athenahealth
there is a better way

Fulfilled Outside of athenaNet:
Security Plan

Conduct security risk analysis, implement security updates as needed, and correct identified deficiencies.

How does CMS define this measure?

Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), implement security updates as necessary, and correct identified security deficiencies as part of its risk management process. For more detailed CMS criteria click here.

What configuration is required in athenaNet?

n/a

How is the measure calculated?

This measure must be satisfied outside of athenaNet at your practice. During the athenahealth Attestation process, you will be able to indicate that you have conducted or reviewed the security risk analysis.

How should this measure be satisfied?

You must protect electronic health information by conducting or reviewing a security risk analysis of certified EHR technology and implementing updates as necessary at least once prior to the end of the EHR reporting period. A security update would be required if any security deficiencies were identified during the risk analysis. The testing can occur prior to the beginning of the first EHR reporting period. However, a new review would have to occur for each subsequent reporting period.

We will provide self-service materials on the Meaningful Use Resource Center that you can leverage to complete the requirements of this measure at no cost.

Additionally, we will provide the contact information of a 3rd party security consultant that you may wish to engage for additional security support.

What are the athenahealth best practices?

athenahealth cannot provide specific security risk guidance.

However, at athenahealth, we take the security and privacy of health information very seriously. We have taken measures to ensure that our system is secure and have met our obligations in compliance with the HIPAA Security Standards Final Rule, as well as CCHIT Meaningful Use Security Requirements to specifically protect all electronic health information created or maintained by our certified EHR technology.

Our security and privacy related policies and protections are extensive and complex, but in the self-service materials we provide a high-level overview of security and privacy information.

Are there any CMS exclusions for this measure?

None.

Anything else I should know?

You can use the following 3rd party materials and references to satisfy the requirements of this measure.

athenahealth
there is a better way

Fulfilled Outside of athenaNet:
Security Plan

Security "Self-Service" Tools

You can utilize the following "self-service" tools to navigate the requirements of the security assessment measure. In this set of tools, you will find:

- Security and privacy reference sites provided by The U.S. Department of Health and Human Services (HHS)
- A summary of athenahealth Security and Privacy policies
- A summary of athenahealth's Compliance Program
- A 3rd party reference article entitled "Why, how, and when to conduct an information security risk analysis" by Feisal Nanji of Techumen, LLC, an advisory firm providing services to secure health information.
- A 3rd party "Sample HIPAA Risk Assessment" provided by Techumen, LLC, an advisory firm providing services to secure health information.

HHS Security and Privacy Reference Sites

Summary of the HIPAA Security Rule on the HHS security website

This is a summary of key elements of the Security Rule including who is covered, what information is protected, and what safeguards must be in place to ensure appropriate protection of electronic protected health information (e-PHI). Because it is an overview of the Security Rule, it does not address every detail of each provision.

http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

Security Rule Guidance Material

In this section, you will find educational materials to help you learn more about the HIPAA Security Rule and other sources of standards for safeguarding e-PHI.

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

Additional Support Option

The government takes security and privacy seriously. To gain a sense for what this measure entails, you can review the 3rd party documents that follow. athenahealth strongly encourages you to complete the requirements of this measure as soon as possible. For additional support in navigating the requirements of the security analysis, you may wish to contact Techumen Security Advisory, a trusted security consultant and the provider of the helpful resources included in this guide.

For more information about Techumen services, please email feisal@techumen.com.

You may also choose to work with another consultant or Regional Extension Center (REC) that can provide security analysis support.

athenahealth
there is a better way

athenahealth Security and Privacy

As a HIPAA covered entity, and with a mission to be the most trusted business service to medical practices, athenahealth takes the security and privacy of health information very seriously. Our security and privacy related policies and protections are extensive and complex, and are fully outlined in our HIPAA Statement of Security Standards Compliance.

High-level features of our compliance program include:

- Written standards
- Staff empowerment through training, metrics-based variable compensation, and formal connection of compliance to performance evaluations
- Multiple channels for employees to report possible non-compliance or systemic errors
- Technical controls
- Regular system and process reviews
- Regular audit of our overall compliance effort, including external audits
- Formulation of corrective plans to address any instances of non-compliance

athenaNet's web-based, ASP model addresses information security as a priority and is focused on protecting the confidentiality, integrity, and availability of data for our physician clients. This model offers unique security advantages over traditional software systems in a number of ways.

