Global Information Assurance Certification Paper

Risk Analysis and HIPAA Security Rule Compliance

Jeff Estes
GIAC Security Essentials Practical
Version 1.4b, Option 1
July 30, 2003

Risk Analysis and HIPAA Security Rule Compliance

Managing risk is a primary function of any information security program. With the publishing of the Final Security Rule of the Health Insurance Portability and Accountability Act (HIPAA) in February 2003, risk analysis and risk management are now federally legislated requirements for companies who electronically maintain or transmit customer or patient health data, including healthcare providers and payers. The compliance date for the Final HIPAA Security Rule is April 21, 2005. Many organizations covered by HIPAA (covered entities) will struggle with this requirement. Undoubtedly, software publishers and individual entrepreneurs will attempt to create customized HIPAA risk analysis solutions to cash-in on the sudden, urgent need for HIPAA compliance. A query for HIPAA risk analysis on any common Internet search engine[1] will return thousands of responses, which may indicate that commercial solutions are already being advertised.

It may be assumed the importance of analyzing and accepting risk is ingrained in the insurance portion of the healthcare industry. Surprisingly, in a business that devotes significant salary dollars to actuaries for the sole purpose of calculating risk and probability, the idea of analyzing the risk of data exposure to the business is a foreign concept. HIPAA has helped heighten awareness of Risk Management issues, however. In fact, the feature article of the April 2003 issue of "Best's Review" [2] discusses Risk Management in the insurance industry.

This paper examines the components of formal and informal risk analysis processes as required by HIPAA, with an eye toward the benefits of risk management for any information security program. First, fundamentals of risk analysis in general are studied and applied to the HIPAA Security Rule. Next, baseline HIPAA terminology and definitions are established, and Implementation Specifications contingent upon a thorough risk analysis in the Final HIPAA Security Rule are examined. Finally, the focus shifts to steps for completing a thorough risk analysis for HIPAA compliance using commercially available software and less formal methods.

Risk Analysis Fundamentals

The Dictionary.com Web site[3] defines risk as:

> **(noun) 1:** The possibility of suffering harm or loss; danger.
> **2:** A factor, thing, element, or course involving uncertain danger; a hazard: "the usual risks of the desert: rattlesnakes, the heat, and lack of water" (Frank Clancy).
> **3 a:** The danger or probability of loss to an insurer. **b:** The amount that an insurance company stands to lose.
> **4 a:** The variability of returns from an investment. **b:** The chance of nonpayment of a debt.
> **5:** One considered with respect to the possibility of loss: *a poor risk.*

For purposes of HIPAA compliance, definition 3a is most appropriate. A HIPAA compliant risk analysis would identify the chance of loss or exposure of customer

data by identifying potential exposures of data held by the covered entity, and assign a degree of probability to that event occurring.

The reasons for performing a thorough risk analysis as required by HIPAA are to identify potential areas of exposure to covered entities and to improve the state of information security throughout the healthcare industry. If implemented correctly, the resulting compliance should provide a level of security appropriate to contain the level of risks identified and should reduce incidents of accidental exposure of patient and/or policyholder confidential health data.

The first step in preparing for a risk analysis is to assemble a project team consisting of representatives from each affected area. The risk analysis team should not be limited to members of the Information Technology (IT) department, and should not require any security expertise at all. Participation in the process by the business owners ensures their heightened awareness of the issue of risk, and will help gain their support for necessary technological improvements. Above all, the acceptance of risk should be a business decision, supported by system and security solutions when appropriate.

The risk analysis team has a greater chance for success if there is a clear picture of the expected results, so the first assignment should be to create an organizational plan detailing the goals for completing the risk analysis. The plan should include: [6]

- A work breakdown structure identifying high level tasks for completion
- A listing of applicable Implementation Requirements from the HIPAA Security Rule (see Table A below)
- A preliminary list of business areas and system applications within the organization where protected health information (PHI)[*] resides. The list may need to be modified as other business areas and applications with PHI are identified
- A process for ranking and scoring potential exposures (this is important to establish a consistent approach for the team)
- A process for reporting findings to management, and
- A documentation strategy.

