How to Complete a HIPAA Security Risk Analysis

Bob Chaput, MA, CISSP, CHP, CHSS
Clearwater Compliance LLC
Bob Chaput
CISSP, MA, CHP, CHSS, MCSE

- President – Clearwater Compliance LLC
- 30+ years in Business, Operations and Technology
- 20+ years in Healthcare
- Executive | Educator | Entrepreneur
- Global Executive: GE, JNJ, HWAY
- Responsible for largest healthcare datasets in world
- Numerous Technical Certifications (MCSE, MCSA, etc)
- Expertise and Focus: Healthcare, Financial Services, Legal

- Member: NMGMA, HIMSS, ISSA, HCCA, ACHE, AHIMA, NTC, ACP, Chambers, Boards

bob.chaput@clearwatercompliance.com | 800-704-3394

http://www.linkedin.com/in/BobChaput
Learning Objectives

- Discuss the explicit Meaningful Use requirement for Risk Analysis with customers and colleagues
- Define key Risk Analysis terms
- Explain the difference between Risk Analysis and Risk Management
- Describe the Specific requirements outlined in HHS/OCR Final Guidance
- Explain a practical risk analysis methodology
- Follow Step-by-Step Instructions for completing a HIPAA Risk Analysis
- Complete an Information Asset Inventory
- Determine risks to information assets
- Explain risk management alternatives
Session Agenda

1. Why Care?
2. Key Risk Analysis Terminology
3. HIPAA Regulatory Requirements
4. How to Get Started
5. Specific, Practical Best Practices
6. Risk Analysis Exercise
Why Should You Care?

1. It’s the law… HIPAA & HITECH!

2. Your stakeholders trust and expect you to do this

3. Your reputation depends on it!
Legal Activity

- BCBS Tennessee to pay $1.5 million in HIPAA settlement
- Sutter Health Hit With $1B Class-Action Lawsuit
- Patient files $20M lawsuit against Stanford Hospital
- TRICARE Health Management Sued for $4.9B
- UCLA Health System Enters into $865K Resolution Agreement & CAP with OCR
- Cignet Health Fined for Violation of HIPAA Privacy Rule: $4.3M
- MGH entering into a resolution agreement; includes a $1 million settlement
- AvMed Health sued over 'one of the largest medical breaches in history'
- Health Net keeps paying for its data breach in 2009... $625K and counting
- WellPoint's notification delay following data breach brings action by Attorney General's office

Lawsuits and Enforcement are on the upswing...
We regret to inform you that, on March 12, Impairment Resources, LLC filed a petition for relief under Chapter 7 of the US Bankruptcy Code in the US Bankruptcy Court for the District of Delaware under case number 12-10850.

March 12, 2012, 12:39 PM ET

Burglary Triggers Medical Records Firm’s Collapse

The New Year’s Eve burglary of a California office building has led to the collapse of a national medical records firm.

Impairment Resources LLC filed for bankruptcy Friday after the break-in at its San Diego headquarters led to the electronic escape of detailed medical information for roughly 14,000 people, according to papers filed in U.S. Bankruptcy Court in Wilmington, Del. That information included patient addresses, social security numbers and medical diagnoses.

Police never caught the criminals, and company executives were required by law to report the breach to state attorneys general and the Department of Labor’s Office of Inspector General. Some of those agencies, including the Department of Labor, are still investigating the matter, the company said in court papers.

“"The cost of dealing with the breach was prohibitive" for the company, Impairment Resources said when explaining its decision to file for Chapter 7 bankruptcy protection. That type of bankruptcy is used most often by companies to shut down and sell off what’s left to pay off their debts.
“Wall of Shame”

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

03-26-2012
• 409 CEs
• 85 Named BAs

~19.2M Individuals
Or State of NY

19.5M

Or State of NY
“...only way to change is through enforcement…”

“...our 5% budget reduction doesn’t change anything…”

“... enforcement revenues will be used for restitution for victims...AND... reinvestment in STRATEGIC ENFORCEMENT…”

“... enforcement will continue and intensify…”

“...we’re moving from complaint-driven to proactive enforcement…”

“... we’re looking for the “whole menu”...get going on training, PnPs and risk analysis…”
OCR Compliance Expectations...