Confidentiality

- Industry standard SSL/TLS encryption of data in transit from the client network to athenaNet®
- Encrypted backup tapes using industry standard LTO-4 hardware encryption
- Servers are physically isolated and secured within a state-of-the-art Tier 4 data center
- Each client's data is logically isolated from that of all other clients
- Ability to restrict access to a practice's data to connections from their network

Integrity

- Ability to trace every change made to a record back to the responsible individual
- Routine updates are made continuously across the athenahealth network — including bug fixes, security patches, and improved documentation — so practices always have the most updated features available

Availability and Accessibility

- Secure access to client data from anywhere in the US where a computer and Internet connection is available
- Offsite storage of data backups using Iron Mountain, which "protects and stores more records for more customers than any other company in the world"
- We manage all backups so clients don't have to, including ongoing monitoring of the backup process via our Network Operations Center (NOC)
- Redundancy and Response Planning for Disaster Recovery and Business Continuity
- Internet accessibility using high-bandwidth circuits from multiple providers means there is no single point of failure
- athenaNet is built on industry-standard hardware and software from top-tier vendors, including Oracle, Dell, IBM, EMC, Red Hat, Apache, Enterasys, Cisco, Juniper

athenahealth
there is a better way

athenahealth Compliance Program

athenahealth explicitly undertakes the obligation to maintain an effective Compliance Program consistent with the relevant guidelines published by the Office of the Inspector General of the Department of Health and Human Services. We maintain this Program with all of the elements listed by the OIG, including, among other things: a full-time Compliance Officer (Chief Compliance Officer); an active Compliance Committee with overall responsibility for the Program; written compliance plan; written policies and procedures designed to address areas and activities of risk within the company; continuing education of employees in compliance issues conducted by the Compliance Department on a company-wide basis; and special manager level training and department-wide training in key operational areas, evaluation of compliance risks and review of company activities for compliance, a reporting system, active investigation of compliance issues, and remediation/appropriate discipline with respect to compliance failures.

HIPAA Compliance

athenahealth has spent a considerable amount of time, effort and resources to develop the following programs and systems to ensure compliance with the key HIPAA standards and requirements:

HIPAA Standard Transactions

Regulations adopted under HIPAA require HIPAA covered entities to transmit and receive certain electronic transactions in standard formats (the "Transactions Rule"). athenahealth is a health care clearinghouse, and therefore a covered entity under HIPAA. As an early adopter of the HIPAA required transaction formats, athenahealth provides its customers the benefit of an industry-leading Transactions Rule compliance program.

All information needed for HIPAA compliant transactions is fully integrated into athenaNet. This benefits customers by embedding HIPAA transaction requirements automatically into the fabric of the revenue cycle workflow, from patient scheduling through payment posting.

HIPAA Privacy Rule

The Privacy Rule applies to athenahealth both as a covered entity and as a Business Associate of its customers. athenahealth has established a Privacy Rule compliance program to ensure that PHI is used or disclosed only pursuant to Privacy Rule requirements, and that only the minimum necessary PHI is used or disclosed.

HIPAA Security Rule

athenahealth has taken the following steps to comply with the Security Rule:

- **Security Rule Risk Management Plan** — athenahealth has performed a risk analysis pursuant to the Security Rule, and has prepared a risk management plan in which it has identified the measures in place to ensure the confidentiality, integrity, and availability of ePHI maintained by athenahealth.
- **Statement of Security Measures** — athenahealth makes a statement of its security measures available to customers upon request. The statement details the physical, administrative, and technical measures currently in place with respect to athenaNet and athenahealth's corporate information systems, including, without limitation, facility and network access controls, encryption, intrusion detection and prevention, data backup, and disaster recovery measures.

APPEARING IN "COMPLIANCE TODAY" APRIL 2011 ISSUE
(A MONTHLY PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION)

Why, how, and when to conduct an information security risk analysis

By Feisal Nanji

Editor's note: Feisal Nanji is the Executive Director of Techumen, LLC, an advisory firm providing services to secure health information, in New York City. He can be reached at feisal@techumen.com.