Additional items to include are examples of potential external threats and internal weaknesses and sample system and/or business security solutions for comparison. For example, the covered entity may identify the risk of intercepting external email containing PHI as an external threat. A system security solution may be to encrypt the data or to utilize a secure means of communication, such as a virtual private network (VPN). A non-technical business solution may be to implement a policy prohibiting the transmission of PHI in an unsecured manner.

[*] Part II, 45CFR 164.501 in the Final Security Rule removed the official definition of protected health information. The process of identifying PHI is described below in Example 1.

Either may be acceptable solutions, depending upon the level of risk the covered entity is willing to accept.

An example of an internal weakness may be the use of shared printers in areas that regularly handle PHI. If the organization feels there is a danger of exposing PHI to employees who are not allowed access, such as employees from other areas who share the printer or maintenance staff, documentation must quantify the risk and propose solutions. The IT department may recommend sharing printers only within similar business areas using PHI, or issuing personal printers to each employee who handles PHI as a regular part of their duties. The business area may decide the use of shared printers is reasonable, but institute a policy requiring staff to retrieve printouts within a specified period of time, or assign one individual the responsibility of retrieving and delivering printouts at regular intervals throughout the workday.

Above all, the organization plan should include a documentation strategy. The mantra "If you haven't documented it, you haven't done it" should be followed by all organizations striving for compliance. Consistent and thorough documentation will be essential to prove compliance in the event of litigation or audit so great care should be taken to create a thorough and clear record in the event proof is required. A well-organized plan of documentation will prove the level of effort exerted and demonstrate the level of commitment to protect PHI by the company. The authors of HIPAA have gone to great lengths to avoid a common prescription for compliance, and the documentation generated by the covered entity will serve as their major proof of compliance.

After the organizational plan is completed, the covered entity should choose whether to conduct a formal or informal risk analysis. A formal risk analysis utilizes a commercial product to identify potential exposures. The benefits of formal risk analysis are discussed later in the Risk Analysis Tools section of this paper. An informal analysis may be conducted by comparing the Security Rule point-by-point with existing departmental policies and procedures. The team may wish to interview current subject matter experts regarding their policies and document their results. A resultant gap analysis should highlight areas of concern. Those areas may then be prioritized, weighted, and scored to identify the greatest risk of exposure and highest probability of occurrence. The topics receiving the highest risk score would logically include those most important to organizational well-being and should be addressed first. The Rule was written with security best practices in mind, so a comparison will probably identify areas where the organization is already in compliance. For example, the covered entity may have existing policies for data backup or for password strength. If the company-wide policy already meets HIPAA requirements, the policy should be documented as verification of compliance. In cases where no policy exists, or doesn't meet the requirements of HIPAA, the covered entity should address the item and implement a solution which will reduce the level of risk to an acceptable level.

The major concern with an informal analysis is the strong reliance on existing knowledge and awareness of current procedures. If the interviews aren't conducted in a controlled environment, or don't include the necessary level of detail, salient points could easily be missed. The quality of the interview relies on the quality of questions and documentation, as well as the answers given.

HIPAA Security Rule Fundamentals

The Final HIPAA Security Rule is divided into Administrative, Physical, and Technical Safeguards, which are designed to protect the confidentiality, integrity, and availability of PHI. The Administrative Safeguards section contains requirements for business policies and procedures necessary to support technical solutions for safeguarding PHI. Administrative Safeguards include a requirement for ensuring PHI is adequately protected and available in case of a catastrophic event, and for ensuring that those with whom the covered entity exchanges data are required to protect the information at the same level of diligence. Physical Safeguards require covered entities to protect customer data by controlling access to facilities or media containing PHI. Examples include requirements for building and perimeter security and policies and procedures for computer workstations and other removable media. Technical Safeguards for PHI include systems solutions and policies for ensuring associates have appropriate access to PHI at the minimum level required to perform their job function, and that these access levels are audited periodically. In addition, Technical Safeguards include requirements ensuring data integrity and secure transmission of PHI where appropriate.

