Welcome

- Slide materials and recording will be available after the webinar

- Submit questions in “Question Area” on Go-To-Webinar Control Panel

- In case of technical issues, check “Chat Area”

- All Attendees are in Listen Only Mode
Topics of Discussion

- Overview
- Protect Electronic Health Information Measure
- What is a Risk Analysis?
- Three Areas to Assess
- Desktop Audit Checklist/Supporting Documentation
- Additional Resources
Brief Overview

- The American Recovery and Reinvestment Act of 2009 (ARRA)
  - The economic stimulus package signed into law by President Barrack Obama on Feb. 17, 2009
  - Included in this law is $22 Billion of which $19.2 billion intended to be used to increase the use of Electronic Health Records (EHR) by hospitals and physicians...called the Health Information Technology of Economic and Clinical Health Act, or the HITECH Act
The HITECH Act

- Plan - promote the adoption and Meaningful Use (MU) of health information technology (HIT); every American will have an electronic health record by 2014
- Goal – improve quality of health care, reduce medical errors, reduce health disparities, improve public health, increase prevention and care coordination, improve continuity of health care and reduce health care costs
- Incentives for eligible professionals and hospitals who meet MU requirements
### Meaningful Use Stage 1 Protect Electronic Health Information Measure for EPs

<table>
<thead>
<tr>
<th>Objective</th>
<th>Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measure</td>
<td>Conduct or review a security risk analysis in accordance with the requirements under 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>
<tr>
<td>Exclusion</td>
<td>No exclusion.</td>
</tr>
</tbody>
</table>
### Protect Electronic Health Information

<table>
<thead>
<tr>
<th>Objective</th>
<th>Protect electronic health information created or maintained by the certified EHR technology (CEHRT) through the implementation of appropriate technical capabilities.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measure</td>
<td>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 stored in CEHRT 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 provider's risk management process for EPs.</td>
</tr>
<tr>
<td>Exclusion</td>
<td>No exclusion.</td>
</tr>
</tbody>
</table>
## Meaningful Use Stage 1 Protect Electronic Health Information Measure for Hospitals

<table>
<thead>
<tr>
<th>Objective</th>
<th>Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measure</td>
<td>Conduct or review a security risk analysis in accordance with the requirements under 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>
<tr>
<td>Exclusion</td>
<td>No exclusion.</td>
</tr>
</tbody>
</table>
Meaningful Use Stage 2 Protect Electronic Health Information Measure for Hospitals

<table>
<thead>
<tr>
<th>Protect Electronic Health Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objective</strong></td>
</tr>
<tr>
<td>Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.</td>
</tr>
<tr>
<td><strong>Measure</strong></td>
</tr>
<tr>
<td>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 stored in CEHRT 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 provider’s risk management process for eligible hospitals.</td>
</tr>
<tr>
<td><strong>Exclusion</strong></td>
</tr>
<tr>
<td>No exclusion.</td>
</tr>
</tbody>
</table>
What is a Risk Analysis?

- Review existing security of protected health information.
- Identify threats and vulnerabilities.
- Mitigate risks and vulnerabilities.
- Access risk for likelihood and impact.
- Monitor results.

Qsource
Health IT Consulting
Review Current Security Measures

Identify e-PHI
Where does e-PHI reside
Is e-PHI being transported out of your organization

Confidentiality
Policies and procedures in place to be sure e-PHI is only shared with appropriate entities

Accessibility
Plans in place to ensure data is available even in the event of unforeseen circumstances or disaster

Integrity
Safeguards to be sure data is accurate and consistent without loss or corruption
Identify Threats and Vulnerabilities

Now that you know where e-PHI resides what threats and vulnerabilities are in place

- Potential threats
  - Theft of portable devices
  - Natural disasters
  - Viruses

- Vulnerabilities
  - Human error
  - Lack of firewalls
Assess Likelihood

What is the likelihood there could be breach, loss, or corruption based on safeguards that are currently in place?

Low – Modest or Insignificant chance of occurrence

Medium – Significant chance of occurrence

High – Probable chance of occurrence

Source: healthit.gov

www.healthit.gov/sites/default/files/tools/hit_security_risk_assessment_tool_v1.0_revised-1_0.xlsm
Assess Impact

What would the impact be?

