Global Information Assurance Certification Paper

Risk Management in the HIPAA Environment

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

Clifford G. Hanks

Risk Management in the HIPAA Environment

Clifford G. Hanks, MCSE, MCP+I, CNA, GGSC
January 14, 2002

Overview

Information Security is receiving new emphasis in hospitals across the nation, largely due to legislation passed in 1996 known as the Health Insurance Portability and Accountability Act (HIPAA). This legislation does not require specific information security measures as much as it requires documented review, selection, and certification of security practices that are appropriate for each individual healthcare entity. But what is appropriate for a specific healthcare provider and what methodology can be used to make and justify the required decisions? The answer, obviously, must take into consideration what the legislation (HIPAA) requires and those requirements include risk analysis and risk management.

The purpose of this paper is to develop a possible method for making and documenting information security decisions, by HIPAA concerned entities, using risk management methods, tailored to meet HIPAA requirements. The HIPAA requirements will be reviewed first followed by risk analysis procedures, encompassing a more detailed look at the HIPAA requirements, and finally a look at risk management in the HIPAA environment.

HIPAA

On August 21, 1996, the 104th Congress of the United States enacted the Health Insurance Portability and Accountability Act (HIPAA). There are two basic sections of the Act, Title I, Portability and Title II, Administrative Simplification.

The intent of Title I of HIPAA is to protect the health insurance coverage of individuals when they change employment status, to improve access and quality of healthcare, and to combat waste and fraud.[1] It was realized that this would require maintaining and exchanging huge amounts of electronic data between many healthcare entities and require converting these records to and from many formats because there was no common electronic data interchange (EDI) standard in use by all the affected organizations. Without a common standard, this would be a very tedious, expensive, and time-consuming task, prone to errors and mistakes. To facilitate EDI, HIPAA Title II, Administrative Simplification, requires the use of standard medical code sets and transaction standards by all health care entities, when transmitting, handling and storing protected/patient health information (PHI). The transaction rule that requires the use of standard code sets has been published and compliance was required as

of October 16, 2002. This is the section of HIPAA most people in healthcare information systems are talking about when they mention HIPAA.

Two additional goals of HIPAA are to protect the insurability and the privacy of the individual. This is addressed in the Privacy Standard, Section 164 and the HIPAA Security Standard, Section 142.308 of HIPAA, Title II.

The Privacy Standard spells out what data is protected and what is required of healthcare workers and businesses, prior to releasing protected information. Compliance with this rule is required as of April 14, 2003 and this is the section of HIPAA most healthcare workers, nurses and doctors are talking about when they mention HIPAA.

Proposed Security Standards rules where published in August 1998 by the Department of Health and Human Services (HHS)[2] and the final rules are yet to be published. This is the section of HIPAA that most information technology workers are talking about when they discuss HIPAA.

The Security Standard mandates that all HIPAA designated entities must: "…assess potential risks and vulnerabilities to the individual health data in its possession and develop, implement, and maintain appropriate security measures."[3] It goes on to say that these measures must include:

a) Administrative Procedures
b) Physical Safeguards
c) Technical Security Services
d) Technical Security Mechanisms

Section 142.308(a), Administrative Procedures, deals largely with establishing policies. This section covers several specific policies, plans and procedures dealing with good information security but subsection (10) gets right to the reason for information security and our subject, Risk Management. Section 142.308(a)(10) Security management process, states, in part:

> (10) Security management process (creation, administration, and oversight of policies to ensure the prevention, detection, containment, and correction of security breaches involving risk analysis and risk management). It includes the establishment of accountability, management controls (policies and education), electronic controls, physical security, and penalties for the abuse and misuse of its assets (both physical and electronic) that includes all of the following implementation features:
>
> (i) Risk analysis, a process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place.
>
> (ii) Risk management (process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk).

This subsection goes on to require disciplinary policies which it calls "sanction policies" and requires an overall security policy/statement for the organization, but, the main point is, as seen above, both risk analysis and risk management are specifically required by HIPAA legislation for all affected organizations.

Risk Analysis in the HIPAA environment

What is Risk Analysis? According to the Society for Risk Analysis, it is:

> A detailed examination including risk assessment, risk evaluation, and risk management alternatives, performed to understand the nature of unwanted, negative consequences to human life, health, property, or the environment.[4]

HIPAA requires risk analysis but doesn't stipulate whether the process is to be performed quantitatively or qualitatively. To perform a quantitative risk assessment, the analyst must determine a monetary value of each asset; a task not readily addressed when the asset is PHI. The benefit of quantitative analysis is the ability to perform a cost-benefit analysis in the monetary language easily understood by management.

