a daily basis. These two requirements pertain to employee workstations: 1) Workstation Use and 2) Workstation Security.

Workstation use involves policies and procedures specifying the operations that should be performed on each workstation and how those operations should be performed.

Workstation security will address questions of how to block unauthorized access to the workstation as well as the information which may be visible on the workstation monitor. Remembering that the overall objective is to protect the confidentiality, integrity, and availability of PHI, simple procedures, such as: physical locks on workstations, screen saver passwords, software locks, proximity tokens (for some high profile areas) and visual shields that limit viewing of the information unless positioned directly in front of the monitor, may be used. Proximity tokens provide the ability to automatically log an employee off a system if they are more than some specified distance from the workstation. This is an interesting option for physicians or nurses that log into multiple workstations in examination rooms when seeing patients. In addition, it is a potential option for employees that consistently forget to log off their systems and walk away for breaks or at the end of a day.

The two remaining required standards apply to the disposal and re-use of electronic media. It is widely known that data often remains on electronic media after it has been disposed. In January, 2002, two researchers purchased 158 used disk drives through Internet and at swap meets. The total expenditure for these drives was less than $1,000. They found more than 5,000 credit card numbers, medical reports, and other detailed personal and corporate financial information.[11] The market for used hard drives is growing. And, literally thousands of patient records could become compromised if hard disks are not disposed of properly. Section 164.310(d)(1) mandates that electronic media is rendered non-readable, or electronically wiped prior to disposal. Mechanisms for performing this include:

- Physically destroying the drive. Grinding, pulverize, shred, melt, etc.
- Degaussing the drive (randomizing the magnetic domains) with a Type 1 or Type 2 Degausser (often rendering the drive totally unusable)
- Over-writing the drive multiple times with random patterns of 0's and 1's.

The article by Garfinkle and Shelat goes into great detail about various commercial and free software that is available for this task.

Depending upon which hard disks are disposed of, and how often this occurs, detailed records may need to be maintained showing which hard drives were disposed of (or swapped and re-used) and how they were rendered unreadable. Again, beyond a simple physical task is a management record keeping requirement.

Finally, this section raises the issue of physical access to the premises. This is an addressable issue, depending upon the size and complexity of the organization. While this may not take on a "technology" bent, building access and security is often tied to electronic access cards. Such cards eliminate the need for keys (which can be copied) and can leave an audit trail showing who accessed specific areas at specific times.

TECHNICAL SAFEGUARDS

Section 164.312 includes four mandatory and five addressable requirements. The red thread running through the four mandatory requirements all pertain to unique employee ID's and the auditing of each persons access to PHI. Access control will require a unique user identification mechanism to track employee access to system resources and data. This requirement extends to emergency procedures so that PHI can be accessed and medical care given, during non-normal conditions.

Keeping in mind the overall requirements of PHI confidentiality, integrity, and availability, auditing is required to ensure that PHI has not been modified or destroyed in any non-authorized manner (integrity check). The final rule includes "hardware, software, and procedural mechanisms that can record and examine activity in information systems."[12]

Interestingly, earlier provisions of the Act mandated that "Person or Entity Authentication" (164.312(d) required either a 1) "biometric identification system; 2) a "password" system; 3) a personal identification number; or 4) a "telephone callback" or "token" system that uses a physical device for user identification.[13] The final rule omits these specific options and simply refers to a general requirement for person or entity authentication.

Finally, it is also interesting to note that encryption is an addressable issue. Depending upon the data involved, it may be prudent for medical institutions to begin encrypting PHI. In either case, medical institutions will be required to document why they are, or are not, encrypting specific PHI. It seems difficult to believe that encryption will not be a requirement if medical institutions begin transferring PHI over the internet. Public key technology has become much more common and is used in a growing number of business applications. Further, encryption of patient health information in the database may be considered as another "defense-in-depth" approach. Since encryption technology is becoming more common place, it seems reasonable to add such a layer of protection should someone gain unauthorized access to the patient database. Encrypted data "at-rest" would have prevented the hackers from using the credit card numbers that were recently stolen from a credit card processing center. It is reasonable to assume that, should PHI be compromised and stolen, lawsuits will focus on the health care entities negligence for failing to use available technology to protect data.

## HEALTH CARE SCENARIO

Given this brief overview of the final rule of the Administrative Simplification section of HIPAA, a single question needs to be asked, "What does this mean to a health care entity?" To assist with answering that question, a common medical scenario should be examined and understood.[14]

### STEP 1: INTAKE:

Patient M (PM) walks into an emergency room. During the registration process (intake), a nurse takes PM's name, social security number, address, insurance information, physician name, presenting problem, and other information. This information is usually recorded on a computer system. In addition, paper forms are also filled out, often as part of an interview process, requesting past medical history, current meds being taken, allergies, insurance information, etc. Often, this setting is in an open room (a waiting room), or a smaller room with more than one station for intake. The sign-in process is generally very public. At this point, the ER physician knows only what the patient has told him/her and what is recorded on the forms.