Each of these sections is further sub-divided into Standards with Required or Addressable Implementation Specifications. Standards are general requirements that describe the level at which the covered entity is expected to protect customer data. Implementation Specifications contain activities necessary to achieve compliance with the Standard, and may be designated as Required or Addressable. In cases where the Standard does not include separate Implementation Specifications, the Standard itself serves as a Required Implementation Specification. An important point to remember is "Addressable" does not mean "Optional" in regard to Implementation Specifications. The covered entity has three options for an Addressable Implementation Specification:

- if the solution is considered reasonable and doesn't reduce the impact of other security solutions, it must be implemented;
- if it is not considered a reasonable solution, another equivalent solution may be chosen; or
- if the standard can be achieved through other means, the organization may decide not to implement a solution at all.[5]

If the third option is chosen, the covered entity is required to document their reasons for the decision.

HIPAA covered entities are those organizations which maintain individually identifiable health information as part of their business. The tendency may be to only consider organizations within the healthcare and insurance industries as HIPAA covered entities. However, companies who maintain employee personal health information for their group insurance policies are also covered and have an obligation to protect employee health data at the same level as providers and insurers. It is important to remember the data must be maintained or transmitted in electronic form to be subject to the HIPAA Security Rule.

The primary concern for a covered entity should be to accurately and completely identify and locate the information the organization is required to protect – the protected health information (PHI). The identification of PHI is a potentially complex process, and requires analysis of the Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule).[4] As a basic rule, PHI is data used or disclosed for treatment, payment, or healthcare operations which can be used to identify the individual directly. PHI may also be context-based, and the organization may find it helpful to create a checklist similar to Example 1 (below) to identify the PHI in its possession.

Example 1 - Questionnaire for identifying PHI

1. Does the document or record contain any of the following identification elements?
    1) Names;
    2) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code;
    3) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death;
    4) Telephone numbers;
    5) Fax numbers;
    6) Electronic mail addresses;
    7) Social security numbers;
    8) Medical record numbers;
    9) Health plan beneficiary numbers;
    10) Account numbers;
    11) Certificate/license numbers;
    12) Vehicle identifiers and serial numbers, including license plate numbers;
    13) Device identifiers and serial numbers;
    14) Web Universal Resource Locators (URLs);
    15) Internet Protocol (IP) address numbers;
    16) Biometric identifiers, including finger and voice prints;
    17) Full face photographic images and any comparable images; or
    18) Any other unique identifying number, characteristic, or code.

If yes, proceed to question #3.
If no, proceed to question # 2.

2. Do you have any actual knowledge that this information could be used alone or in combination with other information to identify the subject of the information?

If yes, proceed to question #3.
If no, data is not protected health information under HIPAA so you may stop here.

3. Does the document or record relate to the past, present, or future, physical or mental health or condition of an individual (e.g. diagnosis code, medical exam results, lab results, anything that suggests a medical condition)?

If yes, proceed to question # 6.
If no, proceed to question # 4.

4. Does the document or record relate to the provision of health care to an individual? (e.g., procedure codes, listings of pharmaceuticals or treatments prescribed, therapy notes).

If yes, proceed to question # 6.
If no, proceed to question # 5.

5. Does the document or record relate to payment for the provision of health care to an individual?

If yes, proceed to question #6.
If no, data is not protected health information under HIPAA so you may stop here.

6. Was the document or record created or received by the company or group health plan?

If yes, proceed to question #7.
If no, data is not protected health information under HIPAA so you may stop here r.

7. Is the document or record an "employment record"?

An "Employment Record" means records held by a covered entity in its role as an employer.

If yes, the data is not protected health information (because employment records are specifically exempted from the definition of PHI).
If no, information is protected health information.

Data must meet all criteria above to qualify as PHI. Some pieces of data that should be protected are obvious, such as an individual's name and address in combination with a diagnosis or treatment information. Other data may not be as obvious and should be examined within the context it is presented. Consider the following as an example of the importance of identifying PHI in context. A medical report is received at Company A indicating an unnamed employee is expecting a child. Fellow employees may reasonably infer the employee in question is a female of child-bearing age. It would be almost impossible to identify the subject of the medical report if Company A is a large organization (over 5000 employees). However, if Company A is a small business with 10 employees, the probability of identifying the expectant mother with the same data is significantly increased. If this scenario is applied to a specific area, department, or team within the large version of Company A, the probability of

identification also increases. Therefore, the organization must consider contextual use of data in the identification of PHI.

