STATEMENT OF WORK
FOR
HIPAA SECURITY RISK ANALYSIS

April 14, 2004

Prepared by:  Bob Matthews
HIPAA Compliance Services Manager
HIPAA Academy
4320 Winfield Road
Warrenville, IL 60555
www.HIPAAAcademy.Net

Contact:  877.899.9974 x20, Bob.Matthews@HIPAAAcademy.Net
About the HIPAA Academy

The HIPAA Academy (www.HIPAAAcademy.Net) is the gold standard in the industry for HIPAA consulting, training and certification. HIPAA Academy delivers solutions in the areas of HIPAA Professional Services, HIPAA Advisory Services, HIPAA Risk Analysis, Gap Analysis, Security Policy development, HIPAA Audit and Evaluation and HIPAA Training and Certification. HIPAA Academy clients include several state governments, including the State of Oregon and Illinois, as well as many county governments.

HIPAA Academy’s Certified HIPAA Security Specialist (CHSS) program is a fast-growing certification program whose attendees include CISSPs, RSA Security, Sprint, AT&T, HP, and many hospitals and government agencies. The HIPAA Academy’s Getting Started with HIPAA and The Seven Steps to HIPAA Security Compliance are the best-selling text on the subject at several sites, including Amazon.com and BN.com. The HIPAA Academy has authored several industry leading texts on HIPAA Security. These are available at the e-store at www.HIPAAAcademy.Net.

Contact Information

ecfirst.com (HIPAA Academy)
4320 Winfield Road, Suite 200, Warrenville, IL 60555

Phone: 877.899.9974 x20
Fax: 515.453.8471
Website: www.HIPAAAcademy.Net

Federal Tax ID: 42–1486030
Executive Summary

Risk analysis and information system activity review are required implementation specifications defined in the System Management Process standard in the HIPAA Security Rule. Business Impact Analysis (BIA) is a critical initial step in contingency planning. A BIA helps to identify and prioritize critical systems and components. Risk analysis and BIA are the initial activities that covered entities must launch to identify vulnerabilities as well as gaps related to compliance requirements.

Key Deliverable

The HIPAAShield™ Risk Analysis Report will include information in the following areas:

e-PHI Documentation
- Identify systems with e-PHI
- Document the purpose of these systems
- Document the flow of e-PHI
- Risk Assessment Surveys
- Critical Asset Inventory

Risk Assessment
- Identify vulnerabilities and threats to e-PHI
- Gap analysis with HIPAA Security Rule requirements

Safeguards Determination
- Recommend safeguards for e-PHI
- Identify remediation activities to comply with HIPAA Security Rule

Your Organization Will Be Compliant In These Areas

At the conclusion of the HIPAAShield™ Risk Analysis engagement, your organization will be compliant with these implementation specifications defined in the HIPAA Security Rule:

<table>
<thead>
<tr>
<th>Standards</th>
<th>Implementation Specifications</th>
<th>R = Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Process</td>
<td>• Risk Analysis</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>• Information System Activity Review</td>
<td>R</td>
</tr>
</tbody>
</table>

Figure 1: Scope of Risk Analysis Project.

Further, your organization will have all the information required to launch projects and activities related to all “gaps” identified that your organization needs to address to be compliant with the HIPAA Security Rule.
Our Commitment to Your Organization

Our responsibilities include, but are not limited to, performing the following tasks:

- Understand the HIPAA Security Rule Specifications
- Determine and document the status of each Program Area with relation to each HIPAA Security Rule Specification
- Meet Business stakeholders to ensure their needs are incorporated into the business specifications
- Identify business processes impacted by HIPAA Security Rule compliance
- Work with programs within your organization to communicate how HIPAA Security Rule requirements would fit into the business environment
- Create diagrams of new and/or modified business processes and functions
- Interview appropriate technical and business users
- Identify internal entities responsible for maintaining technical components and environments and
- Report to the Security Project Manager on a daily/weekly/monthly basis on project issues and status. Prepare written reports as assigned

The Seven Steps to HIPAA Security Compliance™

Risk analysis identifies areas that need to be addressed for HIPAA security compliance as well as all gaps that may be exploited by insider and outsider attacks. Organizations are required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information (e-PHI).