A Culture of Compliance

- OCR aggressively enforcing the HIPAA Privacy and Security Rules
- Covered entities and business associates should have robust HIPAA Privacy and Security compliance programs
- A robust compliance program includes employee training, vigilant implementation of policies and procedures, regular internal audits, and a prompt action plan to respond to incidents
Stage 1 Meaningful Use (MU)

MU = Money Up
EP Meaningful Use - Core

Eligible Professionals' 15 Core Objectives

1. Computerized provider order entry (CPOE)
2. E-Prescribing (eRx)
3. Report ambulatory clinical quality measures to CMS/States
4. Implement one clinical decision support rule
5. Provide patients with an electronic copy of their health information, upon request
6. Provide clinical summaries for patients for each office visit
7. Drug-drug and drug-allergy interaction checks
8. Record demographics
9. Maintain an up-to-date problem list of current and active diagnoses
10. Maintain active medication list
11. Maintain active medication allergy list
12. Record and chart changes in vital signs
13. Record smoking status for patients 13 years or older
14. Capability to exchange key clinical information among providers of care and patient-authorized entities electronically
15. **Protect electronic health information**

<table>
<thead>
<tr>
<th>Meaningful use Stage 1 objective</th>
<th>Meaningful use Stage 1 measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.</td>
<td>Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.</td>
</tr>
</tbody>
</table>

HBMA Healthcare Billing & Management Association
EH & CAH Meaningful Use

EHs and CAHs 14 Core Objectives

1. Use CPOE for medication orders directly entered by any licensed healthcare professional who can enter orders into the medical record per State, local, and professional guidelines.
2. Implement drug-drug and drug-allergy interaction checks.
3. Maintain an up-to-date problem list of current and active diagnoses.
4. Maintain active medication list.
5. Maintain active medication allergy list.
6. Record specific set of demographics.
7. Record and chart specific changes in the certain vital.
8. Record smoking for patients 13 years old or older.
9. Report hospital clinical quality measures to CMS or, in the case of Medicaid eligible hospitals, the States.
10. Implement one clinical decision support rule related to a high priority hospital condition, along with the ability to track compliance with that rule.
11. Provide patients with an electronic copy of their health information (including diagnostic test results, problem list, medication lists, medication allergies, discharge summary, procedures), upon request.
12. Provide patients with an electronic copy of their discharge instructions at time of discharge, upon request.
13. Capability to exchange key clinical information (for example, problem list, medication list, medication allergies, and diagnostic test results), among providers of care and patient authorized entities electronically.
14. **Protect electronic health information**

<table>
<thead>
<tr>
<th>Meaningful use Stage 1 objective</th>
<th>Meaningful use Stage 1 measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.</td>
<td>Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.</td>
</tr>
</tbody>
</table>
What’s The Big Deal?

• **Street cost for a stolen Record**
  - Medical: $50 vs SSN: $1

• **Payout for identity theft**
  - Medical: $20,000 vs Regular: $2,000

• **Medical records can be exploited 4x longer**
  - Credit cards can be cancelled; medical records can’t

---

1. RSA Report on Cybercrime and the Healthcare Industry

---

- Medical Record Abuse consequences
  - Prescription Fraud
  - Embarrassment
  - Financial Fraud
  - Personal Data Resale
  - Blackmail / Extortion
  - Medical Claims Fraud
  - Job loss / reputational
Session Agenda

1. Why Care?
2. Key Risk Analysis Terminology
3. HIPAA Regulatory Requirements
4. How to Get Started
5. Specific, Practical Best Practices
6. Risk Analysis Exercise
Key Terms & Concepts

- Protected Health Information (PHI)
- electronic PHI (ePHI)
- Secured PHI
- Unsecured PHI
- Data Breach
- Encryption
- Destruction
- Safe Harbor
- Security Essentials
- Required versus Addressable

- Risk Management
- Threats
- Vulnerabilities
- Risks
- Risk Analysis
- Qualitative Risk Analysis
- Quantitative Risk Analysis
- Risk Treatment
Protected Health Information

• Protected Health Information (PHI) is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

• PHI is interpreted rather broadly and includes any part of a patient’s medical record or payment history

• ...and, that is linked to personal (18) identifiers
Data Breach

- A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.
Unsecured PHI

• Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable.

