

Health Care Compliance Association

protiviti

## CYBERSECURITY CONSIDERATIONS & RISK ANALYSIS PROCESSES

27th Annual  
**Compliance Institute**  
MARCH 26-29, 2017  
NATIONAL HARBOR, MD | CHARLOTTED NATIONAL

*Protiviti's Portion of the joint session:  
"HIPAA COMPLIANCE THAT ADDRESSES THE RISKS OF TODAY AND WILL GROW WITH YOU IN THE FUTURE"*

---

---

---

---

---

---

---

---

---

---

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AAE. Protiviti is not bonded or registered as a public accounting firm and does not bear opinions on financial statements or other attestations services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

### THE THREAT IS REAL

89% of healthcare organizations surveyed have suffered **at least one** data breach in the **last 2 years**

- 45% of CEs have experienced more than five data breaches over the past 2 years
- 61% of BAs experienced data breaches
- Data breaches could be costing the U.S. healthcare industry an average of \$6.2 billion annually
- The average economic impact of data breaches per organization is \$2.2 million.

Source: Sixth Annual Study on Patient Privacy & Security of Healthcare Data. Ponemon Institute, May 2016.

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AAE. Protiviti is not bonded or registered as a public accounting firm and does not bear opinions on financial statements or other attestations services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

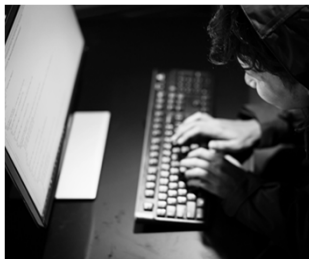
---

### THE THREAT IS REAL

Criminal attacks are now the number-one cause of data breaches (cyber-attacks, malicious insiders, and/or paper medical file theft)

Attacks are targeting medical files and billing / insurance records

CEs say 48% of medical identity theft's root cause was an unintentional employee action (phishing, social engineering, etc.).



© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AAE. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

### THE THREAT IS REAL

Medical Information is sold on the black market typically at a premium, reports range widely on the actual cost, but they go for well above the cost of stolen credit card info. An interactive map of healthcare breaches by number of occurrence can be found at the World Privacy Forum website.

#### Healthcare IT News

Privacy & Security

#### Cybercriminals to launch more ransomware attacks as black market price of health data drops

Executives at the World Privacy Forum and Institute for Critical Infrastructure Technology said that the availability of EHR data is outpacing demand, which means that cybercriminals have to undertake more attacks to steal the same amount of money.



By Jessica Davis | October 10, 2016 | 9:27 AM

SHARE 217

Source: <http://www.worldprivacyforum.org/medicalidentitytheft.html>

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AAE. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

### AREA OF SCRUTINY



⚠ Deficient Risk Analysis! ⚠

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AAE. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

**ENFORCEMENT**

Phase II will mostly consist of "desk audits," but some will be selected for an on-site more comprehensive audit, starting in 2017

All entities are eligible for selection for the on-site audits EVEN those who have already gone through a "desk audit"

A report of the summarized findings will be created and made available sometime after the conclusion of the planned audits in 2017

**Desk Audit Scope**

- Privacy – Notice of Privacy Practices (does not apply to BAs)
- Breach Notification – Timing and Content of Breach Notifications or Breach Risk Assessments
- Security – Risk Analysis and Risk Management

**Audit Protocols – Updated and available now**

- <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html>

7 © 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners. protiviti

---

---

---

---

---

---

---

---

---

---

**ENFORCEMENT**

Add @hhs.gov as a known address to avoid losing emails in spam

Covered Entities - make sure you have a list of your Business Associates ready

Your documentation should be able to stand on its own because the main interaction with OCR is uploading your documents:

- Can they be understood by an auditor?
- Would they benefit from a narrative that explains them?