In either case, risk assessment is the first step of risk management.[5] The National Institute of Standards and Technology (NIST) Special Publication 800-30, Risk Management Guide for Information Technology Systems has a very well developed risk assessment methodology that contains nine primary steps. Let's review those nine steps and consider the implications of HIPAA and the HIPAA environment.

Step 1 is system characterization. Most risk assessment methods start with a list of assets and the asset's value (AV) but the NIST methodology first addresses the fact that the entire IT system requires protection for the organization to continue performing its mission. The first step is to define the entire organization's IT system, its boundaries and the organization's mission and then list all the assets within that scope. Assets include the normal areas of hardware, software, and data, but NIST suggest the inclusion of interfaces, personnel, information in transit, and information in storage. Also suggested is defining the purpose and the current risk controls in place on each asset.

In a HIPAA or healthcare related organization, each asset is either PHI (Protected/Patient Health Information) or non-PHI and must be classified correctly for proper consideration. HIPAA mandates what is PHI and HIPAA requirements apply solely to PHI.

Step 2 is threat identification. All applicable threats to the organization's IT system and mission should be considered. Natural threats, man-made threats, and environmental threats are common categories to consider and the man-made or human threat should include both intentional and accidental events.

In the past, many healthcare facilities have considered themselves exempt from hackers due to the nature of the data and the lack of motivation for hackers but that all changed in the summer of 2000, when the University of Washington Medical Center was hacked by a self proclaimed security consultant "as a renegade public service aimed at exposing the poor security surrounding medical information".[6]

Step 3 is vulnerability identification. Before any possible threat can cause damage to the system under study, there must be some system vulnerability that can be exploited by the threat whether the threat is human or not. In this phase, vulnerabilities to the system and assets developed in

step 1 are identified for each threat listed in step 2, forming threat-vulnerability pairs. Each threat-vulnerability pair is a potential risk.

Vulnerability scanners like Nmap or ISS can also be used to scan for actual, known vulnerabilities and included in the risk analysis. Additional sources for known vulnerabilities are available via online vulnerability lists like the NIST ICAT vulnerability database[7] and the SANS/FBI Top 20 List.[8]

In addition, review of the organization's computer technical support history could provide clues for identifying the most common vulnerabilities to consider. In the healthcare industry, training emphasis has been historically on practitioner and healthcare related training and vulnerabilities resulting from lack of basic computer skills and computer training of personnel could be some of the most prevalent.

Step 4 is control analysis or identification of current risk controls in place. The threat-vulnerability pairs resulting from steps 2 and 3 can be mitigated by technical or administrative controls. In this step, current and planned system controls effecting each threat-vulnerability pair are to be listed and evaluated, including the estimated costs and effectiveness of current and planned controls. Quantitative analysis could show later, that a current control is not cost effective or less cost effective than a different or newer technology option.

The HIPAA Security Standard, Section 142.308, requires that adequate physical and technical controls be used to protect stored and transmitted PHI under specified conditions, such as encryption of data transmitted over public networks. Also, the entire sub-section (a) of 142.308 mandates administrative procedures and controls that will have to be in place prior to the security rule deadline.

Step 5 is determining the likelihood of each risk event's occurrence. Some threat-vulnerability pairs are more likely to occur than other pairs and should be given higher consideration if the resulting impact is also high. Each threat-vulnerability pair needs to be evaluated, considering factors such as threat motivation and ease of exploitation. The likelihood or annualized rate of occurrence (ARO) of some events, especially naturally occurring events, may be available from actuarial records or online databases like the CERT Coordination Center (CERT/CC)[9] and can be specified quantitatively. The alternative is to estimate the ARO or qualitatively classify each threat-vulnerability pair using some rating scale such as "Low, Medium, or High."

Step 6 is impact analysis, the evaluation of the impact to the organization if each of the listed events where to occur. Certain threat-vulnerability events will have a greater impact on the organizational mission than other events, and will need to be addressed sooner than lower impact events, if likely to occur. Impact is often rated qualitatively, using a similar rating scale such as "Low, Medium, or High." A quantitative approach requires assigning a value to the impact or exposure factor (EF) representing percentage loss per event if the event were to occur.

In the HIPAA environment, the loss of data integrity or availability could adversely effect quality of healthcare and even life. Appropriate consideration of all such possible events identified is definitely required. Reviews for additional threat-vulnerabilities that could have such a high impact should be frequently accomplished.

Step 7 is risk determination.