Under the Health Insurance Portability and Accountability Act (HIPAA) Security Rule all electronic protected health information (e-PHI) created, received, maintained, or transmitted by a "covered entity" is subject to the Security Rule. If we assume that information technology powers modern health care, then it stores or disseminates most everything an entity might know about a patient. Thus, e-PHI security and privacy is fundamental and paramount.

The Security Rule requires entities to evaluate risks and vulnerabilities in their technology environments and to implement reasonable and appropriate security measures to protect e-PHI. The Office for Civil Rights (OCR), the security watchdog for the Department of Health and Human Services (DHHS), in particular, is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule.[1] The OCR is also the body responsible for ensuring that covered entities are complying with the intent of the Security Rule. From a compliance perspective then, it may seem especially wise to take heed to what the OCR is saying.

In its first guidance released on July 14, 2010,[2] the OCR states "A risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information."

In short, an information technology risk analysis is the fundamental security cornerstone the DHHS expects covered entities to meet. As the OCR ratchets up its compliance activities, as it has promised to do after the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act, covered entities who have not conducted an adequate risk analysis must be prepared to face the OCR's wrath.

How to do a risk analysis?

A risk analysis using a risk-based approach is the very foundation from which to build your information security compliance program. Without this baseline, your organization is swimming aimlessly.

The OCR goes on to stress in its Guidance on Risk Analysis:

> We note that some of the content contained in this guidance is based on recommendations of the National Institute of Standards and Technology (NIST). NIST, a federal agency, publishes freely available material in the public domain, including guidelines. Although only federal agencies are required to follow guidelines set by NIST, the guidelines represent the industry standard for good business practices with respect to standards for securing e-PHI. Therefore, non-federal organizations may find their content valuable when developing and performing compliance activities.

So in short, OCR "suggests" that a covered entity might use the NIST risk-based approach for doing a risk analysis. Our view is that when CMS "suggests" something, it very much is like God telling you to do so. "Suggestion" is merely loosely worded as an imperative. Of course, other good risk frameworks exist, such as Control Objectives for Information Technology (COBIT) developed by the Information Systems for Auditing and Control Association (ISACA), or Octave developed by the CERT institute at the Carnegie-Mellon University. These frameworks may be used, but why bother? The NIST guidance, as provided in its Special Publication 800-30, is excellent, thorough, and easily tailored for small, medium, and large covered entities.

NIST's risk assessment methodology encompasses nine primary steps. Considerable detail is available in NIST's Special Publication 800-30. For this article however, it is appropriate to provide an overview of each of these nine steps.

1. **System characterization.** To fully understand your technology risk, you must understand key technology components in your infrastructure. These could be applications, hardware, operating systems, laptops, and mobile devices. In other words pretty much anything that receives, stores, or transmits information is in play.

2. **Threat Identification.** Threats can be highly specific and discrete and will usually be based on threat motivation and capability. In general, however, threats can be divided into three types:
   - Human threats created or instigated by human beings
   - Environmental threats caused by what insurance companies term "Acts of God"
   - Natural threats that arise from the inherent nature of information systems

3. **Vulnerability Identification.** Your systems will be vulnerable to a wide range of these threats, but what exactly are your systems? They could be described as applications, databases, networks, and amalgams of these. So step 1 (i.e., a "system characterization" or inventory of how your information flows within your organization) is vital. If your systems have been identified well, vulnerability identification becomes much easier to do.

4. **Controls Analysis.** Controls analysis allows an organization to assess the capabilities of your existing set of controls to meet your environment's needs. It does this by helping you identify any existing policies and procedures or standards that may be in violation. Controls are typically described as one of three types:
   - Preventative—lower the likelihood of the threat exercising the vulnerability;
   - Mitigating—lower the impact if the threat exercises the vulnerability; or

- Detective—alert management that the threat has exercised the vulnerability.

  Thus, controls will be technology or processes based, or involve interactions among people. Because many controls safeguard against multiple vulnerabilities, it is usually easier to keep track of multiple instances of a control than to attempt to define and consolidate an "underlying control".