Assess against the protocols

- Desk audit focus
- Comprehensive

8 © 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners. protiviti

---

---

---

---

---

---

---

---

---

---

**ENFORCEMENT**

HIPAA compliance reviews and complaint investigations are even more thorough than the Phase II audits

Complaint Investigation – complaint driven

Compliance Review – breach driven

**HIPAA Penalties vs. Settlements**

- OCR most often "settles" and creates "corrective action plans"
- These amounts are vastly reduced compared to what they could enforce through actual civil monetary penalties under the HITECH Act

**Trending Issues**

- Lack of BAA
- BAA not updated after HITECH
- Incomplete or inaccurate Risk Analysis
- Lack of transmission security
- Patching of software
- Audit logs
- Insider threat
- Improper disposal
- Insufficient backup and contingency planning

9 © 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners. protiviti

---

---

---

---

---

---

---

---

---

---

EVALUATION VS. RISK ANALYSIS

<p><b>Evaluation</b></p> <ul style="list-style-type: none"> <li>Gap assessment comparing compliance practices against the individual standards/requirements</li> <li>Guidance may be found at: <a href="http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html">http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html</a></li> </ul>
<p><b>Risk Analysis / Risk Management</b></p> <ul style="list-style-type: none"> <li>Identify and assess risks to all of your ePHI</li> <li>Take action to reduce risks and vulnerabilities to a reasonable and appropriate level</li> <li>Guidance may be found at: <a href="http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html">http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html</a></li> </ul>

10 © 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AAE. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

EVALUATION VS. RISK ANALYSIS

Standard	Requirement	Specification	Detail
Evaluation §164.308(a)(8)	§164.308(a)(8) Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	N/A	N/A

11 © 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AAE. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

EVALUATION VS. RISK ANALYSIS

Standard	Requirement	Specification	Detail
Security Management Process §164.308(a)(1)	§164.308(a)(1)(i) Implement policies to prevent, contain, and correct security violations.	Risk Analysis	§164.308(a)(1)(i)(A) Conduct an accurate and thorough <b>assessment of the potential risks and vulnerabilities</b> to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
		Risk Management	§164.308(a)(1)(i)(B) <b>Implement security measures</b> sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

12 © 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AAE. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

PERFORMING AN EVALUATION

- Discussed earlier today (First Class Solutions, Inc.)
- OCR HIPAA Audit Protocol has been updated
- Foundational & comprehensive starting point
- Significantly enhanced, but still does not guarantee compliance




---

---

---

---

---

---

---

---

---

---

PERFORMING AN EVALUATION

Security Rule Educational Series

HHS's website has a Security Rule Educational Paper Series that provides further clarification to the Security Rule requirements

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

Has links to a number of good reference documents including some developed specifically to clarify the Security Rule

---

---

---

---

---

---

---

---

---

---

PERFORMING AN EVALUATION

2.3 Security Gap Evaluation – Observations and Recommendations Matrix

Standards Requirement	Specification / Detail	Current Control Activities	Gaps / Opportunities / Opportunity	Management's Plan
<b>Information Security Management</b> <b>Security</b> HIPAA 164.308(a)(1) HIPAA 164.308(a)(2) HIPAA 164.308(a)(3) HIPAA 164.308(a)(4) HIPAA 164.308(a)(5)	Risk Analysis (Required) HIPAA 164.308(a)(1)(ii) Conduct an annual risk analysis and thorough assessment of the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	An annual risk analysis is required per the Information Security Risk Management policy that details the approach. The policy requires that the IT Security Administrator provides a report annually detailing the risks to the RBC's information resources and any remediation activities. Risk Policy Information Security Risk Management	Gap: Although a policy exists regarding an annual risk analysis, a software and documented risk analysis does not appear to be performed every year. Opportunity: The current risk analysis is completed and documented on an annual basis in accordance with OCR's and HHS's guidance. An annual risk analysis should meet the one that represents an analysis by the RBC, provided which includes: • Scope of the Analysis • Data Collection • Assets and Document Physical Threats and Vulnerabilities • Assess Current Security Measures • Determine the Likelihood of Threat Occurrence • Determine the Potential Impact of Threat Occurrence • Determine the Level of Risk	TBD

---

---

---

---

---

---

---

---

---

---

**AREA OF SCRUTINY**


While high-level guidance has been issued, there are no baseline standards from the federal government in support of "risk analysis" efforts.

