Ensuring Privacy & Security of Patient Information

Danika Brinda, Assistant Professor and REACH P&S Subject Matter Expert
Jane McGrath, Program Manager REACH/Stratis Health

Session 12, Thursday, June 12, 2014
Objectives

• Recognize the difference between compliance with HIPAA and meeting the MU core measure
• Understand HIPAA requirements for Stage 2 Meaningful Use (MU)
• Prepare for what auditors are looking for and finding
• Appreciate pitfalls and opportunities for a successful Risk Assessment
• Identify tools & resources
Objectives

• Recognize the difference between compliance with HIPAA and meeting the MU core measure

• Understand HIPAA requirements for Stage 2 Meaningful Use (MU)

• Prepare for what auditors are looking for and finding

• Appreciate pitfalls and opportunities for a successful Risk Assessment

• Identify tools & resources
Health Insurance Portability and Accountability Act (HIPAA) of 1996

- First attempt at development of federal rules and regulations to protect the privacy and security of Protected Health Information (PHI)

1996
HIPAA Regulation Enacted

2003
Privacy Rule Mandated

2005
Security Rule Mandated

2009
Interim ARRA/HITECH Provision on Privacy and Security

2013
Final ARRA/HITECH Provision on Privacy and Security
Compliance vs. Meaningful Use

• Compliance
  – HIPAA
  – OCR Audits
  – OCR Investigations

• Meaningful Use
  – EHR Incentive Program
    • Medicare MU audits
    • Medicaid MU audits
Objectives

• Recognize the difference between compliance with HIPAA and meeting the MU core measure

• Understand HIPAA requirements for Stage 2 Meaningful Use (MU)

• Prepare for what auditors are looking for and finding

• Appreciate pitfalls and opportunities for a successful Risk Assessment

• Identify tools & resources
# Protect Electronic Health Information

## Stage 1 (Core)
- **Measure**
  - Conduct or review a security risk analysis, implement security updates as necessary and correct identified security deficiencies
- **Denominator**
  - Yes/No Attest
- **Exclusion**
  - None

## Stage 2 (Core)
- **Measure**
  - Conduct or review a security risk analysis, including addressing the encryption/security of data stored in CEHRT, implement security updates as necessary and correct identified security deficiencies
- **Denominator**
  - Yes/No Attest
- **Exclusion**
  - None
Risk Analysis

“Conduct or review a security risk analysis”

– Security or Privacy & Security
– Internal/external risk analysis/assessment
– Conduct vs. Review
– Conduct/Review every 6-9 months
  • Sooner if system/physical changes
  • Omnibus changes
Mitigation / Remediation Plan

“Implement security updates as necessary and correct identified security deficiencies”

– Detail deficiencies
– Identify responsible person
– Establish risk level
– Review & Assess monthly/quarterly
Address Encryption

“including addressing the encryption/security of data stored in CEHRT”

– Evaluate all encryption being used in the organization
– Evaluate all areas where ePHI is being stored
– Evaluate the need to encrypt
– If not encrypting, need to document current safeguards detailing why encryption is not needed
Objectives

• Recognize the difference between compliance with HIPAA and meeting the MU core measure
• Understand HIPAA requirements for Stage 2 Meaningful Use (MU)
• Prepare for what auditors are looking for and finding
• Appreciate pitfalls and opportunities for a successful Risk Assessment
• Identify tools & resources
Meaningful Use Auditors

• Medicare and Medicaid MU Audits
  – Looking for evidence of:
    • Risk Assessment
    • Mitigation Plan
  – Anecdotal findings:
    • No risk assessment
    • No mitigation plan
    • Smaller providers struggling
REACH Findings

Who

- Small/Medium Providers
- Security Risk Assessment
- Mitigation Plan
- Policies & Procedures

No / Incomplete

MU Attestation
What is the Status of MU Audits?