5. **Likelihood determination.** The risk assessment team should use their best judgment to assign likelihoods, considering the threat motivation and ability, the nature of the vulnerability, and the current and planned controls. We suggest that a risk assessment methodology use three tiers to determine likelihood:
   - **High:** The threat will successfully exercise the vulnerability more than once a year
   - **Medium:** The threat will successfully exercise the vulnerability less than once a year, but more than once every three years
   - **Low:** The threat will successfully exercise the vulnerability less than once every three years.

   The output of this step of the risk assessment process is a likelihood determination for each threat-and-vulnerability pair facing the system or systems undergoing the risk assessment

6. **Impact analysis.** In the absence of any historical data, the risk assessment team should use their best judgment to analyze that impact, considering for each system the effects of lost confidentiality, integrity, or availability, and the effect of any current or planned mitigating controls. For a recent client, we suggested a risk assessment methodology that uses three tiers to determine impact:
   - **High:** The impact will cost more than 0.1% of covered entity revenue in financial outlays, require more than 400 man-hours to repair, endanger patient safety, or damage a covered entity's reputation for security.

- **Medium:** The threat will cost more than 0.01% of revenue in financial outlays or require more than 40 man-hours to repair.
- **Low:** The threat will cost less than 0.01% of revenue or require less than 40 man hours to repair.

7. **Risk determination.** Risk determination is a combination of the impact rating and the likelihood determination. We suggest a three-tiered matrix to quickly make decisions (see table 1). Response speed is critical when an incident occurs, and having a ready way to gauge risk is therefore instrumental.

Table 1: Risk matrix

	Likelihood		
Impact	High	Medium	Low
High	High	High	Medium*
Medium	High	Medium	Low
Low	Medium	Low	Low

The area marked with an asterisk (*) is potentially problematic; these are low likelihood, high impact events that are, by nature, difficult to predict. As part of the risk management process, the Compliance group, IT Security Committee, or the Audit Committee should review all risks assigned to this quadrant to determine if the risks have been appropriately ranked, and if additional controls are needed.

8. **Control recommendations.** Based on the determination of risk, your organization will need a road map for planning controls for future implementation. Through this process, your management team can make fundamental decisions to either accept each risk as it stands or alleviate some of the risk by imposing additional controls. This is an especially useful exercise, because it covers approvals, scheduling, and budgeting for additional control implementation.

9. **Results documentation.** Finally, all of this effort must be documented. As compliance officers who have gone through frequent audits, you know the

value of excellent documentation. This, therefore, is a must and should be considered the capstone of your work. A readily available, well written, and thoughtful document that describes your entire risk analysis process will go a long way to assuage any auditor.

When to conduct a risk analysis

Risk occurs when change happens. As a compliance officer you should require a risk assessment over a period of time when enough technology change has occurred.

The beauty about doing an annual risk assessment is that it becomes part of the compliance process; that is, the risk assessment can be merely updated as an addendum and not as an overbearing intrusion that is upsetting to staff and patients. A regular review of your risk posture is what is required to protect e-PHI. Too many new threat vectors and vulnerabilities are introduced into our information environments each day. We all need a reasoned, systematic, and regular approach to do good work.

---

[1] 45 C.F.R. §§ 164.302 – 318

[2] Office of Civil Rights: Guidance on Risk Analysis Requirements under the HIPAA Security Rule. July 14, 2010. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

Sample HIPAA Risk Assessment

Smith & Associates, P.C.

December 2, 2009

Contents

Introduction

In order to better protect our patients' sensitive information, and to comply with the Health Insurance Portability and Accountability Act (HIPAA), Smith & Associates conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic protected health information it holds. This assessment was initially performed on November 12, 2008, and will be updated annually by the Head of IT.

Scope

The assessment covered all systems, people, and processes at the Stamford, New Haven, and Fairfield offices. It also covered the key third parties of AT&T, our internet provider, Quest Corp, which handles our lab operations, and ABC Property Management, which owns and operates the Stamford office building.