OCR issued "Guidance on Risk Analysis Requirements under the HIPAA Security Rule" on July 14, 2010

- Definitions
- Elements of a Risk Analysis
- 9 pages

NIST SP 800-30 – Guide for Conducting Risk Assessments

- 41 pages



© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/Veterans. Protiviti is not bonded or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

---

---

**ELEMENTS OF A RISK ANALYSIS**

**1. Scope of Analysis**

- An organization's risk analysis should include the potential risks and vulnerabilities to the confidentiality, availability and integrity of all ePHI that an organization creates, receives, maintains, or transmits. (45 C.F.R. § 164.306(a))
  - All ePHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its ePHI.
    - o Hard Drives/USB Drives/Floppy Disks
    - o CD/DVD
    - o Cell Phones/PDAs
    - o Backup Media/Transmission Media
    - o Etc.

**2. Data Collection**

- Identify and document where the ePHI is stored, received, maintained or transmitted. (45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1))
  - Questionnaires, Interviews, Automated Scanning Tools

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/Veterans. Protiviti is not bonded or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

---

---

**AREA OF SCRUTINY**

Scope of your Risk Analysis is a big area for OCR

**Audit protocol**

- Does the entity...conduct an accurate and thorough assessment of the potential risks...to the confidentiality, integrity, and availability of all the ePHI it creates, receives, maintains, or transmits?
- Obtain and review the written risk analysis documentation for:
  - A defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI
- The word "all" appears four different times in this one protocol

**Resolution Agreements**

- Failure to conduct risk analysis and implement risk management plans (MAPFRE 1/18/17 \$2.2m)
- Failure to conduct a thorough risk analysis of all of its ePHI (Lahey Hospital 11/24/2015, \$850k)
- Neither entity had conducted an accurate and thorough risk analysis (New York Presbyterian and Columbia University 5/7/2014, \$4.8m)

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/Veterans. Protiviti is not bonded or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

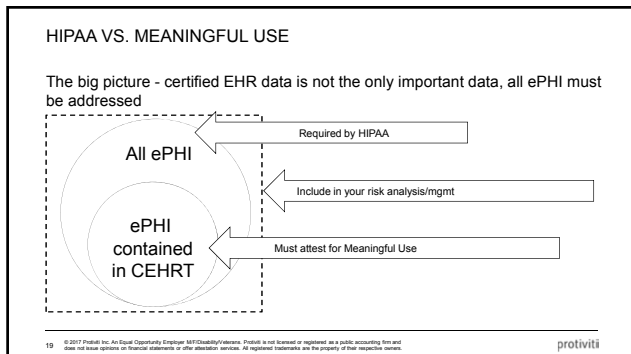
---

---

---

---

---




---

---

---

---

---

---

---

---

---

---

### SCOPE – EXAMPLES

Applications	Asset Types
EHR	<ul style="list-style-type: none"> <li>• Desktops/Laptops</li> <li>• Server</li> <li>• SAN/Disk Array</li> <li>• Backup Tapes</li> <li>• USBs</li> <li>• Medical Devices</li> <li>• Printers</li> <li>• Mobile Devices</li> </ul>
Email	<ul style="list-style-type: none"> <li>• Vendor Cloud</li> <li>• Desktops/Laptops</li> <li>• Mobile Devices (smartphones/tablets/etc.)</li> </ul>
Network Shares	<ul style="list-style-type: none"> <li>• Server</li> <li>• Backup Tapes</li> </ul>
Electronic Voicemail	<ul style="list-style-type: none"> <li>• Server</li> <li>• Backup Tapes</li> <li>• Desktops/Laptops</li> </ul>

© 2017 Protiviti Inc. An Equal Opportunity Employer. All Rights Reserved. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners. protiviti