- Audits are ongoing with each Stage of Meaningful Use
- Approx. 1 in 20 meaningful use attesters will be audited
- Pre and Post audits are being conducted
- Meaningful Use attesters and healthcare organizations can be audited more than once
2012 – 2013 HIPAA Audits

• 115 Audits were conducted in the end of 2012 – August 2013.
• No findings were found in 13 entities (11% of total audited)
• Security non-compliance was 60% of total findings
• Smaller entities struggle with all areas of the HIPAA Privacy and Security rules
OCR Findings by Rule

- Security: 60%
- Privacy: 30%
- Breach: 10%

NIST / OCR 5/22/13
What is the Status of HIPAA Audits?

• On February 24, HHS OCR announce the next phase of HIPAA Audits
• 1200 organizations will be surveyed
  – 800 Covered Entities
  – 400 Business Associates
• The survey is intended to gather information on the respondents (size, complexity, etc)
• Not all organization surveyed will have an actual HIPAA audit conducted
OCR’s HOT Areas of Interest

• Security Risk Assessments
• Effective and On-going Mitigation
• Breach Notification
• Encryption
• Training of workforce
• Policies and Procedures for HIPAA Compliance
Objectives

• Recognize the difference between compliance with HIPAA and meeting the MU core measure
• Understand HIPAA requirements for Stage 2 Meaningful Use (MU)
• Prepare for what auditors are looking for and finding
• Appreciate pitfalls and opportunities for a successful Risk Assessment
• Identify tools & resources
Pitfalls

• HIPAA is complex
• P&S Role/Responsibility is add-on
• Lack of understanding of the MU requirement
• Lack of time and resources
• Security Risk Assessment (SRA) required for each MU reporting period
• Assume EHR vendor/owner is responsible for SRA
Consequences

- **Trust** - Undermine patient confidence / trust
- **Fines** - OCR
- **Incentive $** - Return MU $ plus interest
- **Reputation** – Local regional news
Opportunities - Be Prepared

- Conduct a Risk Assessment
- Review and update all policies and procedures
- Actively address and correct identified deficiencies
- Review and become familiar with HIPAA Audit Protocol
- Conduct internal HIPAA audits
- Document, Document, Document
- Educate all staff and leaders on the importance of HIPAA Compliance
Objectives

- Recognize the difference between compliance with HIPAA and meeting the MU core measure
- Understand HIPAA requirements for Stage 2 Meaningful Use (MU)
- Prepare for what auditors are looking for and finding
- Appreciate pitfalls and opportunities for a successful Risk Assessment
- Identify tools & resources
Tools & Resources

• NEW: HIPAA Privacy & Security Portal

• KHA REACH website
  http://www.khareach.org/portal/privacy-security
# HIPAA P&S Checklist

<table>
<thead>
<tr>
<th>HIPAA/HITECH REFERENCE</th>
<th>HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT</th>
<th>STATUS</th>
<th>POLICY/PROCEDURE</th>
<th>RISK SCORE</th>
<th>RESPONSIBLE PARTY</th>
<th>DUE DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>business associate appropriately safeguard the information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>164.308(b)(4)</td>
<td>Have you established written contracts or other arrangements with your trading partners that documents satisfactory assurances that the BA will appropriately safeguard the information? (R)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>164.310(a)(2)(i)</td>
<td>Have you established (and implemented as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency? (A)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>164.310(a)(2)(ii)</td>
<td>Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Walkthrough Checklist

<table>
<thead>
<tr>
<th>Item</th>
<th>Yes/No Unsure</th>
<th>ID</th>
<th>Control Description</th>
<th>Findings Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policies</td>
<td></td>
<td>PE-1</td>
<td>Documented policies and procedures (P&amp;Ps) that address physical and environmental security</td>
<td></td>
</tr>
<tr>
<td>Physical Authorization</td>
<td></td>
<td>PE-2</td>
<td>Method to determine who is authorized to access secure area of the office (e.g. badges, swipe cards, biometrics)</td>
<td></td>
</tr>
<tr>
<td>Inventory of Assets</td>
<td></td>
<td>PE-3f</td>
<td>Inventory of physical assets maintained.</td>
<td></td>
</tr>
<tr>
<td>Delivery/Removal Records</td>
<td></td>
<td>PE-16</td>
<td>The organization authorizes, monitors, and controls components containing EHR entering and exiting the facility.</td>
<td></td>
</tr>
</tbody>
</table>