Mathematically stated the risk or annualized loss expectancy (ALE) is the product of the single loss expectancy (SLE) and the annualized rate of occurrence (ARO) or

ALE ($/year) = SLE ($/event) * ARO (events/year)[10]

Where SLE is found by the product of the assets value (AV) and the impact of the threat-vulnerability event or exposure factor (EF).

SLE ($/event) = AV ($) * EF (% loss/event)[11]

This would result in a quantitative risk assessment and the deliverable should contain columns such as Asset Description, Purpose, Location, Asset Value, Threat-Vulnerability Pairs, Annualized Rate of Occurrence, Exposure Factor, and resulting ALE.

In the HIPAA environment, quantitative assignment of a value for patient health information (PHI) seems to trivialize the mission of healthcare and conversely, may tend to inflate the value of data that, in most cases, isn't of any real value to anyone other than the patient and the patient's care-givers. For these reasons and the additional time and effort required to complete a quantitative analysis, the qualitative approach may often be preferred in healthcare. The final qualitative risk assessment would include assignment of a qualitative risk level based on qualitative threat likelihood and impact ratings using a matrix similar to the example in Table 1, below.

Risk Matrix Table	Low Impact	Med Impact	High Impact
High Likelihood	Medium	High	Very High
Med Likelihood	Low	Medium	High
Low Likelihood	Very Low	Low	Medium

Table 1, Sample Qualitative Risk Assessment Matrix

Step 8 is additional control recommendations. This step is the research, evaluation and recommendation of additional methods to reduce the risks challenging the organization. To be effective, risk mitigation controls must reduce the threat, the vulnerability or both.

HIPAA lists security control requirements in four basic groups.

(a.) Administrative procedures
(b.) Physical safeguards
(c.) Technical security services
(d.) Technical security mechanisms

Administrative policies and procedures can have a large impact on vulnerability and are, typically, relatively inexpensive and highly cost effective. A policy on how to do something more securely or directives on not doing something risky, like writing down passwords where someone else can gain access to it, can be highly effective.

Physical safeguards reduce the vulnerability by controlling physical access to hardware, supporting infrastructure, and data in storage. Physical controls not only reduce threat of physical theft but also can reduce threats from environmental and natural causes, such as wind, water, earthquake and fire or loss of power and equipment cooling.

Technical security services are, according to HIPAA, designed to guard data integrity, confidentiality, and availability through access controls, user authorization procedures, user identification and authentication and data authentication. In the healthcare environment, the availability of data can be crucial and HIPAA specifically calls for a procedure for the emergency access to critical data in a crisis situation.

Technical security mechanisms are, according to HIPAA, processes that guard against unauthorized access to data that is transmitted over a communications network. These are data integrity and message authentication controls like virtual private networks (VPN's) or file encryption and check sums.

Step 9 is documentation of results or the risk assessment report, the final step. The format and detail of the report should depend on the target audience for the report, usually senior management, and should be presented in the format preferred by them. This should be determined early in the assessment process so that the proper data, quantitative or qualitative, is available for the report.

Note: The data collected and included in the risk assessment report is very sensitive information. A ready made list of the company's assets, their values and associated vulnerabilities and the current security practices in use could be all a potential threat needs to go from a threat to a successful exploit. In other words, the risk assessment itself is a potential vulnerability that needs to not only be included in the formal risk assessment but have adequate security controls in place before its started, rather than after the risk assessment.

Risk Management

According to the HIPAA Security Standard, Section 142.308(a)(10)(ii), Risk Management is the "process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk."

This closely parallels the three phases of risk management per NIST's Special Publication 800-30, which are:

(1) Risk Assessment
(2) Risk Mitigation
(3) Risk re-assessment or Evaluation.

After completion of the risk assessment phase as discussed above, the risk mitigation phase can begin. In the risk mitigation phase, additional security controls are evaluated and the most appropriate or cost effective controls are selected for implementation.

The most appropriate controls would be those that reduce the most risk or the ones that are the most cost effective, i.e. reduce the most risk per dollar spent. The highest risk events provide the most potential for a higher risk reduction per dollar spent, so start with controls that address the larger risk areas and evaluate the impact to all risk events that the new controls affect.

After choosing the first control to implement, the process for choosing the next most appropriate control should start with a new evaluation of risk by adjusting the risk assessment for each risk event for the previous chosen control. What would have been the next most cost-effective control, may become the least cost effective if it has no effect on the residual risk.

This process can be performed until the information security budget is exceeded or until the combined cost to the company of the residual risk and the cost of risk control measures is minimized. If quantitative data is available, a cost benefit analysis could be performed by plotting the cost of each chosen risk control and the cost to the company of the residual risk. The optimum point would be where

the total cost of risk and the cost of mitigation controls to the company is minimized as illustrated in Figure 1, below.

