Risk Analysis Webinar

Tom Walsh, CISSP
President

Webinar Objectives

• Provide a brief overview of the HIPAA Security Rule
• Discuss the nine steps for conducting a risk analysis which include: assessing reasonably anticipated threats, evaluating current security controls, determining vulnerabilities, and rating the residual risks
• Review security controls for managing risks
• Review the key requirements of HIPAA, HITECH Act, and Meaningful Use for risk analysis and management
• Provide examples of how risk analysis can be documented and managed

Copyright © 2012, Tom Walsh Consulting, LLC
Introduction – Tom Walsh

- Certified Information Systems Security Professional (CISSP)
- Co-authored three books on healthcare information security topics
- Information security consultant for two community based hospitals and a large physician organization
- Former information security manager for large healthcare system in Kansas City, MO
- A little nerdy, but overall, a nice guy 😊

Copyright © 2012, Tom Walsh Consulting, LLC

Handouts for the Webinar

Download this comprehensive handbook from the Kansas Hospital Association website (www.kha-net.org)

Copyright © 2012, Tom Walsh Consulting, LLC
Handouts for the Webinar

HIPAA

HIPAA Public Law 104-191
- Title I: Insurance Portability
- Title II: Administrative Simplification
- Title III: Medical Savings and Tax Deduction
- Title IV: Group Health Plan Provisions
- Title V: Revenue Offset Provisions

Transactions, Identifiers, Security, Privacy, Enforcement

Copyright © 2012, Tom Walsh Consulting, LLC
HIPAA Security Rule

• Proposed Rule - August 1998
  – Almost 14 years ago!
• Final Rule released on February 2003
• Compliance deadline: April 21, 2005
  – Over seven years ago!
• 24 Standards, 70 implementation specifications *(Required or Addressable)*
• Reasonable and appropriate safeguards

Copyright © 2012, Tom Walsh Consulting, LLC
Risk Analysis

Under HIPAA each covered entity:
• Assesses its own security risks
• Determines its risk tolerance or risk aversion
• Devises, implements, and maintains appropriate security to address its business requirements
• Documents its security decisions

Risk Analysis

Two types:
• Qualitative - (Easiest and most common) Rating risks on a scale such as:

High  Medium  Low

• Quantitative - (Most difficult to determine) Placing a dollar value on the risk based upon some formulas or calculations
Risk Analysis
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*

**Why?**
1. Because it is a comprehensive framework *(It closely follows other risk analysis methodologies)*
2. Referenced several times by HHS and/or CMS:
   1. HI PAA Security Rule
   2. Various whitepapers
   3. Audit reports (2008 and 2009)
1. System Characterization

- **Hardware**
  - Servers
  - Network equipment (includes wireless)
  - Computer workstations
  - Laptops and tablets
  - Smartphones

- **Software**
  - Operating systems
  - Applications and programs

- **Information and/or Data**
  - Highly sensitive, confidential or mission critical

See page 5

2. Threat Identification

- **Acts of Nature**
  - Some type of natural disaster that is beyond our control

- **Acts of Man**
  - Unintentional or accidental
  - Intentional

- **Environmental**
  - Power outage, broken water pipe, network outage, cut LAN cable

See page 6
Unreasonable Threats

- Chemical spills
- Biological contamination
- Nuclear mishaps
- Aircraft accident
- Civil unrest / Rioting
- Bomb threats
- Sinking ground
- Tsunami
- Volcano eruption
- Blackmail
- Substance abuse
- Inflation

Thorough does not mean unreasonable

3. Vulnerability Identification

- Hardware
  - Improperly configured equipment
- Software
  - Operating systems needing patching
  - Poorly written applications
- Environmental
  - Lack of environmental controls
  - Lack of physical safeguards
- Operational practices
  - Lack of policies and procedures
  - Untrained personnel

See page 8
4. Control Analysis

- Survey or checklists are usually used to collect data on existing controls
  - Most common mistake: Trying to ask too many questions

<table>
<thead>
<tr>
<th>Access Control</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>18. Is there an access control list of authorized users?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19. Are users only granted access by a request from management?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20. Are users' default privileges set for least privilege?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21. Are user accounts locked out after five unsuccessful log-in attempts?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22. Is there a method in place to notify the server administrator when a user's access is no longer required (i.e. user termination or transfer)?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Risk Assessment / Analysis

- After identifying the threats and vulnerabilities, determine risks considering existing controls

\[
\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}
\]