• CEs and BAs must only provide the required notification if the breach involved unsecured protected health information.
Encryption

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.¹

¹45 C.F.R. § 164.304 Definitions
Safe Harbor

“This guidance is intended to describe the technologies and methodologies that can be used to render PHI unusable, unreadable, or indecipherable to unauthorized individuals. While covered entities and business associates are not required to follow the guidance, the specified technologies and methodologies, if used, create the functional equivalent of a safe harbor, and thus, result in covered entities and business associates not being required to provide the notification otherwise required by section 13402 in the event of a breach.”

1 DEPARTMENT OF HEALTH AND HUMAN SERVICES 45 CFR Parts 160 and 164 Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information
Risk Analysis

The examination of assets, their threats and vulnerabilities to identify and evaluate risks

... Risk analysis is defining the whole shape of your information security – make sure you do it right!

...
Qualitative Risk Analysis

- Uses scales for assessing impacts and likelihood – e.g. (Low, Medium, High) or (0-5)
- Owner of the asset makes the assessment according to own experience
- Advantages: cheaper, quicker method
- Disadvantage: subjective
Quantitative Risk Analysis

- Uses numerical values:
  - Impacts - $
  - Probability - % within a year

- Advantages:
  - Easier to present to management
  - Much more accurate

- Disadvantages:
  - No data for certain risks
  - Expensive
Risk Analysis “Algebra”

Step 1:
\[ k \div 3 = 4 \]
\[ k = 12 \]

Step 2:
\[ k \div 3 = 4 \]
\[ x_3 = 12 \]

Step 3:
\[ k = 12 \]

Step 4:
\[ \int_0^w u^2 d\Psi(u|i) + w^2 \times [1 - \Psi(w|i)] \]
\[ - w^2 \times [1 - \Psi(w|i)]^2 - \left( \int_0^w u d\Psi(u|i) \right)^2 \]
\[ - 2w \times [1 - \Psi(w|i)] \int_0^w u d\Psi(u|i) \]
What is Risk Management?

Risk = Impact * Likelihood

Goal = Understand What Risks Exist and Into What Category They Fall

Overall Risk Value

Impact

<table>
<thead>
<tr>
<th>HIGH</th>
<th>Medium</th>
<th>High</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDIUM</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>LOW</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>LOW</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td></td>
</tr>
</tbody>
</table>
Threat Sources

1. **Adversarial**
   - Individual-Insider, -Outsider,
     Group-Ad hoc,-Established…

2. **Accidental**
   - Ordinary User, Privileged User

3. **Structural**
   - IT Equipment, Environmental Controls, Software

4. **Environmental**
   - Natural or man-made disaster (fire, flood, hurricane),
     Unusual natural event, Infrastructure failure/outage (telecomm, power)

… An adapted definition of threat Source, from NIST SP *00-30, is “The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability…”
Vulnerabilities

1. Lack of strong password
2. Lack of personal firewall
3. Lack of data backup
4. Lack of policies
5. Failure to follow policies
6. Lack of training
7. Lack of encryption on laptops with ePHI…
8. …and on and on …

NIST Special Publication (SP) 800-30 as “[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.”
Controls Help Address Vulnerabilities

Threat Source
- Burglar who may steal Laptop with ePHI

Vulnerabilities
- Device is portable
- Weak password
- ePHI is not encrypted
- ePHI is not backed up