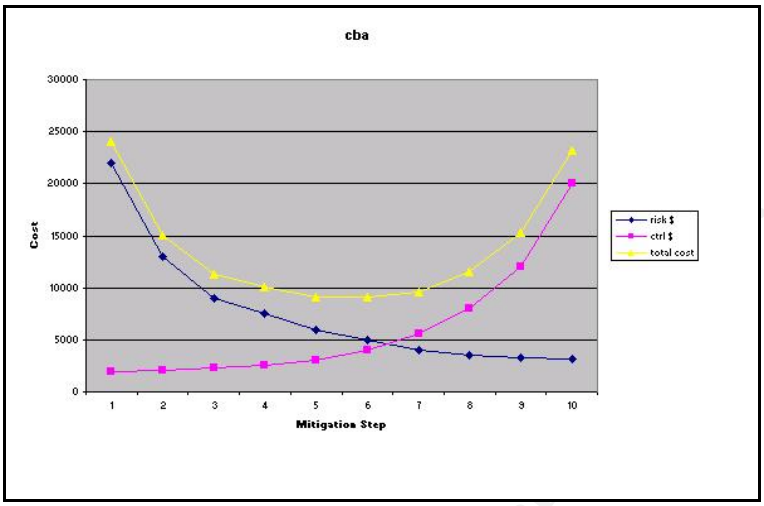

Figure 1, Cost Benefit Analysis Illustration

When dealing with information technology and healthcare, the risk environment is very dynamic. New threats, new vulnerabilities and new methods of dealing with them are discovered daily, requiring on-going risk monitoring and periodic risk re-assessment. This is phase 3, the on-going, never-ending re-evaluation phase of the risk management process.

Conclusions

Keeping up with new threats and vulnerabilities can be the key to risk management and there are many sources available to assist with this daunting task.

(1) Check with your anti-virus vendor very frequently for new anti-virus signatures and periodically for program updates and patches.

(2) Do the same for your operating system, check frequently for critical updates and patches.

(3) Subscribe to vulnerability list services like the SANS Critical Vulnerability Analysis weekly mailing at http://server2.sans.org/sansnews and the CERT Advisory mailing list at http://www.cert.org.

Apply controls that are inexpensive and provide reasonable risk mitigation.

(1) Set and enforce strict password policies

(2) Rename default administrator and guest accounts and change default passwords.

(3) Block executable and dangerous email attachments at the email server.

(4) Setup security audits and review logs regularly.

(5) Remove unnecessary applications and services.

(6) Perform frequent data backups and store them in a safe place.

(7) Use password protected screen savers to restrict access.

(8) Use a defense in depth strategy where possible.

(9) Educate and train users.

In the HIPAA environment, protect the PHI using the security standard, which includes a requirement for performing risk analysis and risk management.

(1) Administrative procedures

(2) Physical safeguards

(3) Technical security services

(4) Technical security mechanisms

Use risk management not only because it is required by HIPAA but because it will help select the most appropriate and cost effective information security measures.

---

[1] "Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, August 21, 1996, 104th Congress, Goals". URL: http://www.medscout.com/hipaa/goals/ (November 2002)

[2] United States Department of Health and Human Services, August 21, 2002, URL: http://www.hhs.gov/news/press/2002prs/hipaa.html (August 2002)

[3] "Security and Electronic Signature Standards." Federal Register Vol. 63, No.155 (1998): Section 142.308.

[4] The Society for Risk Analysis, Risk Glossary URL: http://www.sra.org (October 2002)

[5] Stonebumer, Gary, Goguen, Alice, and Feringa, Alexis. *Risk Management Guide for Information Technology Systems.* Special Publication 800-30. NIST. October 2001.

[6] Poulsen, Kevin. *Hospital Records Hack,* Security Focus, December 6, 2000. URL: http://online.securityfocus.com/news/122 (January 2003).
[7] ICAT database. URL: http://icat.nist.gov/icat.cfm. (January 2003).
[8] SANS/FBI Top 20 List URL: http://www.sans.org/top20. (January 2003).
[9] CERT/CC URL: http://www.cert.org/nav/index_red.html. (January 2003).
[10] Tipton, Harold F. and Krause, Micki. "Information Security Management Handbook". URL: http://www.cccure.org/Documents/HISM/229-230.html (January 2003).
[11] Tipton, Harold F. and Krause, Micki. "Information Security Management Handbook". URL: http://www.cccure.org/Documents/HISM/230-232.html (January 2003).