*If any one of the three equals zero, there is no risk*

- Risks are rated by the likelihood of a threat exploiting a vulnerability and the possible consequences or impact
5. Likelihood Determination

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

Source: NIST SP 800-30 Risk Management Guide for Information Technology Systems

6. Impact Analysis

<table>
<thead>
<tr>
<th>Magnitude of Impact</th>
<th>Impact Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Exercise of the vulnerability (1) may result in the high 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.</td>
</tr>
<tr>
<td>Medium</td>
<td>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.</td>
</tr>
<tr>
<td>Low</td>
<td>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.</td>
</tr>
</tbody>
</table>

Source: NIST SP 800-30 Risk Management Guide for Information Technology Systems
7. Risk Determination

Determining a “Risk Score”

The higher the number, the greater your risks.

Source: The OCTAVE™ Approach

<table>
<thead>
<tr>
<th>Impact</th>
<th>H</th>
<th>M</th>
<th>L</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>M</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>H</td>
<td>3</td>
<td>6</td>
<td>9</td>
</tr>
</tbody>
</table>

Likelihood Impact Risk Score Color Rating

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Score</th>
<th>Color Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>9</td>
<td>Red</td>
</tr>
<tr>
<td>H</td>
<td>M</td>
<td>6</td>
<td>Red</td>
</tr>
<tr>
<td>M</td>
<td>H</td>
<td>6</td>
<td>Red</td>
</tr>
<tr>
<td>M</td>
<td>M</td>
<td>4</td>
<td>Yellow</td>
</tr>
<tr>
<td>H</td>
<td>L</td>
<td>3</td>
<td>Yellow</td>
</tr>
<tr>
<td>L</td>
<td>H</td>
<td>3</td>
<td>Yellow</td>
</tr>
<tr>
<td>M</td>
<td>L</td>
<td>2</td>
<td>Green</td>
</tr>
<tr>
<td>L</td>
<td>M</td>
<td>2</td>
<td>Green</td>
</tr>
<tr>
<td>L</td>
<td>L</td>
<td>1</td>
<td>Green</td>
</tr>
</tbody>
</table>
8. Control Recommendations

Types of Controls
• Technical
• Non-technical
  – Administrative
  – Physical / Environmental

Purpose of Controls
1. Prevention (proactive)
2. Detection (reactive)
3. Assurance (proactive)
4. Recovery (reactive)
9. Results Documentation

- Overview
- System description
- Description of Risk Analysis Approach
- Results (Findings)
- Recommendations
- Information/Data Owner Comments
- Statement of Understanding

Data Owner Involvement

- Risk can either be:
  - Mitigated/Reduced (Applying controls)
  - Transferred (Insuring against a loss) or
  - Accepted (Doing nothing, but recognizing risk)

- Risk should be handled in a cost-effective manner relative to the value of the asset
Risk Analysis Documentation

<table>
<thead>
<tr>
<th>Threats</th>
<th>Vulnerability</th>
<th>Impact or Loss</th>
<th>Prob. Score</th>
<th>Impact Score</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware or mechanical failure</td>
<td>No backup system; No redundancy system</td>
<td>Business interruption (Availability or Integrity)</td>
<td>H</td>
<td>H</td>
<td>9</td>
</tr>
<tr>
<td>Workforce Behavior - Careless act of employees; Accidental loss or disclosure of PHI</td>
<td>Lack of training; Lack of adequate access controls; No security incident handling procedures; Inadequate sanctions; No media re-use policy; No data destruction procedures</td>
<td>Confidentiality, Integrity, or Availability Litigation; Criminal or civil</td>
<td>H</td>
<td>M</td>
<td>6</td>
</tr>
<tr>
<td>Environmental (fire, water damage, heat, etc.)</td>
<td>Insufficient disaster or contingency planning</td>
<td>Business interruption (Availability)</td>
<td>L</td>
<td>H</td>
<td>3</td>
</tr>
</tbody>
</table>

Risk Profile Approach

**Major App 1**
- Data
- Application
- Network
- Hardware & Operating System
- Physical/Environment
- Operational Practices

**Major App 2**
- Data
- Application
- Network
- Hardware & Operating System
- Physical/Environment
- Operational Practices