The example above is a popular example at HIPAA conferences, because it denotes a positive experience in the lives of many people. Conversely, consider the same scenario depicting a medical condition with traditionally negative emotional attachments, such as cancer or AIDS. In this example, the need for protecting an individual's personal health data becomes painfully clear.

Risk and the Final HIPAA Security Rule

The concepts of risk analysis and risk management are prevalent throughout the Final HIPAA Security Rule. The Centers for Medicare & Medicaid Services (CMS) within the U.S. Department of Health and Human Services (HHS), authors of HIPAA, sought advice and input from security professionals before finalizing the Security Rule. Their focus on the issue of risk is illustrated in this quote from the Final HIPAA Security Rule:

> The confidentiality of health information is threatened not only by the risk of improper access to stored information, but also by the risk of interception during electronic transmission of the information. The purpose of this final rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. [5]

Before the Final Security Rule was released, HHS published a "Proposed" version for public comment. In the proposed rule each Implementation Requirement was listed alphabetically to avoid giving the impression that any one implementation requirement was more important than the others. By contrast, the Final Rule lists the Standard Security Management Process first as the "foundation on which all further Standards depend."[4] The Implementation Specifications for this standard include Risk Analysis, Risk Management, Sanction Policy, and Information System Activity Review.

As stated in the Final HIPAA Security Rule, the Implementation Specification Risk Analysis requires each covered entity to:

> "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity." [5]

The process of conducting a risk assessment is a daunting task for even the most mature information security program. Healthcare providers, most of whom are much more comfortable with a patient than a computer, may find themselves ill-equipped to meet such a standard and have expressed a desire to find a commercial product to fill their needs. Unfortunately, a single "one-size-fits-all" solution does not exist, and each covered entity needs to undertake a thorough analysis of their exposures and determine the level of risk the organization is willing to accept.

The concept of risk acceptance is arguably the least clearly defined idea within the Final Security Rule. The authors of HIPAA, in an effort to avoid crafting a single standard for all large and small organizations, pushed the burden onto the covered entity to define their own standards. Each covered entity must conduct an analysis to identify areas of risk, quantify the likelihood of incidents occurring, choose solutions for themselves, and be ready to defend their choices in court – a familiar scenario for the litigation-plagued healthcare industry.

An example of a Required Implementation Specification which is dependent upon the results of a risk analysis is the Contingency Plan. Before developing a plan for contingencies in the event of an emergency, the organization first needs to identify its "crown jewels." That is, those applications or data stores without which the company cannot function. Every application housing PHI should be analyzed and prioritized in comparison with all others to create a strategy for bringing information systems back on line after a system interruption or major catastrophe. Next, the covered entity should create a work plan detailing the highest priority items to address, and then develop individual recovery plans and workarounds to bring the items into compliance. In this way, the covered entity is identifying the level of risk it is willing to accept and establishing recovery procedures that may be repeatable by other areas.

Solutions to several other Implementation Specifications are predicated upon the results of the risk analysis performed by the HIPAA covered entity including standards within all categories of safeguards (see Table A). To achieve HIPAA compliance, the risk analysis conducted by the covered entity must include its administrative policies, the physical security of its facilities, and technical security surrounding its information systems. Obviously, multiple solutions may be applied to mitigate a single security issue depending upon the level of risk the organization is willing to accept, financial investment required, and existing security practices. The covered entity must choose the solution that best fits within their overall security policy.

Large healthcare organizations may find the necessary coordination across departments to be quite burdensome as they collate information from disparate sources. However, the subject matter experts identified in the risk analysis are useful resources to represent business areas during the development of contingency plans for the organization.

Table A.