---

---

---

---

---

---

---

---

---

---

### ELEMENTS OF A RISK ANALYSIS

**3. Identify and Document Potential Threats and Vulnerabilities**

- Identify and document reasonably anticipated threats and vulnerabilities to ePHI. (45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii))
  - Threat – “[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.”
    - o Natural – Floods, Earthquakes, Tornadoes, etc.
    - o Human – Inadvertent data entry, malicious software upload, unauthorized access to confidential data
    - o Environmental – Long term power failure, pollution, chemicals, liquid leaks
  - Vulnerability – “[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.”

© 2017 Protiviti Inc. An Equal Opportunity Employer. All Rights Reserved. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners. protiviti

---

---

---

---

---

---

---

---

---

---

THREAT & VULNERABILITY – EXAMPLES

Assets	Threat	Vulnerability
Desktops, Laptops, Servers, etc.	Malware – theft of sensitive data	Lack of sufficient anti-malware (installed/updated)
Desktops, Laptops, Servers, SAN, etc.	Hacker – theft of sensitive data	Unpatched vulnerabilities in network systems
Desktops, Laptops, Smartphones, USBs, etc.	Burglar/Thief – theft of equipment	Media is not handled and guarded properly
Desktops, Laptops, Smartphones, USBs, etc.	Careless IT personnel – improper destruction/disposal or reuse of media	Media is not properly disposed of
Desktops, Laptops, Servers, SAN, etc.	System Cracker – social engineering	Employees are overly trusting and uneducated/unaware of social engineering tactics

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AAE. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

ELEMENTS OF A RISK ANALYSIS

4. Assess Current Security Measures

- Assess and document the security measures an entity uses to safeguard ePHI (45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1))
  - Documentation – Policy, Procedure, Process, etc.
  - Practice – Physical or logical controls in place

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AAE. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

SECURITY MEASURES – EXAMPLE

Assets	Threat	Vulnerability	Security Measures (Controls)
Desktops, Laptops, Smartphones, USBs, etc.	Burglar/Thief – theft of equipment	Media is not handled and guarded properly	1) Employees are educated to protect the physical security of the device on a yearly basis
Desktops, Laptops, Servers, SAN, etc.	System Cracker – social engineering	Employees are overly trusting and uneducated/unaware of social engineering tactics	1) Employees are educated on social engineering threats yearly 2) Social engineering tests are performed twice a year to assess employee awareness

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AAE. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---



ELEMENTS OF A RISK ANALYSIS

5. Determine the Likelihood of Threat Occurrence

- Document all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability and integrity of ePHI of an organization. (45 C.F.R. §§ 164.306(b)(2)(iv), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii))
  - Threat-source motivation and capability
  - Nature of the vulnerability

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

25 © 2017 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

---

---

---

---

---

---

---

---

---

---

---

---

ELEMENTS OF A RISK ANALYSIS

6. Determine the Potential Impact of Threat Occurrence

- Assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. (45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii))
  - Quantitative vs. Qualitative Assessment
  - Loss of Integrity, Confidentiality, Availability

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources, (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest, or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources, (2) may violate, harm, or impede an organization's mission, reputation, or interest, or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Source: OCR's "Guidance on Risk Analysis Requirements under the HIPAA Security Rule"

26 © 2017 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

---

---

---

---

---

---

---

---

---

---

---

---

ELEMENTS OF A RISK ANALYSIS

7. Determine the Level of Risk

- Assign a risk level based on the average of the assigned likelihood and impact levels. (45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1))
  - Inherent Risk = Likelihood \* Impact
  - Residual Risk = Inherent Risk - Safeguards (Controls)

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

Source: OCR's "Guidance on Risk Analysis Requirements under the HIPAA Security Rule"