Definitions

Electronic Personal Health Information (PHI): Individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to any of the following:

- The past, present or future physical or mental health or condition of an individual
- Provision of healthcare to an individual
- Payment for the provision of healthcare to an individual

If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered individually identifiable health information. Elements that make health information individually identifiable include, but are not limited to, the following:

- Name
- Telephone/fax number
- E-mail address
- Social Security number
- Driver's license number
- Internet address
- Any other unique identifying number characteristic or code

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally or intentionally) and result in a security breach to PHI.

Threat: The potential for an event or and individual to exercise a specific vulnerability.

Risk: The impact on Smith & Associates, considering (1) the probability that a particular threat will exercise a particular vulnerability and (2) the resulting impact if this should occur. Risk = Threat X Vulnerability X Cost

Control: A measure – technical or manual – of reducing the risk to Smith & Associates' PHI.

Risk Assessment Approach

The risk assessment was performed by George Lee, MD, Brad Wallace, Head of IT, and Lucille Taylor, Practice Administrator. The participants used their knowledge of Smith & Associates' operations, their expertise in the IT and medical fields, and interviews with other Smith & Associates employees to perform the risk assessment. Information provided by the DEF Insurance Company, the Smith & Associates' insurance carrier, was used to evaluate the likelihood of natural and environmental threats; the team used its intelligence, guided by experience, to evaluate the likelihood of man-made threats. The list of possible impacts was then circulated to all Smith & Associates employees to learn any impacts that the team may have overlooked. Vulnerability information was taken from the National Vulnerability Database at the National Institute for Standards and Technology (NIST).

The likelihood of particular threats, and their impact on the patients' information, was assessed on a qualitative Low-Medium-High scale assigned by the risk assessment team where no historical information existed. A threat that had occurred more than once in the past five years was given a likelihood of "High", and that had occurred once in the past five years was given a likelihood of "Medium".

Asset Inventory

The Smith & Associates systems (hardware and software) that store or handle patient ePHI are listed below. For a complete network diagram, consult the document "Smith & Associates Network Diagram" on the corporate intranet at http://intranet.smithmd.com/IT/Network_Diagram.vsd.

Stamford Office:

- Server1.smithmd.com – eClinicalWorks 8.0 (Practice Management and EMR), Quickbooks Pro 2007, Miscellaneous shared files (U: Drive)
- Server2. smithmd.com – Microsoft Exchange 2003
- Server3. smithmd.com – Microsoft Windows Server 2003 Terminal Services
- Quest.smithmd.com – Lab results from Quest. One-way interface only; no data goes to Quest.
- Stamfordswitch.smithmd.com : Dell PowerConnect 5448 48 Port Managed Gigabit Ethernet Switch
- stamfordfw.smithmd.com: Sonicwall NSA 240 VPN/Firewall
- 30 Dell workstations, 22 running Windows XP and 8 running Windows 2000
- AT&T T-1 Internet connection
- Cablevision backup internet connection (hot swap, currently unconnected)

Fairfield Office

- Fairfieldsw.smithmd.com: Sonicwall NSA 240 VPN/Firewall
- Fairfieldswitch.smithmd.com: Dell PowerConnect 5424 24 Port Managed Gigabit Ethernet Switch
- 10 Dell workstations, all running Windows XP
- AT&T – 768K SDSL Internet connection

New Haven Office

- Newhavenfw.smithmd.com: Sonicwall NSA 240 VPN/Firewall
- newhavenswitch.smithmd.com: Dell PowerConnect 5424 24 Port Managed Gigabit Ethernet Switch
- 10 Workstations, 8 running Windows XP and 2 running Windows 2000
- AT&T – 768K SDSL Internet connection

Potential Threats and Vulnerabilities

Threats, vulnerabilities, likelihood, and impacts were developed by the methodology discussed in "Risk Assessment Approach", above. The Risk Rating was assessed via the following table:

Threat Likelihood	Impact		
	High	Medium	Low
High	High	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Identified threats and vulnerabilities are below. Separate risks were rated where appropriate.