Administrative Safeguards (§164.308)	
	Workforce Security (a)(3)(i)
	Security Incident Procedures (a)(6)
	Contingency Plan (a)(7)(i)
	Evaluation (a)(8)
Physical Safeguards (§164.310)	

	Workstation Security (c)
	Device and Media Controls (d)(1)
Technical Safeguards (§164.312)	
	Access Control (a)(1)
	Audit Controls (b)
	Integrity (c)(1)
	Transmission Security (e)(1)

Risk Analysis Tools

Inclusion of commercial risk assessment tools and consultants is for illustrative purposes only and indicates neither endorsement nor indictment of the products. The order of listing should not be interpreted as a ranking. Web sites promoting risk assessment tools and methodologies are abundant on the Internet and the examples chosen randomly based on the results from a common search engine.[1] The choice of a commercial risk assessment product or methodology is the responsibility of the HIPAA covered entity as they determine the best fit with their enterprise needs and goals. The Security Rule refrains from recommending specific commercial products or approaches, deferring instead to the Strategic National Implementation Process (SNIP), a subgroup of the Workgroup for Electronic Data Interchange (WEDI™), established to facilitate national HIPAA compliance.[7] The SNIP Web site includes a link to the "HIPAA Resource Directory" which includes sample tools and a large amount of reference information for HIPAA education. The site also includes a link to commercial vendor solutions and an overview of the HIPAA legislation.

The choice of utilizing a commercial risk analysis product may add additional start-up time to evaluate and select the right software for the covered entity, but should also add the benefits of suggested solutions and professional looking reports. Less technologically advanced businesses, such as many small doctors' offices, may prefer general commercial risk analysis software package, a risk analysis program designed for HIPAA compliance, or may choose to outsource the work completely. Several consulting firms offer a complete HIPAA risk analysis utilizing a proprietary methodology. The firms may also suggest mitigating strategies and implement the solutions for an additional fee.

Covered entities preferring a general risk analysis approach may choose a software solution such as Consultative, Objective and Bi-functional Risk Analysis (COBRA), from C & A Security Risk Analysis Group (U.K.),[8] or System Scanner® from Internet Security Systems (ISS™).[9] COBRA includes three stages – "Questionnaire Building," "Risk Surveying," and "Report Generation". Though this program was not designed for HIPAA, it still may prove to be a viable solution for covered entities who desire the ability to customize their approach. Attention has been paid to incorporating business language to facilitate business partner involvement, as well as Information Technology staff. The Web site

includes a trial version of COBRA for download and general information of the risk analysis process. Prospective customers are encouraged to contact the company with questions.

System Scanner® is the network risk analysis tool of the RealSecure® Vulnerability Assessment Component. The Internet Security Systems (ISS™) Web site contains several risk analysis tools, each with a different focus such as policy analysis, database, and network. The company also offers a 5-step risk analysis package for HIPAA compliance - Assessment, Design, Deployment, Management and Education (ADDME™). Further information, including a PDF for download may be obtained at the ISS™ Web site.

Covered entities preferring a HIPAA-specific risk analysis program may choose HIPAAsure™ from Caveo Technologies, Inc.,[10] or HIPAA-Watch for Security from RiskWatch™.[11] HIPAAsure™ is a commercial product marketed to healthcare organizations for overall HIPAA compliance. HIPAAsure™ appears to have been developed to provide a thorough, flexible approach to complying with HIPAA. The end result should be a comprehensive organizational view of the organizations' compliance efforts. The product contains modules titled "Gap Analysis," "Risk Assessment," "Testing," and "Security Solutions." Separating the gap analysis from the risk assessment indicates a desire to simplify the process for the less technologically developed portions of the healthcare industry. More importantly, this may be a single package solution which a covered entity could purchase to provide a significant roadmap toward meeting each of the HIPAA Implementation Specifications.

HIPAA-Watch for Security was designed for compliance with the Final Security Rule and includes additional information on security best-practices. The RiskWatch™ organization offers several other tools for risk analysis outside the healthcare industry. The Web site offers a PDF for download and online training sessions.