27 © 2017 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

---

---

---

---

---

---

---

---

---

---

---

---

RISK DETERMINATION – EXAMPLES

Assets	Threat	Vulnerability	Security Measures (Controls)	Likelihood	Impact	Risk Rating
Desktops, Laptops, Smartphones, USBs, etc.	Burglar/ Thief – theft of equipment	Media is not handled and guarded properly	1) Employees are educated to protect the physical security of the device on a yearly basis	High (5)	High (5)	Critical (25)
Desktops, Laptops, Servers, SAN, etc.	System Cracker – social engineering	Employees are overly trusting and uneducated or unaware of social engineering tactics	1) Employees are educated on social engineering threats yearly 2) Social engineering tests are performed twice a year to assess employee awareness	Moderate (3)	High (5)	High (15)

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AA/AA/AA. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

ELEMENTS OF A RISK ANALYSIS

**8. Finalize Documentation**

- The Security Rule requires the risk analysis to be documented but does not require a specific format. (45 C.F.R. § 164.316(b)(1))

**9. Periodic Review and Updates to the Risk Assessment**

- Conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii))

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AA/AA/AA. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

ELEMENTS OF RISK MANAGEMENT

Risk management is the **implementation of security measures** to sufficiently reduce an organization's risk of losing or compromising its ePHI and to meet the general security standards.

**Example Risk Management Steps**

- Develop and implement a risk management plan [This plan describes what will be done to further mitigate the identified risk.]
- Implement security measures.
- Evaluate and maintain security measures."

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AA/AA/AA. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

RISK MANAGEMENT – EXAMPLES

Assets	Threat	Vulnerability	Controls	Likelihood	Impact	Risk Rating
Desktops, Laptops, Smartphones, USBs, etc.	Burglar/ Thief – theft of equipment	Media is not handled and guarded properly	1) Employees are educated to protect the physical security of the device on a yearly basis	High (5)	High (5)	Critical (25)
Risk Management Plan: Encrypt all devices that may receive ePHI. Implement a MDM Solution to manage these devices. Use the MDM solution to perform monthly inventory checks to see if any devices have gone missing and investigate. Remotely wipe any devices that cannot be located.				Responsible Party: CIO Remediation Date: Est. 10/1/2017		

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AA/VE/AA. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners. protiviti

---

---

---

---

---

---

---

---

---

---

---

---

RISK MANAGEMENT – EXAMPLES

Assets	Threat	Vulnerability	Controls	Likelihood	Impact	Risk Rating
Desktops, Laptops, Servers, SAN, etc.	System Cracker – social engineering	Employees are overly trusting and uneducated or unaware of social engineering tactics	1) Employees are educated on social engineering threats yearly 2) Social engineering tests are performed twice a year to assess the employees awareness	Moderate (3)	High (5)	High (15)
Risk Management Plan: Increase education to occur quarterly through a variety of different avenues. Communicate the results of the social engineering tests to reaffirm the issue with the workforce. Use real-life examples to further enhance awareness.				Responsible Party: Education Team Remediation Date: Est. 12/31/2017		

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AA/VE/AA. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners. protiviti

---

---

---

---

---

---

---

---

---

---

---

---

AREA OF SCRUTINY 

OCR will be looking for evidence that you took action on the identified risks in some form or fashion

<p><b>Audit Protocol</b></p> <ul style="list-style-type: none"> <li>Obtain and review documentation demonstrating the security measures implemented and/or in the process of being implemented as a result of the risk analysis or assessment. Evaluate and determine whether the implemented security measures appropriately respond to the threats and vulnerabilities identified in the risk analysis according to the risk rating and that such security measures are sufficient to mitigate or remediate identified risks to an acceptable level.</li> <li>Have this info documented</li> </ul>
<p><b>HIPAA Penalty Enforcement</b></p> <ul style="list-style-type: none"> <li>February 1, 2017 – OCR levied a \$3.2 million civil money penalty against Children’s Medical Center of Dallas for lack of addressing known security risks.                     <ul style="list-style-type: none"> <li>Encryption was identified as a risk in 2007, was not remediated until 2013</li> <li>Children’s suffered 2 breaches during this time that encryption would have protected against</li> </ul> </li> </ul>