Copyright © 2012, Tom Walsh Consulting, LLC
Risk Profile Approach

A hierarchical approach to assessing controls and risks

<table>
<thead>
<tr>
<th>Major App 1</th>
<th>Major App 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Application</td>
<td>Data Application</td>
</tr>
<tr>
<td>Network</td>
<td>Network</td>
</tr>
<tr>
<td>Hardware &amp; Operating System</td>
<td>Hardware &amp; Operating System</td>
</tr>
<tr>
<td>Physical/Environment</td>
<td>Physical/Environment</td>
</tr>
<tr>
<td>Operational Practices</td>
<td>Operational Practices</td>
</tr>
</tbody>
</table>

Reported Breaches

- Theft: 55%
- Loss: 12%
- Unauthorized Access: 20%
- Improper Disposal: 5%
- Hacking: 6%
- Other: 2%

As of June 30, 2012 –

443 breaches were reported to HHS where each breach affected 500 or more patients
Total number of patients affected by these large breaches: 20,098,153

Business Associates were responsible for 21% of all reported breaches

Copyright © 2012, Tom Walsh Consulting, LLC
### By the numbers…

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Number of Incidents</th>
<th>% of Total Incidents</th>
<th>Number of Patients</th>
<th>% of Patients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop</td>
<td>109</td>
<td>25%</td>
<td>1,912,319</td>
<td>10%</td>
</tr>
<tr>
<td>Portable Devices</td>
<td>63</td>
<td>14%</td>
<td>1,507,810</td>
<td>8%</td>
</tr>
<tr>
<td>Desktop Computer</td>
<td>55</td>
<td>12%</td>
<td>2,253,622</td>
<td>11%</td>
</tr>
<tr>
<td>Hard Drives</td>
<td>1</td>
<td>0.2%</td>
<td>1,023,209</td>
<td>5%</td>
</tr>
</tbody>
</table>

In most healthcare organizations today, smartphones and tablets are personally-owned.

### Risk Analysis – HIPAA

§ 164.308(a)(1)(ii)(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 [or business associate].
Risk Analysis – Meaningful Use

Ensure adequate privacy and security protections for personal health information

Stage 1 Measures:
• 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

Stage 2 – Proposed Measures:
• (16)(i) Objective. Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.
• (ii) Measure. Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the EP’s risk management process.
Risk Analysis – HIPAA Audit Protocol

• Inquire of management as to whether formal or informal policies or practices exist to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.

• Obtain and review relevant documentation and evaluate the content relative to the specified criteria for an assessment of potential risks and vulnerabilities of ePHI. Evidence of covered entity risk assessment process or methodology considers the elements in the criteria and has been updated or maintained to reflect changes in the covered entity’s environment. *(The Risk Analysis Handbook defines the NIST process recommended by HHS, CMS, and OCR.)*

Copyright © 2012, Tom Walsh Consulting, LLC

---

Risk Analysis – HIPAA Audit Protocol

• Determine if the covered entity risk assessment has been conducted on a periodic basis. *(Whenever there is a significant change, or at least once every three years.)*

• Determine if the covered entity has identified all systems that contain, process, or transmit ePHI. *(Step 1 of the risk analysis process – System Characterization)*

Copyright © 2012, Tom Walsh Consulting, LLC
Exercise – EMR Risk Profile

Linking Threats to Control Analysis Questions:

The number or numbers contained within the square brackets represent the most likely threats being addressed by the checklist question. For example, [2, 3] at the end of a question would indicate that the control being assessed in that particular checklist question is used to defend against two threats: an unauthorized user or inappropriate access (internal) and having or tampering by an external person.

Reasonably anticipated threats:

1. Authorized user missing their access privileges, tampering, or improper use
2. Unauthorized user or inappropriate access (internal)
3. Accidental or unauthorized disclosures of confidential information
4. Program error, application bug, and/or server failure
5. Hacking or tampering by an external person

Instructions:

Check "Yes" to indicate compliance. If the system lacks the capability or the control is not in place, check "No" and if you are unsure of the answer, then check "Don’t Know." Check "Not Applicable" if the question is non-applicable. Please provide any comments, explanations, or other compelling controls that are in place in the Comments section.