Information Asset
- Laptop with ePHI

Controls
- Policies & Procedures
- Training & Awareness
- Cable lock down
- Strong passwords
- Encryption
- Remote wipe
- Data Backup
Risk = \( f([\text{Assets}+\text{Threats}+\text{Vulnerabilities}+\text{Controls}] \times [\text{Likelihood} \times \text{Impact}]) \)

**Likelihood**
- Not Applicable
- Rare
- Unlikely
- Moderate
- Likely
- Almost Certain

**Impact**
- Not Applicable
- Insignificant
- Minor
- Moderate
- Major
- Disastrous

Based on threat, vulnerabilities and current controls in place.

Based on size, sensitivity and effort or cost of remediation.

**Risks**
- Financial
- Political
- Legal
- Regulatory
- Operational impact
- Reputational
Asset * Threat * Vulnerabilities = Risk
What A Risk Analysis Is Not

- A network vulnerability scan
- A penetration test
- A configuration audit
- A network diagram review
- A questionnaire
- Information system activity review

A Risk Analysis IS the process of identifying, prioritizing, and estimating risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, …, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.
NOT Risk Management
Session Agenda

1. Why Care?
2. Key Risk Analysis Terminology
3. HIPAA Regulatory Requirements
4. How to Get Started
5. Specific, Practical Best Practices
6. Risk Analysis Exercise
HITECH meets HIPAA ... at Meaningful Use

Risk Analysis

45 CFR 164.308(a)(1)(i)(A)

HIPAA Security Final Rule

Meaningful Use Final Rule

35
Two Dimensions of HIPAA Security Business Risk Management

Compliance

45 CFR 164.308(a)(8)

Security

45 CFR 164.308(a)(1)(ii)(A)

Overall Business Risk Management Program; Not “an IT project”
Security Evaluation v. Risk Analysis

45 C.F.R. §164.308(a)(8)

**Standard: Evaluation.** Perform a periodic technical and non-technical 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, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.


(1)(i) **Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations. 

(ii) Implementation specifications:

(A) **Risk analysis (Required).** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
Regardless of the risk analysis methodology employed…

1. **Scope of the Analysis** - all ePHI that an organization creates, receives, maintains, or transmits must be included in the risk analysis. (45 C.F.R. § 164.306(a)).

2. **Data Collection** - The data on ePHI gathered using these methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316 (b)(1)).

3. **Identify and Document Potential Threats and Vulnerabilities** - Organizations must identify and document reasonably anticipated threats to ePHI. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii)).

4. **Assess Current Security Measures** - Organizations should assess and document the security measures an entity uses to safeguard ePHI. (See 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1)).

5. **Determine the Likelihood of Threat Occurrence** - The Security Rule requires organizations to take into account the likelihood of potential risks to ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv)).

6. **Determine the Potential Impact of Threat Occurrence** - The Rule also requires consideration of the “criticality,” or impact, of potential risks to confidentiality, integrity, and availability of ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv)).

7. **Determine the Level of Risk** - The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)).

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

9. **Periodic Review and Updates to the Risk Assessment** - The risk analysis process should be ongoing. In order for an entity to update and document its security measures “as needed,” which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed.
2 Dimensions of HIPAA Security Risk Management

1. What is our exposure of our information assets (e.g., ePHI)?

2. What do we need to do to treat risks?
Session Agenda

1. Why Care?
2. Key Risk Analysis Terminology
3. HIPAA Regulatory Requirements
4. How to Get Started
5. Specific, Practical Best Practices
6. Risk Analysis Exercise
Risk Management = Assessment + Treatment

- Risk assessment:
  - What should we protect?
  - Why?
  - From what?
  - Evaluation

- Risk treatment:
  - Determining security measures (controls)
The Process

- Risk Approach
- Asset Inventory
- Risk Analysis
- Risk Treatment
- Documentation
Step 1) Risk Analysis Approach