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/AA/VE/AA. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or other attestable services. All registered trademarks are the property of their respective owners. protiviti

---

---

---

---

---

---

---

---

---

---

---

---

**TRENDING RISK AREAS**  
*RISKS TO LOOK FOR IN YOUR ENVIRONMENT*

---

---

---

---

---

---

---

---

**TRENDING RISK AREAS – VENDOR MANAGEMENT**

- Vendors are a key part of many healthcare organization's business processes, but have also been an avenue for compromising of PHI/ePHI.
- Threat: Vendor's are not diligent in their security measures.
- Vulnerability: Vendor's lack of controls may put your data at risk.
- Recommended Controls:
  - Robust contracts and BAAs that specify the requirements to protect the data and implications for failure to do so
  - Vendor management and assessment process up-front and ongoing to assess the controls the vendor has in place. Could be accomplished through:
    - Reviewing SSAE16 SOC Reports (Third party's assessment of controls)
    - Questionnaire to vendor
    - Audits of vendor to test controls effectiveness
  - Process to monitor for new vendor's, working with Contracting/AP/Supply Chain, etc.

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/Veterans. Protiviti is not bonded or registered as a public accounting firm and does not bear opinions on financial statements or other attestations services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---


---

**TRENDING RISK AREAS – MEDICAL DEVICES**

- Threats: Hackers, Patients, Malware, etc.
- Vulnerabilities: Unpatched vulnerabilities, out of date operating systems, default user/admin credentials, weak wireless encryption, etc.
- Recommend Controls:
  - Physically secure devices
  - Segment these devices network segments
  - Regular vulnerability scans
  - Implement a life cycle management program for devices
- Need to be managed throughout the entire life cycle:
  - Planning & Requirements
  - Procurement & Contracting
  - Implementation
  - Maintenance
  - Decommission

**FDA RECALLED:**

- Hospira Symbiq Infusion System – Cybersecurity vuln.
- Alaris Medley Large Volume Pump – Defective part



© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V/Veterans. Protiviti is not bonded or registered as a public accounting firm and does not bear opinions on financial statements or other attestations services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

**TRENDING RISK AREAS – BUSINESS CONTINUITY / DISASTER RECOVERY**

- With the increased reliance on electronic records and applications in the healthcare industry, the more important it is to have proper business continuity/contingency/disaster recovery plans in place.
- Threats: Natural disasters, man-made disasters, cyber attacks, IT changes, etc., etc.
- Vulnerabilities: Proper business continuity and/or disaster recovery (IT) plans are not in place or are not actionable, plans are not tested for readiness, etc.
- Recommended Controls:
  - Detailed Business Impact Analyses to determine key technologies, people, and processes, and required recovery time objectives (RTOs) and recovery point objectives (RPOs)
  - Documented Business Continuity and Disaster Recovery Plans
  - Regular testing of the plans including operationally how workforce would continue functioning without critical applications/network access/etc.
  - Regular testing of the ability to recover critical applications, and the associated timeframe for doing so through different scenarios.

---

---

---

---

---

---

---

---

---

---

---

---

**TRENDING RISK AREAS – SOCIAL ENGINEERING**

- Threats: Attackers External or Internal
- Vulnerabilities: Users not aware of social engineering tactics
- Recommended actions:
  - Education, education, education (upon hire, annual reminders, ad-hoc updates, learning experiences, etc.)
  - Testing of your users, perform phishing efforts, do physical walkthroughs, perform phone calls, etc.
  - Ensure other security controls are strong.
    - Use multi-factor authentication where possible (does not mean two different passwords)
    - Administer least-privilege access (network, apps, devices, etc.)
    - Segment the critical data
    - Perform proactive penetration testing and vulnerability assessments to identify weaknesses and address accordingly
    - Have good backups and a solid and ready Disaster Recovery Plan

---

---

---

---

---

---

---

---

---

---

---

---

**TRENDING RISK AREAS – SOCIAL ENGINEERING**

**HOTEL CONFIRMATION**

Reservation Confirmation: 8288412

For (M/M/AAE)      Month: 01/15      Room: 1000      Rate: \$100.00

Check-in date: Monday, November 7, 2015      Check-out date: Thursday, November 12, 2015

Check-in time: 03:00 PM      Check-out time: 03:00 PM

[Modify your reservation](#)      [Cancel your reservation](#)

**Dear (NAME),**

We are pleased to confirm your reservation. Details about your booking, your itinerary and your confirmation are included below.