1 NIST SP 800-53, [http://csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html)
## Mitigation Plan

**Organization Name**

**Privacy & Security Mitigation Plan**

<table>
<thead>
<tr>
<th>HIPAA/HITECH Ref.</th>
<th>HIPAA Privacy Rule / HIPAA Security Rule HITECH Act</th>
<th>Risk Score/Priority L/M/H</th>
<th>Owner</th>
<th>Date/Status/Notes (Include Policy/Procedure Name/Number) (Status = In Progress, Not Complete, etc)</th>
<th>Planned Comp Date</th>
<th>Actual Comp Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.502</td>
<td>Develop &quot;minimum necessary&quot; policies for:</td>
<td>M</td>
<td>Charles Jones, HIM</td>
<td>10/1/2013 – In Progress - Reviewed and update HIM policy and procedure (HIM P&amp;P, 8.2.3) detailing “minimum necessary.” Referred to Executive Committee for approval.</td>
<td>10/31/2013</td>
<td>11/12/2013</td>
</tr>
<tr>
<td>§164.514</td>
<td>- Uses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Routine disclosures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Non-routine disclosures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Limit request to minimum necessary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Ability to rely on request for minimum necessary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>§164.504</td>
<td>Develop policies for business associate (BA) relationships and amend business associate contracts or agreements:</td>
<td>H</td>
<td>Mary Smith, Finance</td>
<td>8/27/2013 – In Progress - Updated BAA for XYZ Vendor and sent to Attorney for review. Omnibus compliance date for updating BAA is 9/23/2013 (if no BAA) 9/22/2014 (if BAA in effect prior to 1/25/2013)</td>
<td>9/23/2013</td>
<td></td>
</tr>
<tr>
<td>§164.502</td>
<td>Limit disclosures to those that</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk Assessment

Security Risk Assessment

Security Risk Assessment Tool

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC) recognizes that conducting a risk assessment can be a challenging task. That's why ONC, in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed a downloadable SRA Tool (exe - 66 MB) to help guide you through the process. This tool is not required by the HIPAA Security Rule, but is meant to assist providers and professionals as they perform a risk assessment.

We understand that users with Windows 8.1 Operating Systems may experience difficulties downloading the SRA Tool, we are working to resolve the issue and will post here when a resolution is identified and implemented.

The SRA Tool is a self-contained, operating system (OS) independent application that can be run on various environments including Windows OS’s for desktop and laptop computers and Apple’s iOS for iPad only. The iOS SRA Tool application for iPad, available at no cost, can be downloaded from Apple’s App Store®.

The SRA Tool takes you through each HIPAA requirement by presenting a question about your organization’s activities. Your “yes” or “no” answer will show you if you need...
Tools & Resources

- Medscape, [https://login.medscape.com/login/sso/getlogin?urlCache=aHR0cDovL3d3dy5tZWRzY2FwZS5vcmcvc2l0ZXMvYWR2YW5jZXMvcGF0aWVuHMcmlnaHRz&ac=401](https://login.medscape.com/login/sso/getlogin?urlCache=aHR0cDovL3d3dy5tZWRzY2FwZS5vcmcvc2l0ZXMvYWR2YW5jZXMvcGF0aWVuHMcmlnaHRz&ac=401)
Acronyms

• HIPAA – Health Insurance Portability and Accountability Act
• OCR – Officer of Civil Rights (HHS)
• HHS – US Department of Health & Human Services
• HITECH – Health Information Technology for Electronic and Clinical Health Act
• MU – Meaningful Use
• CMS – Centers for Medicare and Medicaid Services
• MEIP – Minnesota EHR Incentive Program
Contact

Jane McGrath, Stratis Health/REACH
jmcgrath@stratishealth.org

Danika Brinda, REACH/College of St. Scholastica
dbrinda@css.edu
Key Health Alliance—Stratis Health, Rural Health Resource Center, and The College of St. Scholastica.

REACH is a project federally funded through the Office of the National Coordinator, Department of Health and Human Services (grant number EP-HIT-09-003).