### STEP 2: NURSE INTERVIEW

Once PM has been called back into the ER, a nurse conducts a more in-depth interview and will ask more detailed questions about PM's medical history, including family history for various bio-systems. All these records are kept in a "chart rack" in the ER. This is simply a means of organizing the charts in some chronological order so that patients can be seen in turn. The chart rack contains a clipboard with all the paperwork from the intake and nurse interviews. This chart rack is available to any hospital employee who walks into that area. In a physicians office visit, the chart rack is often just a wood or metal bracket on the

wall outside the examination room. In this case, these medical records are within easy reach of any person walking through the halls.

STEP 3: PHYSICIAN EXAM

The physician will review the paperwork, interview and examine the patient. Following this, the physician will write orders for tests and meds. These orders are then copied to a hospital specific standardized form (not all hospitals use the same forms) by a nurse. All this is usually done in an open setting with many medical personnel and patients within hearing distance. To assist with this inefficiency, many hospitals have implemented "Computer Physician Order Entry" systems (CPOE) that enable the physician to order medical procedures through a computer process. The problem with this system is that physicians are generally not good typists. Further, they often believe their time is better spent seeing patients rather than typing test orders. This continues to be a major contentious issue in medical circles.

ADMITTANCE TO THE HOSPITAL:

Should the physician determine that PM needs to be admitted, another paper form is completed. This form outlines the following information:

- Admit (to what floor)
- Diagnosis
- Condition
- Diet
- IV orders
- Allergies
- Medications
- Diagnostics (tests ordered)

Within 24 hours of admittance, a new history is taken, a physical should be performed, and all medical data should be dictated by the physician and transcribed. Some hospitals use a third party transcription service and others perform this service, "in-house".

In addition, many health insurance companies require that hospitals notify them within 24 hours of admittance to the hospital in order to ascertain whether the illness and treatment meets insurance coverage criteria. These records are generally faxed to the insurance company shortly after admittance to the hospital. Should the physician require "out-patient" records (medical records from the primary care physician) they are requested and generally faxed, mailed or couriered to the hospital.

DISCHARGE FROM THE HOSPTIAL

When PM is discharged from the hospital, discharge orders are prepared and issued by the physician. These usually consist of a physician's summary of the

illness, treatment, disposition, follow-up care and prescriptions. The orders are copied to hospital forms by a nurse. If the orders are for sub-acute care (such as a nursing home) there are additional forms to fill out for Medicare/Medicaid. Because few hospitals do concurrent coding, billing for the hospital stay occurs after the patient is discharged. PM's medical records are submitted to the finance department where highly trained employees convert the treatment to accounting codes. These are not medically trained employees. Most commonly, this process is done "in-house". In addition, many insurance companies have a case manager on site at a hospital. This person may request copies of medical records at any time.

SCENARIO REVIEW

What is surprising in this realistic example is the lack of technology in common and frequent data handling. To be fair, the act does NOT require ANY technology. What it does require is that in ANY system, PHI is protected. Let us consider the more paper based system. While there is no need for a technological "back-up" of patient records that reside in paper files. There is also NO back-up of that data. If it is lost due to fire or flooding, the patient records are permanently gone. Further, management will continue to spend dollars for expensive storage space and personnel to manage the medical records. It seems OBVIOUS that a superior solution is to scan those records into a database where they can be quickly accessed by medical personnel and emailed (in an encrypted form) to a physician in an emergency room. Such information can also be readily indexed so that a physician can spend less time reviewing records and more time looking for specific facts.

Even the simple action of patient intake, in a non-technology environment, may need to change. While screen visors can be added to workstations so that the information on the screen is not visible to anyone except those directly in front of the monitor, they serve little purpose if the intake is done verbally in an open setting. Some have expressed concern that the simple action of having patients sign-in and then calling their names may be a violation of the HIPAA privacy concerns. Clearly there are number of concerns about what may be an acceptable intake process. The Department of Health and Human Services has stated that the action of having a sign-in list and calling a patients name does not violate patient confidentiality.[15]

Consider the inner sanctum of the emergency room. While the Department of Health and Human Services has clarified that it is an acceptable procedure for medical professionals to consult with one another regarding a patient, [16] physicians may still need to reconsider conversations "in the open" with other medical personnel if they can be overheard by other patients. The key issue is PHI confidentiality and the risk of it being compromised. Even the storage of patient charts "in the open" may need to change. It is easy to perceive of a

technology solution that calls up a patient's intake information on a screen in the privacy of an exam room. The physician will simply need to log into the system, with a unique user id and password, to examine the information and, if necessary, add his/her own notes for tests, diagnosis, orders, etc. Such a system provides better confidentiality, availability, and integrity (fewer handwriting interpretation errors) than a manual system. Various forms of this already exist in the market place. Health care management is beginning to see the value of an investment in this technology. However, there is still resistance from physicians. Many are not good typists and perceive this as doing 'support" work rather than practicing medicine. As a bonus to this system, it seems rational to suppose that medical care accounting codes could be built-in so that accounting personnel (coders) would not be required to review confidential PHI. These are MAJOR changes to an industry. It is worth-while to note that ANY major change to a business is a culture change. And, culture changes are often difficult and painful to accomplish.