Threat	Vulnerability	Likelihood Rating	Impact Rating	Risk Rating
Flood	• Some workstations, practice-wide, are placed on the floor and/or not enclosed.	Low	Medium: Workstations and other office equipment could be destroyed.	Low
Electrical storm	• The computer room in the Stamford office lacks an adequate surge protector for all the equipment placed on it.	Medium	High: Servers could be destroyed and data lost.	High
Blizzard	• Not all workers can operate remotely in the event roads are closed by snow.	Medium	Medium: Employees could not get to work.	Medium
Hurricane	• Not all workers can operate remotely in the event roads are closed. • The Fairfield and New Haven offices lack generator backup to operate if local power is unavailable.	Low	• Medium: Employees could not get to work. • Medium: The office could not operate.	Low
Power Failure	• The Fairfield and New Haven offices lack generator backup to operate if local power is unavailable. • The computer room in the Stamford office lacks a UPS that would enable a graceful shutdown on computer equipment.	Medium	• Medium: The office could not operate. • High: Data could be lost or corrupted.	• Medium • High

Threat	Vulnerability	Likelihood Rating	Impact Rating	Risk Rating
Electrical Fire	• The computer room in the Stamford office lacks a fire suppressant system. • All offices are equipped with a "wet" fire control system.	Medium	• High: Data could be lost or corrupted. • Medium: The office could not operate.	High
Theft	• Practice-wide, some computers are not locked down or otherwise physically secured. • USB keys in use are not encrypted.	High	• High: Data and equipment could be stolen. • High: Data could be stolen or lost.	High
External Cybercrime	• Some computer software on both servers and workstations is outdated. • Some computer software has un-patched vulnerabilities. • DHCP is not used on internal machines at the Fairfield and New Haven offices. • The SonicWall in the New Haven office is running outdated firmware that has several published vulnerabilities. • External-facing machines in the Stamford office are not segregated from the internal network in a DMZ. • The VPN connection in the Stamford office users a weak encryption scheme. • User passwords are weak practice-wide. • User passwords are not changed regularly, practice-wide. • VPN connectivity does not use two-factor authentication.	High	High: Data could be lost or stolen; operations could be impacted or impossible.	High

Threat	Vulnerability	Likelihood Rating	Impact Rating	Risk Rating
Internal Fraud	• Administrative passwords are written down in an unlocked drawer. • One individual (Brad Wallace) is responsible for reviewing system activity. • All Smith & Associates employees have access to PHI, regardless of job function.	Low	High: Data could be stolen, disclosed, or otherwise improperly used.	Medium
Malware	• The anti-virus software in use only updates daily.	High	Medium: Operations could be negatively impacted due to recovery efforts.	High
Phishing	• Communication practices with patients have not been established and communicated to patients. • Smith & Associates staff are occasionally clicking on suspect emails and other potentially fraudulent links.	High	Low: Patients or staff could be fooled.	Medium
Spamming	• The Exchange server lacks spam controls.	High	Low: Mail delivery could be slowed.	Medium
Accidental Loss of PHI	• Backups are not taken daily for all PHI, practice-wide.	High	High: PHI could be lost or corrupted.	High
Accidental Corruption of PHI	• A single user is responsible for entering new patient information at the Fairfield and New Haven offices.	Low	High: PHI could be corrupted.	Medium
Accidental Disclosure of PHI	• USB keys are in use to transport information, practice-wide. • Laptops occasionally contain PHI and are taken out of offices practice-wide. • Shredders or other secure paper disposal are not in use at the Fairfield office. • Secure disposal procedures do not exist for electronic storage media. • PHI is occasionally disclosed over the telephone.	Medium	High: PHI would be disclosed.	High

Threat	Vulnerability	Likelihood Rating	Impact Rating	Risk Rating
Failure of a Key Vendor	• The Fairfield and New Haven offices lack backup Internet connectivity. • There is no backup to the Quest system in the Stamford Office.	Low	High: Operations would be affected.	Medium

Risk Assessment Results

Smith & Associates management has decided to assume the risks identified as "Low" in this assessment. The annual review of the assessment will specifically include information that may move a "Low" risk to a "Medium" or "High" risk. The compensating controls and associated action plan for each High or Medium risk is listed below.