Risk analysis is a process whereby relevant assets and relevant threats are identified, and cost-effective security/control measures are identified or engineered, in order to effectively balance the costs of various security/risk mitigation/control measures against the losses that would be expected if these measures were not in place. Threats and risks are real. Each entity needs to identify and prioritize risks and threats.

A thorough risk assessment should identify the system vulnerabilities, threat, and current controls and attempt to determine the risk based on the likelihood and threat impact. These risks should then be assessed and a risk level assigned, such as high, medium, or low.

The HIPAAShield™ Seven Steps to HIPAA Security Compliance is a comprehensive methodology that provides a complete framework to launch activities to bring an organization into compliance with the HIPAA Security Rule. The HIPAAShield™ security methodology identifies seven critical steps for an organization to implement to become compliant with the HIPAA Security Rule. In this Statement of Work our focus is on Step 2: Risk Analysis. For a much more detailed discussion on Risk Analysis, please review the publication titled, *HIPAA Security and Risk Analysis*. This publication is available from the e-store at [www.HIPAAAcademy.Net](http://www.HIPAAAcademy.Net).
Figure 2 illustrates the Seven Steps. Associated with each step are specific activities. The objective of Step 2: Risk Analysis includes the following activities:

1. Identify vulnerabilities
2. Identify contingency requirements, such as inventory of critical assets
3. Conduct information system activity review

The team must conduct an information system activity review. The objective of an information system activity review is to analyze records of information system activity, such as audit logs, access reports, and security incident tracking reports. This is an important activity. It enables the organization to review the type of information that is currently being logged or recorded and determine if there is a need to record additional information and/or identify additional systems that need to be monitored. The information system activity review will provide essential information to identify vulnerabilities.
To address the area of vulnerability assessment, the organization must create an inventory of all vital enterprise assets, systems and communications. The risk analysis team must create a pre-assessment checklist to document information about all critical systems and applications that process or store e-PHI. The risk analysis team then specifically identifies:

- Key information technology systems and components for each critical asset
- Key systems and components for technology weaknesses/vulnerabilities that may be exploited

Vulnerability tools such as scanning software, checklists and scripts may be used to identify weaknesses in the security of the organization.

A BIA is a critical step in contingency planning. A BIA helps to identify and prioritize critical Information Technology (IT) systems and components. As part of the BIA process, information is collected, analyzed and interpreted. The information provides the basis for defining contingency requirements and priorities. The end result is the creation of a BIA report to identify requirements for contingency planning.

**“We need to be compulsive about managing risk.”**

Uday O. Ali Pabrai, CISSP, CHSS

The end result of the risk analysis process should be a list of vulnerabilities that identify gaps in the security infrastructure that may be exploited. The threat to the infrastructure is serious. The CIO magazine reported that in December of 2002 hard drives that contained more than 500,000 social security numbers of members were stolen from the Phoenix office of TriWest, a managed care provider serving the military. This resulted in a class action suit as a result of the breach.

**Project Phases**

The HIPAA Shield™ Risk Analysis activities are organized on the basis of the following phases:

- Phase I: Documentation Phase
- Phase II: Risk Assessment Phase
- Phase III: Safeguards Determination Phase

The objective of Phase I is to identify all critical systems that process e-PHI or other sensitive business/patient/client information, document the purpose of these systems and document the flow of information. In Phase II the emphasis is to identify threats, vulnerabilities, to determine the likelihood and impact of risk. Phase III’s focus is on the determination of safeguards.
At the conclusion of Step 2: Risk Analysis which includes all 3 phases, the organization will have identified important assets, perceived threats, security requirements, current security practices and organizational vulnerabilities.

Scope

This Risk Analysis Statement of Work activity will result in a complete identification of “gaps” that exist between HIPAA Security Rule requirements and the state of your organization’s security.