Access Controls

1. Are all users assigned their own, unique User ID? [ ]
2. Are shared or generic logon accounts to the EMR prohibited? [ ]
3. Does the application have an automatic time-out which ends access to the application after an appropriate activity period? [ ]
4. Does the application lockout a user or reset an alarm after a predetermined number of consecutive unsuccessful logon attempts? [ ]
5. Are users required to receive training prior to receiving access to the application? [ ]

Authentication

6. Are users forced to change their password from the initially assigned password after login? [ ]
7. Indicate the minimum number of characters for passwords: [ ]

Copyright © 2012, Tom Walsh Consulting, LLC
Exercise – EMR Risk Profile

### Clinic-EMR (SAMPLE)

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Current Controls</th>
<th>Vulnerability</th>
<th>Impacted Logical</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Suggested Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User accounts assigned on a per-unique constraint basis.</td>
<td>Accounts may allow unauthorized access.</td>
<td>Potential for unauthorized access.</td>
<td>High</td>
<td>Loss of confidentiality</td>
<td>Replace accounts with unique User IDs.</td>
</tr>
<tr>
<td>2</td>
<td>Emergency telecommunication endpoints may not be unique</td>
<td>Emergency telecommunication endpoints may not be unique.</td>
<td>Potential for unauthorized access.</td>
<td>High</td>
<td>Loss of confidentiality</td>
<td>Ensure unique User IDs for all endpoints.</td>
</tr>
<tr>
<td>3</td>
<td>Access is allowed to users who are not authorized for access.</td>
<td>Access is allowed to users who are not authorized for access.</td>
<td>Potential for unauthorized access.</td>
<td>High</td>
<td>Loss of confidentiality</td>
<td>Ensure strict access controls.</td>
</tr>
</tbody>
</table>

### Instructions
- Check "Yes" to indicate compliance. If the system lacks the capability or the controls are in place, check "No." If unsure, choose "Unknown." If the question is not applicable, please leave the question blank. If necessary, explain any information or other commentary. The controls in place for the Clinic section are:

### Access Controls
1. Are all users assigned their own, unique User IDs? (Yes/No)
2. Are shared or generic logon accounts in the EMR prohibited? (Yes/No)
3. Does the application have an automatic time-out which ends access to the application after an appropriate inactivity period? (Yes/No)
4. Does the application lock-out a user or alert them after a predetermined number of unsuccessful logon attempts? (Yes/No)
5. Are users required to receive training prior to receiving access to the application? (Yes/No)

### Authentication
6. Are users forced to change their password from their initially assigned password after login? (Yes/No)
7. Indicate the minimum number of characters for passwords: _____________ characters.
### Exercise – EMR Risk Profile

#### Clinic-EMR - (SAMPLE) - Risk Profile

<table>
<thead>
<tr>
<th>Threat</th>
<th>Current Controls</th>
<th>Vulnerability</th>
<th>Impact of Loss</th>
<th>LLR</th>
<th>LI</th>
<th>LO</th>
<th>LI</th>
<th>LO</th>
<th>Behavior, Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Unauthorized access (altered, tampered, or illegitimate)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Unsecured or unencrypted access to sensitive data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Insecure communication channels</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Instructions:** Check “Yes” to indicate compliance. If the system lacks the capability or the control is not in place, check “No.” If you are unsure of the answer, then check “DN” for don’t know. Check “NA” if the question is not applicable. Please provide any comments, explanations, or other clarifying controls that are in place in the Comments section.

<table>
<thead>
<tr>
<th>Access Controls</th>
<th>Yes</th>
<th>No</th>
<th>DN</th>
<th>NA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Are all users assigned their own, unique User ID?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Are shared or generic logons to the EMR prohibited?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Does the application have an automatic time-out which ends access to the application after an appropriate inactivity period?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Yes</th>
<th>No</th>
<th>DN</th>
<th>NA</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Are users force to change their password from the initially assigned password after login?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Indicate the minimum number of characters for passwords</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Copyright © 2012, Tom Walsh Consulting, LLC

---

Copyright © 2012, Tom Walsh Consulting, LLC
## Exercise – EMR Risk Profile

### Suggested Controls

**Vulnerability**

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Suggested Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unauthorized users or inappropriate access (Information)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Lack of access controls and monitoring</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Insufficient access control</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Poor password management</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Lack of regular audit and review of access control mechanisms</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Lack of sufficient controls to prevent or detect unauthorized access to sensitive data</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Risk Profile**

<table>
<thead>
<tr>
<th>Tenure</th>
<th>Current Contract</th>
<th>Vulnerability</th>
<th>Impact of Loss</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Exercise – EMR Risk Profile

Other Clinical Applications

• Pharmacy
• Lab
• Radiology
• Data Warehouse
• Business Intelligence (Decision Support)
• Dictation and Transcription