Examples of consultants for hire include CoyoteWorks™ Technologies, Inc. or Fortrex Technologies, Inc[13]. The CoyoteWorks™ Web site[12] includes a 6-step approach for completing a risk analysis, and high-level information about their services. Fortrex Technologies, Inc. has partnered with Phoenix HealthCare Systems (publishers of the HIPAAdvisory Web site[14]). Fortrex is an information security company which recognizes the need for security consulting in the healthcare industry. The Fortrex Technologies Web site contains several security whitepapers in PDF format, as well as links to their strategic business partners and contact information.

Conclusion

To ensure HIPAA compliance, covered entities must devote the resources necessary to complete a comprehensive risk assessment, implement solutions

where necessary, address each portion of the Security Rule equally and, above all, document decisions made by the organization. HIPAA does not dictate the path to compliance. Rather, each covered entity is required to choose their own path through a formal or informal process, or by utilizing the services of an independent consultant. Court rulings will eventually provide a benchmark to compliance. Until then, each covered entity will be held to the standard set by existing security policies and procedures and by documentation proving efforts to mitigate risk at a level the organization is willing to accept.

The federally mandated compliance date for the HIPAA Security Rule will be challenging for non-technologically savvy healthcare organizations to meet. Though the two-year compliance period may seem distant, covered entities should not postpone the risk analysis process. Several Implementation Specifications from the Final Security Rule refer to and support the HIPAA Privacy Rule, which is already in effect. There have been no court decisions regarding HIPAA as of the writing of this paper, but HHS made it clear in the Preamble to the Final Security Rule that they intend the security standards to support the privacy of PHI.[5] The argument may be made that some security solutions should have already been implemented.

The goal of HIPAA is to reform healthcare in the United States, including the return of control of an individual's personal information to the individual. Assessing risk by the organization is the first step toward assuring the public that personal health data is neither being bought and sold on a wholesale basis, nor openly exposed to hackers and other miscreants. HIPAA was passed into law to improve security around PHI, but compliance will require a new mindset for an industry where open exchange of data has historically been considered essential for treating patients.

References

[1] Search for "HIPAA risk analysis" – URL: http://www.google.com/search?hl=en&ie=UTF-8&oe=UTF-8&q=HIPAA+risk+analysis, (May 10, 2003)

[2] Green, Meg. "Microscope or Binoculars." Best's Review April 2003 (2003): 21 – 27.

[3] Dictionary.com – URL: http://dictionary.reference.com/search?q=risk (July 30, 2003)

[4] Department of Health and Human Services. Office of the Secretary. *Standards for Privacy of Individually Identifiable Health Information; Final Rule.* Washington: Government Printing Office, 2002. (45 CFR Parts 160 and 164). URL: http://www.hhs.gov/ocr/hipaa/privrulepd.pdf

[5] Department of Health and Human Services. Office of the Secretary. *Health Insurance Reform: Security Standards; Final Rule.* Washington: Government Printing Office, 2003. (45 CFR Parts 160, 162, and 164). URL: http://aspe.hhs.gov/admnsimp/FINAL/FR03-8334.pdf (July 30, 2003)

[6] HIPAA Compliance Risk Analysis; Ink2Web Technologies, Inc. – URL: http://www.ink2web.com/hipaacra.html (July 30, 2003)

[7] Workgroup for Electronic Data Interchange (WEDI™) – Strategic National Implementation Process (SNIP) – URL: http://www.wedi.org/snip (July 30, 2003)

[8] Consultative, Objective and Bi-functional Risk Analysis (COBRA), C & A Security Risk Analysis Group – URL: http://www.security-risk-analysis.com (July 30, 2003)

[9] System Scanner®; Internet Security Systems, Inc (ISS™) – URL: http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_system.php (July 30, 2003)

[10] HIPAAsure™; Caveo Technologies, Inc. – URL : http://www.caveoinc.com/HTML/HIPAAssure.htm (July 30, 2003)

[11] HIPAA-Watch for Security; Risk Watch™ - URL: http://www.riskwatch.com (July 30, 2003)

[12] CoyoteWorks™ Technologies, Inc. – URL : http://www.coyoteworks.com/hipaacra (July 30, 2003)

[13] Fortrex Technologies, Inc. – URL: http://www.fortrex.com (July 30, 2003)

[14] HIPAAdvisory – URL: http://www.hipaadvisory.com (July 30, 2003)