Itinerary:

View your hotel itinerary

**DELIVERY NOTICE**

**Your package has been delivered**

Tracking # 89619131219

Ship (M/F) date: Friday, 11/11/15      Delivery date: Wednesday, 11/17/15

Ship from: CA      Ship to: CA

**Shipment Details**

Our records indicate that the following package has been delivered:

Tracking number: 89619131219

Carrier: DHL

Reference: 24490

Delivered to: Location

Service type: First Class

Package type: Your Packaging

Number of pieces: 1

Weight: 2.08 lbs.

Special handling services: Insured at \$1000

---

---

---

---

---

---

---

---

---

---

---

---

TRENDING RISK AREAS – SOCIAL ENGINEERING

PAYMENT NOTIFICATION



SECURE EMAIL



---

---

---

---

---

---

---

---

---

---

TRENDING RISK AREAS – RANSOMWARE

- Threats: Malware, Attackers External and Internal, Social Engineers/Phishing
- Vulnerabilities: Users not aware of threats, poor network security measures, lack of data backups
- Recommended Controls:
  - Education of workforce
  - Testing of network security controls through penetration testing
  - Testing of data backups and disaster recovery readiness
  - Block unnecessary tasks/privileges from users (block office macros, block executable file coming from external domains, restrict administrator tasks on workstations, etc.)
  - Have a plan



---

---

---

---

---

---

---

---

---

---

CLOSING REMARKS

---

---

---

---

---

---

---

---

---

---

### WHAT YOU SHOULD BE DOING TODAY

Take action on the following:

Monitor Phase 2 audit developments and apply lessons-learned.

Ensure sufficient Gap Evaluation and Risk Analysis efforts have been completed.

Periodically test the operating effectiveness of compliance/control activities (not just design).

Remediate identified gaps/risks in a timely manner.

Create documentation/evidence that can stand on its own.

Continue building a "culture of compliance" at your organization!

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions or financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---

### Q&A

---

---

---

---

---

---

---

---

---

---

### CONTACT US

Matt Jackson  
Director  
mattew.jackson@protiviti.com

Phone: 469-374-2479



Matt is a founding member of Protiviti and is a Director in the Dallas office with more than 17 years professional experience providing operational, technology, and regulatory consulting and internal audit services to the healthcare industry. Matt serves as Protiviti's National Healthcare Information Technology Leader as well as Protiviti's HIPAA Solutions Leader. He is a frequent speaker on, and has published various articles related to, internal audit, compliance, and information technology improvement initiatives.

Kevin Dunnahoo  
Senior Manager  
kevin.dunnahoo@protiviti.com

Phone: 972-788-8529



Kevin is a Senior Manager with Protiviti's Dallas office and has more than 9 years of professional experience providing IT consulting and auditing services to the Healthcare industry. Kevin is a member of Protiviti's National Healthcare Practice and is a key lead for HIPAA Security Compliance services. In the Healthcare industry, Kevin has provided value to his clients through his insights and understanding of the HIPAA Security regulations, information security practices, business continuity, and IT audit. Kevin is a certified HCISPP, CISSP, ABCEP, and HITRUST CSF Practitioner, and has also co-authored various Protiviti thought leadership whitepapers specifically related to HIPAA compliance and enforcement.

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions or financial statements or other attestable services. All registered trademarks are the property of their respective owners.

protiviti

---

---

---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

---