Risk #	Threat / Vulnerability	Risk Rating	Compensating Control(s)	Action Plan
1	Electrical storm: The computer room in the Stamford office lacks an adequate surge protector for all the equipment placed on it.	Medium	None.	Implement a surge protector that will protect the equipment against power fluctuations.
2	Blizzard: Not all workers can operate remotely in the event roads are closed.	High	Some users have VPNs.	Edit the Business Continuity Plan to ensure that all essential personnel have remote access to perform their jobs.
3	Power Failure: The Fairfield and New Haven offices lack generator backup to operate if local power is unavailable.	Medium	None.	Edit the Business Continuity Plan to cover the scenario of a power outage in the Fairfield and New Haven offices.

Risk #	Threat / Vulnerability	Risk Rating	Compensating Control(s)	Action Plan
4	Power Failure: The computer room in the Stamford office lacks a UPS that would enable a graceful shutdown on computer equipment.	High	None.	Implement a UPS that will provide enough backup power for a graceful shutdown of the equipment.
5	Theft: Practice-wide, some computers are not locked down or otherwise physically secured.	High	There are locks on the office doors.	Purchase laptop cables for laptop computers. When funds permit, install an alarm system.
6	Theft: USB keys in use are not encrypted	High	None.	Implement Symantec's End-point Protection for portable media.
7	External Cybercrime: Some computer software on both servers and workstations is outdated.	High	There is a firewall between all computers and the internet.	Implement auto-update on workstations and verify success weekly. Implement a process to test and update server software once a month.
8	External Cybercrime: Some computer software has un-patched vulnerabilities.	High	There is a firewall between all computers and the internet.	Implement a vulnerability management program: Sign up for alerts, test patches during off-hours, and implement whenever the vendor recommends applying the patch.
9	External Cybercrime: DHCP is not used on internal machines at the Fairfield and New Haven offices.	High	There is a firewall between all computers and the internet.	Implement a DHCP server and use for all workstations.

Risk #	Threat / Vulnerability	Risk Rating	Compensating Control(s)	Action Plan
10	External Cybercrime: The SonicWall in the New Haven office is running outdated firmware that has several published vulnerabilities.	High	None.	Upgrade the firmware to the latest version. Sign up for a vulnerability mail list to receive notice of future vulnerabilities.
11	External Cybercrime: External-facing machines in the Stamford office are not segregated from the internal network in a DMZ.	High	There is a firewall between all computers and the internet.	Move external-facing machines to a logically segregated network; implement the appropriate network access rules on the screening router.
12	External Cybercrime: The VPN connection in the Stamford office users a weak encryption scheme.	High	VPN traffic is typically brief and infrequent.	Upgrade user's remote connectivity software to the most recent version, which supports strong encryption. Disable weak encryption on the VPN server.
13	External Cybercrime: User passwords are weak practice-wide.	High	None.	Implement strong passwords: 8 characters, mixed-case, one non-alphanumeric character.
14	External Cybercrime: User passwords are not changed regularly, practice-wide.	High	None.	Enable password changing every 90 days on the Windows domain, and prohibit the use of the past four passwords.
15	External Cybercrime: VPN connectivity does not use two-factor authentication.	High	Passwords are required for VPN access.	Once strong, regularly changed passwords are implemented, no further action needed.

Risk #	Threat / Vulnerability	Risk Rating	Compensating Control(s)	Action Plan
16	Internal Fraud: Administrative passwords are written down in an unlocked drawer.	Medium	The password notebooks location is not publicized.	Lock the drawer containing the password notebook. Identify two people to obtain access to it in the event of an emergency; give those people keys.
17	Internal Fraud: One individual (Brad Wallace) is responsible for reviewing system activity.	Medium	None.	Identify a second person to weekly review administrator and user actions on the Windows domain and on the EMR system.
18	Internal Fraud: All Smith & Associates employees have access to PHI, regardless of job function.	Medium	None.	Segregate users by job function and remove access to PHI for those non-clinical personnel.
19	Malware: The anti-virus software in use only updates daily.	High	None.	Configure the AV software to update every four hours.
20	Phishing: Communication practices with patients have not been established and communicated to patients.	Medium	None.	Inform all patients that we will not disclose PHI over email or telephone, and that we will ask them to verify communications we send to them.
21	Phishing: Smith & Associates staff are occasionally clicking on suspect emails and other potentially fraudulent links.	Medium	The AV software should catch most malicious code.	During annual HIPAA training, remind staff not to click on any suspicious emails.