Low – no exposed data or interruption to a few hours interruption

Medium – little exposed data and or multi hour to one day of interruption

High – multi day and or major exposure of secure data
## 10 Myths surrounding Risk Analysis

<table>
<thead>
<tr>
<th>Myths</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The security risk analysis is optional for small providers.</td>
<td></td>
</tr>
<tr>
<td>Simply installing a certified EHR fulfills the security risk analysis MU requirement.</td>
<td></td>
</tr>
<tr>
<td>My EHR vendor took care of everything I need to do about privacy and security.</td>
<td></td>
</tr>
<tr>
<td>I have to outsource the security risk analysis.</td>
<td></td>
</tr>
<tr>
<td>A checklist will suffice for the risk analysis requirement.</td>
<td></td>
</tr>
</tbody>
</table>
# 10 Myths surrounding Risk Analysis

<table>
<thead>
<tr>
<th>Myths</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is a specific risk analysis method that I must follow.</td>
</tr>
<tr>
<td>My security risk analysis only needs to look at my EHR.</td>
</tr>
<tr>
<td>I only need to do a risk analysis once.</td>
</tr>
<tr>
<td>Before I attest for an EHR incentive program, I must fully mitigate all risks.</td>
</tr>
<tr>
<td>Each year, I’ll have to completely redo my security risk analysis.</td>
</tr>
</tbody>
</table>
Mitigate Risks and Vulnerabilities

Is the risk or vulnerability addressable?

- Addressable measures must be implemented or if a practice considers the implementation specification unreasonable or inappropriate the reasons must be documented and an equivalent measure must be implemented.
Mitigate Risks/Vulnerabilities (cont.)

What steps must be taken to mitigate each risk and each vulnerability?

Who is responsible for each mitigation step or set of steps?

What is the timeline for implementing the mitigation step or steps?
Monitor Results

- Event logs
- Employee participation in training
- Vulnerability scans
- Penetration tests
Review Current Security Measures

- Annually for Meaningful Use
- After any Modifications
Three Areas to Assess

- Administrative
  - Policies
  - Procedures
  - Documentation

- Technical
  - Security applications
  - Audit trails

- Physical
  - Access
  - Emergency controls
Of Particular Interest

- Business Associates
- Workforce Management
- Incident Management
- Change Management
- Disaster Recovery
### Desktop Audit Checklist

What documentation do I need to support completion of my Security Risk Assessment?

<table>
<thead>
<tr>
<th>Title</th>
<th>Received</th>
<th>Reviewed</th>
<th>Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Information (Names, address, contact name)</td>
<td>2/24/2015</td>
<td>3/27/2015</td>
<td>Yes</td>
</tr>
<tr>
<td>Business Associates List</td>
<td>2/24/2015</td>
<td>2/27/2015</td>
<td>Yes</td>
</tr>
<tr>
<td>Confidentiality Agreement</td>
<td>3/20/2015</td>
<td>3/23/2015</td>
<td>Yes</td>
</tr>
<tr>
<td>Business Associate Agreement</td>
<td>2/24/2015</td>
<td>2/27/2015</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Diagram</td>
<td>3/20/2015</td>
<td>3/23/2015</td>
<td>Yes</td>
</tr>
<tr>
<td>Job Description for Security Officer</td>
<td>2/24/2015</td>
<td>2/27/2015</td>
<td>Yes</td>
</tr>
<tr>
<td>Inventory List (hardware: ex: Laptops, desktops, mobile devices)</td>
<td>2/24/2015</td>
<td>2/27/2015</td>
<td>Yes</td>
</tr>
<tr>
<td>Previous Risk Assessment</td>
<td>2/24/2015</td>
<td>3/27/2015</td>
<td>Yes</td>
</tr>
<tr>
<td>Documents sent in response to Audit request (if applicable)</td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Previous Remediation plan if separate</td>
<td></td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>
Desktop Audit/Supporting Documentation Information

The following items support completion of your Risk Assessment:

› Business Associate List: including the access that each requires for your practice’s facilities, information systems, electronic devices, and ePHI

› Business Associate Agreement: template used by site if BAA is needed.

› Confidentiality Agreement: signed upon hiring and annually by all employees and providers.

Desktop Audit/Supporting Documentation Information

- Network Diagram
- Job description for Security Officer
- Inventory list: including who the device is assigned to or where device is located.
- Previous Risk Assessments
- Remediation Plan if documented separately
- Items sent in response to an Audit request
Things to include

- Current safeguards
- Risks
- Likelihood
- Impact
- Planned remediation steps
  - Who is responsible
  - Timeline for completion
- Completed remediation steps
Remember

Security program documentation needs to be kept just like other work related supporting documentation.

Keep your Security Risk Assessment/Meaningful Use documentation for 6-7 years after you attest for auditing purposes!
Resources

- Privacy/Security Resources
- Audit Guidance
- www.qsource.org/HIT
- SRA Fact Sheet
- Regulation & Guidance
Questions?
Thank You!

Contact Info:
Tabothy Edgin, MBA, RHIA, CCS
Qsource Consulting Specialist
tedgin@qsourc¢.org
731-343-1410
www.Qsource.org/HIT