A. Risk Analysis Methodology
B. Method for Valuing Risks
C. Criteria for Accepting Risks
Risk Analysis Methodology

- Purpose – define and document whole risk management process
- Implement the process in the same way throughout the whole organization
- Complexity – depends on the size of the organization, regulations etc.
- Usually one document, 5 pages or more
Elements Of Risk Analysis Methodology

- Scope of information risk management
- Qualitative/quantitative
- Elements of evaluation (2 or 3 dimensions)
- Scales of assessment
- Method of calculating risk
- Risk acceptance criteria
- Reviewing the Risk Analysis and Risk Treatment methodology template…
Establishing a Risk Value

Risk = Likelihood * Impact

### Likelihood

<table>
<thead>
<tr>
<th>Rank</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Not Applicable</td>
<td>Will never happen</td>
</tr>
<tr>
<td>1</td>
<td>Rare</td>
<td>May happen once every 10 years</td>
</tr>
<tr>
<td>2</td>
<td>Unlikely</td>
<td>May happen once every 3 years</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>May happen once every 1 year</td>
</tr>
<tr>
<td>4</td>
<td>Likely</td>
<td>May happen once every month</td>
</tr>
<tr>
<td>5</td>
<td>Almost Certain</td>
<td>May happen once every week</td>
</tr>
</tbody>
</table>

### Impact

- Critical = 25
- High = 15-24
- Medium = 8-14
- Low = 0-7

<table>
<thead>
<tr>
<th>Rank</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Not Applicable</td>
<td>Does not apply</td>
</tr>
<tr>
<td>1</td>
<td>Insignificant</td>
<td>Not reportable; Remediate within 1 hour</td>
</tr>
<tr>
<td>2</td>
<td>Minor</td>
<td>Not reportable; Remediate within 1 business day</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>Not reportable; Remediate within 5 business days</td>
</tr>
<tr>
<td>4</td>
<td>Major</td>
<td>Reportable; Less than 1,000 records compromised</td>
</tr>
<tr>
<td>5</td>
<td>Disastrous</td>
<td>Reportable; Greater than 1,000 records compromised</td>
</tr>
</tbody>
</table>

---

**Overall Risk Value**

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HIGH</td>
</tr>
<tr>
<td>LOW</td>
<td>Low</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>Low</td>
</tr>
</tbody>
</table>

---

**Critical**

**High**

**Medium**

**Low**
## Simplified Risk Analysis Example

<table>
<thead>
<tr>
<th>Asset</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Likelihood (1-5)</th>
<th>Impact (1-5)</th>
<th>Risk (L * I)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop</td>
<td>Theft</td>
<td>Device is portable</td>
<td>4</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Weak password</td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ePHI is not encrypted</td>
<td>3</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ePHI is not backed up</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
Criteria For Accepting Risks

- Score Range: 0-25
- Risk Values
  - Critical = 25
  - High = 15-24
  - Medium = 8-14
  - Low = 0-7

Example:
- Acceptable level of risk: 14
- Value of risk A: 9 – no treatment is needed
- Value of risk B: 17 – risk treatment is needed
Step 1) Risk Analysis Approach Exercise

Class Discussion…10 minutes
A. Qualitative or Quantitative Methodology
B. What’s Your Risk Appetite
Step 2) Asset Inventory

A. Inventory information assets that create, receive, maintain and transmit ePHI
Step-by-Step: Inventory

- Information Asset / Application / Database Name Containing ePHI
- Information Asset Owner
- Description of Information Asset / Application / Database Name Containing ePHI
- Location of ePHI
- ePHI Data Source
- ePHI Data Sharing
- Business Processes Supported
- Asset Importance to Business
- Estimated Number of Records
- Planned Risk Analysis Completion

Data elements captured should help inform and guide the risk analysis steps that follow…
Step 2) Asset Inventory Exercise

Written Exercise…10 minutes

A. List Your Information Assets (create, receive, maintain or transmit ePHI)

B. For one Information Asset, list all associated media on which ePHI may reside
Step 3) Risk Analysis

For Each Asset...