Each phase of the HIPAA Security Risk Analysis Project will address the following sets of safeguards that make up the HIPAA Security Standards as defined in the HIPAA Final Security Rule:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

In total, the three categories of Safeguards include 18 Security Standards, made up of 42 Implementation Specifications. The scope of the HIPAA Security Project includes execution of Phases 2 and 3 as listed above for all 42 HIPAA Final Security Rule Implementation Specifications for all potentially impacted e-PHI information systems.

The Security Safeguards and their associated Security Standards and Implementation Specifications that the HIPAA Academy will analyze are as follows.

Administrative Safeguards (164.308)

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect e-PHI and to manage the conduct of the covered entity’s workforce in relation to the protection of that information. Figure 3 summarizes the Administrative Safeguards’ standards and their associated required and addressable implementation specifications.

<table>
<thead>
<tr>
<th>Standards</th>
<th>Implementation Specifications</th>
<th>R = Required</th>
<th>A = Addressable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Process</td>
<td>Risk Analysis</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sanction Policy</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information System Activity Review</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Assigned Security Responsibility</td>
<td></td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Workforce Security</td>
<td>Authorization and/or Supervision</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Workforce Clearance Procedure</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Termination Procedures</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Information Access Management</td>
<td>Isolating Health care Clearinghouse Function</td>
<td>R</td>
<td></td>
</tr>
</tbody>
</table>
Figure 3: Administrative Safeguards Standards.

Physical Safeguards (164.310)

Physical safeguards are physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. Figure 4 summarizes the Physical Safeguards’ standards and their associated required and addressable implementation specifications.

Figure 4: Physical Safeguards Standards.
Technical Safeguards (164.312)

Technical safeguards refer to the technology and the policy and procedures for its use that protect electronic PHI and control access to it. Figure 5 summarizes the Technical Safeguards’ standards and their associated required and addressable implementation specifications.

<table>
<thead>
<tr>
<th>Standards</th>
<th>Implementation Specifications</th>
<th>R = Required</th>
<th>A = Addressable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Unique User Identification</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Emergency Access Procedure</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automatic Logoff</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Encryption and Decryption</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Audit Controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td>Mechanism to Authenticate</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Person or Entity Authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmission Security</td>
<td>Integrity Controls</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
<td>A</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5: Technical Safeguards Standards.

The federal deadline for HIPAA compliance with the HIPAA Security Rule is April 21, 2005.

Deliverables

This Risk Analysis Statement of Work activity will result in a complete identification of “gaps” that exist between HIPAA Security Rule requirements and the state of your organization’s security.

Our Project Leader will interact, interview, research, document and report on findings relative to the Safeguards, Standards and Specifications of the HIPAA Security Rule, whether they are Addressable or Required. Our organization will work closely with all key members of your organization to collect and analyze the information vital for compliance.

<table>
<thead>
<tr>
<th>Deliverable</th>
<th>Phase</th>
<th>Content Deliverables</th>
</tr>
</thead>
</table>
| 1           | Documentation and Risk Assessment | Inventory of Administrative safeguards in place across all potentially impacted e-PHI systems, including:  
|             |                              | • Security management process                                                        |
|             |                              | • Assigned security responsibility                                                    |
|             |                              | • Workforce security                                                                  |
| **2** | Documentation and Risk Assessment | Inventory of Physical Safeguards in place across all potentially impacted e-PHI systems, including:
- Facility access controls
- Workstation use
- Workstation security
- Device and media controls |

| **3** | Documentation and Risk Assessment | Inventory of Technical Safeguards in place across all potentially impacted e-PHI systems, including:
- Access controls
- Audit controls
- Integrity mechanisms
- Person/entity authentication
- Transmissions security |

| **4** | Safeguards Determination | A complete series of findings by Program Area that clearly state the business, procedural, and technical needs considered necessary for satisfying any Security Rule Administrative, Physical and Technical compliance requirements that are not satisfied currently.