Risk #	Threat / Vulnerability	Risk Rating	Compensating Control(s)	Action Plan
22	Spamming: The Exchange server lacks spam controls.	Medium	None.	Implement the real-time blacklist option (RTBL) in Exchange.
23	Accidental Loss of PHI: Backups are not taken daily for all PHI, practice-wide.	High	Most PHI does not change frequently. Full backups are done weekly Information can be retrieved from multiple sources.	Perform a nightly full backup of all PHI. Mirror any hard drives containing PHI.
24	Accidental Corruption of PHI: A single user is responsible for entering new patient information at the Fairfield and New Haven offices.	Medium	The patient will notice any errors in his/her information and speak up.	Ask the patient to verify information before leaving the office.
25	Accidental Disclosure of PHI: USB keys are in use to transport information, practice-wide.	High	None.	Prohibit staff from placing PHI on USB drives.
26	Accidental Disclosure of PHI: Laptops occasionally contain PHI and are taken out of offices practice-wide.	High	None.	Prohibit staff from placing PHI on laptops.
27	Accidental Disclosure of PHI: Shredders or other secure paper disposal are not in use at the Fairfield office.	High	Paper is recycled by the city.	Purchase a shredder and require staff to use it to dispose of PHI.

Risk #	Threat / Vulnerability	Risk Rating	Compensating Control(s)	Action Plan
28	Accidental Disclosure of PHI: Secure disposal procedures do not exist for electronic storage media.	High	None.	Use DiskErase before disposing of storage media.
29	Accidental Disclosure of PHI: PHI is occasionally disclosed over the telephone.	High	The patient's identity is verified before disclosing information.	Instruct staff not to disclose any PHI over the telephone. Inform patients of the new policy.
30	Failure of a Key Vendor: The Fairfield and New Haven offices lack backup Internet connectivity.	Medium	A Wi-Fi signal is available for poaching from other businesses near the New Haven office.	Update the Business Continuity Plan to include the scenario of an AT&T outage.
31	Failure of a Key Vendor: There is no backup to the Quest system in the Stamford Office.	Medium	None.	Update the Business Continuity Plan to include the scenario of a Quest outage.

Discussion of HIPAA Addressable Safeguards

The Risk Assessment included consideration of all the safeguards identified as "addressable" in HIPAA. The following safeguards were deemed to not be "reasonable and appropriate", based on the unique circumstances of Smith & Associates:

Clause	Safeguard	Rationale	Alternative
164.308(a)(7)(i): Contingency Plan.	Applications and data criticality (A): Organizations must assess the relative criticality of specific applications and data in support of other contingency plan components. This means organizations must think through the prioritization of their applications in the event of the disaster. This will reduce confusion and risk to the EPHI during a disaster.	All applications in use are equally critical and can be restored in a reasonable timeframe; prioritization is not needed.	We will include all business applications in our Business Continuity Plan.
164.310(a)(1): Facility Access Controls.	Maintenance records (A): Organizations must document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors and locks).	Building management maintains this information; it is unnecessary for Smith & Associates to do the same.	N/A
164.310(d): Device and Media Controls.	Data backup and storage (A). The organization must create a retrievable, exact copy of EPHI, when needed, before movement of equipment.	Equipment, to date, has not been moved and no backup has been needed.	N/A

Clause	Safeguard	Rationale	Alternative
164.312(a)(1): Access Control.	Encryption and decryption (A): Organizations must implement a mechanism to encrypt and decrypt EPHI. This addressable specification, on the other hand, may prove to be unduly burdensome for most organizations and may meet the justification that it is an unreasonable requirement in their organization.	The physical, network, and administrative controls around PHI provide adequate security; encrypting PHI at rest would be unduly burdensome.	N/A

Summary

Smith & Associates management accepted the Risk Assessment, and authorized resources for executing on the Action Plans recommended, on December 2, 2009. As this is the first Risk Assessment performed, there are no prior actions that need comment.

Review History

In accordance with HIPAA, this Risk Assessment will be reviewed and updated annually. The Review History is below.

Date	Reviewer	Initials	Edits