A. Identify threats in the environment
B. Identify vulnerabilities that threats could trigger
C. Identify current controls
D. Describe the risks based on threats and vulnerabilities
E. Determine the likelihood of the risk
F. Determine the severity of the impact
G. Determine and summarize the risk level
### Simplified Risk Analysis Example

<table>
<thead>
<tr>
<th>Asset</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>Likelihood (1-5)</th>
<th>Impact (1-5)</th>
<th>Risk (L * I)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop</td>
<td>Theft</td>
<td>Device is portable</td>
<td>4</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Weak password</td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ePHI is not encrypted</td>
<td>3</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ePHI is not backed up</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
Step 3) Risk Analysis

Class Discussion Exercise…10 minutes

A. Name threats/threat sources to one of your information assets

B. Name vulnerabilities to that information asset
Step 4) Risk Treatment

Identify and evaluate options for the treatment of risks:
1. Transfer the risks
2. Avoid risks
3. Mitigate risks (by implementing controls)
4. Accept risks
Risks of all types & sizes exist

Risk Identification

Risk Treatment

Avoid / Transfer Risks

Mitigate / Transfer Risks

Accept Risks
Risk Treatment

- Select control objectives and controls for the treatment of risks
- Balance the costs and benefits
- Take into account legal, regulatory and contractual requirements
## Risk treatment - example

**Asset:** Laptop with ePHI  
**Threat:** Theft  
**Vulnerability:** Left in a car; no encryption

<table>
<thead>
<tr>
<th>Impact (1-5)</th>
<th>Likelihood (1-5)</th>
<th>Risk</th>
<th>Controls</th>
<th>Impact (1-5)</th>
<th>Likelihood (1-5)</th>
<th>Residual Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5</td>
<td>25</td>
<td>Policy</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Disk encryption</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Awareness tng</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Legal documents</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Data backup</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>
Step 4) Risk Treatment

Risk Treatment Exercise
Step 5) Documentation

- Risk Treatment Plan
- Risk Assessment Report
- Approval of Residual Risks
Risk Treatment Plan

- Management action
- Resources
- Responsibilities
- Priorities
- Consideration of funding
Risk Assessment Report

- **Purpose** – to document the whole risk assessment and risk treatment process

- **Includes:**
  - Risk assessment methodology
  - Criteria for accepting risks
  - Risk assessment
  - Risk treatment
Approval of residual risks

- All risks, whether acceptable or not
- By the management!
- Approval can be separate document, or part of Risk Assessment Report
Conclusions

During the risk treatment, you plan how to potentially spend a lot of money & other resources

You need to do it in a creative and collaborative way so to be accepted by business side of the organization
Risk Management Planning Resources

- HHS / OCR Final Guidance on Risk Analysis
- NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments – DRAFT
- NIST SP800-34 Contingency Planning Guide for Federal Information Systems
- NIST SP800-39-final_Managing Information Security Risk
- NIST SP800-53 Revision 3 Final, Recommended controls for Federal Information Systems and Organizations
Steps to Complete A HIPAA (Meaningful Use) Risk Analysis

1. Form a Cross-Functional Task Force
2. Set Business Risk Management Goals
3. Get Educated – Learn the Requirements and the Consequences
4. Build / Buy a Risk Analysis Software Tool Based on the HHS/OCR Final Guidance
5. Set a Scoring Methodology
6. Complete the HIPAA Risk Analysis Methodology
7. Document Control Gaps
8. Make Risk Mitigation Decisions
9. Prioritize Work Plans based on Risks
10. Execute Risk Mitigation Plan
Summary and Next Steps

- Risk Analysis is a Critical, Foundational Step
- Consider Assessing the Forest as Well
- Completing a Risk Analysis is key to HIPAA compliance
  - But, is not your only requirement…
- Stay Business Risk Management-Focused
- Don’t Call The Geek Squad
- Large or Small: Get Help (Tools, Experts, etc)
- Consider tools and templates
Supplemental materials