This information will be based on the inventories across all potentially impacted e-PHI systems conducted in the Assessment Phase.

The Recommendations for Identifying Safeguards will be based on several factors including volume of information to be conveyed and number of affected e-PHI Program Areas.

This deliverable will include an updated, completed list of e-PHI impacted Program Areas and their systems. |

---

Figure 6: Risk Analysis Project Activities and Deliverables.
For planning purposes, assume site visits for assessing physical safeguards. Other safeguards (technical, administrative) will be handled through surveys, teleconferences, and other communications means without site visits.

The HIPAAShield™ Risk Analysis Report
A HIPAAShield™ Risk Analysis Report will be created based on our review and analysis of information collected from your organization. All areas that the organization is in compliance with the legislation will be clearly identified, as well as gaps that may exist where the organization is not in compliance with standards and implementation specification defined in the HIPAA Security Rule. The HIPAAShield™ Risk Analysis Report outlines potential threats to your organization along with recommendations for remediation activities.

HIPAAShield™ Risk Analysis Report also includes the complete results of any vulnerability or penetration testing performed on your network (if a vulnerability assessment is conducted by The HIPAA Academy within the scope of this engagement). This HIPAAShield™ Risk Analysis Report will include information in the following areas:

e-PHI Documentation
- Identify systems with e-PHI
- Document the purpose of these systems
- Document the flow of e-PHI
- Risk Assessment Surveys
- Critical Asset Inventory

Risk Assessment
- Identify vulnerabilities and threats to e-PHI
- Gap analysis with HIPAA Security Rule requirements

Safeguards Determination
- Recommend safeguards for e-PHI
- Identify remediation activities to comply with HIPAA Security Rule

Your Organization Will Be Compliant In These Areas
At the conclusion of the HIPAAShield™ Risk Analysis engagement, your organization will be compliant with these implementation specifications defined in the HIPAA Security Rule:

<table>
<thead>
<tr>
<th>Standards</th>
<th>Implementation Specifications</th>
<th>R = Required A - Addressable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Process</td>
<td>• Risk Analysis</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>• Information System Activity Review</td>
<td>R</td>
</tr>
</tbody>
</table>

Figure 7: Scope of Risk Analysis Project.
Further, your organization will have all the information required to launch projects and activities related to all “gaps” identified that your organization needs to address to be compliant with the HIPAA Security Rule.
Pricing

Option A (without vulnerability assessment)
2 consultants, 1-day onsite and 4 days off-site
$9,995 plus expenses

Option B (with vulnerability assessment)
2 consultants 2 days onsite and 8 days offline
$19,995 plus expenses less discount of $3000 if PO is received by 4/30/04

<table>
<thead>
<tr>
<th>Services</th>
<th>Price per Site</th>
<th>No. of Sites</th>
<th>Total Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option A (only Risk Analysis)</td>
<td>$9,995</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Option B (Risk Analysis &amp; Vulnerability Assessment)</td>
<td>$19,995</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presentation of Risk Analysis Report (optional)</td>
<td>$1,500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LESS: Discount (if any)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Price</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Pricing is based on the following assumption:
- One site (one location). Please call Bob Matthews to discuss any requirements that may need the Statement of Work (SOW) to be amended to meet the specific needs of your organization.

Please contact HIPAA Academy for discounts related to additional sites.
Start date for the engagement will be decided on a mutually agreeable date.

Payment Schedule
All expenses will require prior approval and will be billed at cost. 50% of the payment must be received 1 week prior to the start date of the engagement. The prices mentioned in the SOW are valid until close of business April 30, 2004.

HIPAA Academy
Name: Bob Matthews
Title: HIPAA Services Manager
Phone: 877.899.9974 x20

Client Information
Name: _________________________________
Title: __________________________________
Phone: _________________________________
Date: _________________________________
P.O. #:_________________________________

Signature: ____________________________

© All Rights Reserved, HIPAA Academy, 2004.
www.HIPAAacademy.Net