Documentation must be retained for six years!
### Risk Profile Approach

<table>
<thead>
<tr>
<th>Major App 1</th>
<th>Major App 2</th>
<th>A hierarchical approach to assessing controls and risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Data</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Application</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Network</td>
<td>Risk Profile</td>
</tr>
<tr>
<td>Hardware &amp; Operating System</td>
<td>Hardware &amp; Operating System</td>
<td>Risk Profile</td>
</tr>
<tr>
<td>Physical/Environment</td>
<td>Physical/Environment</td>
<td>Risk Profile</td>
</tr>
<tr>
<td>Operational Practices</td>
<td>Operational Practices</td>
<td>Risk Profile</td>
</tr>
</tbody>
</table>

### General Support Systems

“General Support Systems” would include such systems as:
- Computer Workstations
- Network
- Active Directory (or LDAP)
- Data Center
- Operational and Organizational Practices
- Remote Access & Web Portal
- Laptops and Tablets
- Smartphones (and/or Mobile Devices)
Risk Analysis Report

Findings (Yellow = 4 or 3) (listed in order of priority)

The following findings rated risk scores of 4 and should be given serious consideration for remediation:

1. IT assigns users their password and it does not change; minimum password length is set at three characters and complexity rules are not enforced
2. No auto logoff after a predetermined period of inactivity
3. Notification from HR when an employee leaves is not consistent; HR may not always provide notification when an employee changes jobs, is on medical disability, or is placed on disciplinary suspension
4. Managers are not periodically provided a listing of their employees and their access privileges to review and verify that their access is appropriate
5. Inactive user accounts (Ex: More than 30 days since last use) are not reviewed
6. Users can have concurrent logons under the same user ID
7. Audit logs are not regularly reviewed and are primarily used for problem solving
8. No warning banner displayed at logon prompt notifying users that their activities are being monitored and audited
9. Users are not required to receive training in order to receive their password
10. Physicians do not promptly notify IT when their office fax number changes (misdirected faxes)

The following selected findings rated risk scores of 3 which is generally an acceptable level of risk, but these selected vulnerabilities should also be given some considered for remediation:

11. There is no formal change control process
12. Recovery procedures for this application are not detailed in the IT disaster recovery plan

See Appendix E

Risk Analysis Report

Recommendations

The following recommendations (listed in order of priority) should be considered to help reduce risks:

<table>
<thead>
<tr>
<th>Suggested Controls</th>
<th>Estimated Resources (Capital, Expense, and Hours)</th>
<th>Information/System Owner – Decisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Set users' passwords to a minimum length of six or more characters and if possible, enforce complexity and initial and periodic expiration</td>
<td>30 hrs to implement password rule changes and notify users</td>
<td>Mitigate risks (Approve the control) Transfer or insure against risks Accept risks (Deny the control)</td>
</tr>
<tr>
<td>2. Consider establishing an auto logoff after 10 minutes of inactivity or activating computer workstation screen savers in patient care areas (or otherwise) to trigger within five minutes to prevent incidental disclosure of PHI</td>
<td>5 hrs to investigate auto logoff capabilities 2 hrs to implement</td>
<td></td>
</tr>
<tr>
<td>3. Establish a process so that HR quickly notifies IT when an employee terminates, changes jobs, is on medical leave, or is placed on disciplinary suspension</td>
<td>5 hrs to review termination notification process</td>
<td></td>
</tr>
<tr>
<td>4. Work with managers on periodically reviewing user access privileges and roles to determine if access is appropriate</td>
<td>10 hrs every 6 months to review user access rights</td>
<td></td>
</tr>
<tr>
<td>5. Create a process to automatically disable user accounts that have been inactive for long periods of time (Ex: 30+ days)</td>
<td>5 hrs annually to review manually, 5 hrs to automate</td>
<td></td>
</tr>
</tbody>
</table>
Risk Analysis Report

Information/System Owner Comments
(The Information/Data Owner can note any exceptions to the risk profile, findings, or recommendations.)

Statement of Understanding
I, the Information/System Owner, understand that the vulnerabilities identified in this report could cause a negative impact to business operations if the threat was realized. For each recommendation in this report, I have determined whether risks will be mitigated by implementing the recommended controls, transferred or insured against, or accepted. I understand that choosing to accept the risks could adversely affect business operations and/or result in noncompliance with regulatory requirements.

I have been informed of the risks for operation of the system in its current configuration.

Information/Data Owner or Designee                        Date

Copyright © 2012, Tom Walsh Consulting, LLC

Thanks for Attending!

Tom Walsh, CISSP

twalshconsulting@aol.com

913-696-1573