With a paper-based system, it seems difficult to validate that only those personnel who have an immediate need to view PHI actually have access to it. PHI confidentiality is problematical in a number of areas within the existing system. However, confidentiality extends beyond the health care entity to other primary care facilities and insurance companies. It seems clear that the current reliance on fax machines to send medical records and forms will need to change. While there is nothing "wrong" with fax machine technology, fax machines will need to be in controlled room and have a control access mechanism, potentially with auditing capabilities. Questions will need to be answered regarding cleaning crew access to these rooms.

SUMMARY

This paper sought to review the significant aspects of the final rule for Administrative Simplification of HIPAA and to apply those rules to a common setting in today's hospitals. While HIPAA does not require anything shockingly new from a technology perspective, it does force the health industry to become more attentive to basic industry technology best practices. In the existing common scenario, there are a number of business inefficiencies and potential violations of HIPAA requirements. Clearly, the movement to a more technologically advanced record keeping and access system has the potential to address the business inefficiencies and HIPAA concerns of PHI confidentiality, integrity, and availability. And, even more clearly, the health care industry is facing a large challenge to how it has traditionally done business. Common practices will need to be reviewed to determine whether they violate or can be improved to better protect PHI. And, no matter what the technology situation in any organization, technology will continue to become more powerful, helpful, and less expensive, offering solutions to privacy and efficiency. However even if the health care entity chooses to maintain its existing technology systems, industry best practices will need to be addressed. The acid test of any system, paper or technology, is "how does it protect PHI?"

## ENDNOTES:

[1] Dallas/Fort Worth Hospital Council. HIPAA Collaborative Resources. "History and Overview of HIPAA"; http://www.dfwhc.org/hipaa/history.htm
[2] Dallas/Fort Worth Hospital Council. HIPAA Collaborative Resources. "History and Overview of HIPAA"; http://www.dfwhc.org/hipaa/history.htm
[3]Final Rule; Department of Health and Human Services, 45 Center for Medicare and Medicaid Services (CMS); CMS-0049-F RIN 0938-AI57, pp 3-4. http://www.cms.hhs.gov/regulations/hipaa/cms0003-5/0049f-econ-ofr-2-12-03.pdf
[4] Final Rule; Department of Health and Human Services, 45 Center for Medicare and Medicaid Services (CMS); CMS-0049-F, RIN 0938-A157, p.46. http://www.cms.hhs.gov/regulations/hipaa/cms0003-5/0049f-econ-ofr-2-12-03.pdf
[5] Phoenix Health Care Systems. Security Standards Matrix: http://www.hipaadvisory.com/regs/finalsecurity/regulationtext.htm#appendix
[6] Final Rule, Department of Health and Human Services; 45 Center for Medicare and Medicaid Services (CMS), CMS-0049-F RIN 0938-AI57; Section 164.308 (a) (1) (i) p. 77 http://www.cms.hhs.gov/regulations/hipaa/cms0003-5/0049f-econ-ofr-2-12-03.pdf
[7] Stonebumer, Gary, Goguen, Alice, and Feringa, Alexis. Risk Management Guide for Information Technology Systems, Special Publication 800-30. NIST. October 2001
[8] Harris, Shon, All-in-One CISSP Certification Exam Guide, McGraw-Hill/Osborne 2002. pp 72-91
[9] Bricker and Eckler LLP: Final HIPAA Security Regulations: Administrative Safeguards, 2003, http://www.bricker.com/attserv/practice/hcare/hipaa/164.308.asp
[10] Bricker and Eckler LLP: Final HIPAA Security Regulations: Administrative Safeguards, 2003, http://www.bricker.com/attserv/practice/hcare/hipaa/164.308.asp
[11] Garfinkle, Shelat, "Remembrance of Data Passed, A Study of Disk Sanitation Practices", IEEE Security and Privacy, January/February 2003.V 1 no. 1.
[12] Brinkler and Echler LLP: Final HIPAA Security Regulations: Technical Safeguards, 2003 http://www.bricker.com/attserv/practice/hcare/hipaa/164.312.asp
[13] Brinkler and Echler LLP: Final HIPAA Security Regulations: Technical Safeguards, 2003 http://www.bricker.com/attserv/practice/hcare/hipaa/164.312.asp
[14] Edmundson, Ross Dr., Medical Director Health Care Management, Florida Hospital, (March 3, 2003), Ross@edmundson.net Typical Emergency Room and Hospital Procedures, Email, M. Edmundson. Miles.edmundson@msn.com
[15] Department of Health and Human Services. April, 2002. HIPAA Privacy Quiz http://www.regreform.hhs.gov/HIPAAQUIZ_0204171/sld007.htm
[16] Department of Health and Human Services, April, 2002, HIPAA Privacy Quiz http://www.regreform.hhs.gov/HIPAAQUIZ_0204171/sld002.htm