What we will discuss

- Recap of OCR phase 1 audits
- Omnibus refresh
- 10 things to focus on
- How to prepare
- Continued success
- Q&A
OCR PHASE 1
AUDIT RECAP
OCR Audit: Phase 1
Audit Protocol consisted of 11 Modules

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

- Rights to Request Privacy Protection of PHI
- Notice of Privacy Practices
- Access of Individuals to PHI
- Administrative Requirements
- Uses and Disclosures of PHI
- Amendment of PHI
- Accounting of Disclosures

The information above is from the US Department of Health & Human Services Presentation: OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2 (Linda Sanches, March 2014)
OCR Audit: Phase 1
Privacy: Percentage of Findings by Areas of Focus

- Notices of Privacy Practices for PHI: 2%
- Right to Request Privacy Protection for PHI: 16%
- Access of Individuals to PHI: 44%
- No#ces of Privacy Prac#ces for PHI: 18%
- Right to Request Privacy Protection for PHI: 16%
- Access of Individuals to PHI: 44%

Security: Percentage of Findings by Area of Focus

- Risk Analysis: 7%
- Access Management: 18%
- Security Incident Procedures: 14%
- Contingency Planning and Backup: 14%
- Workstation Security: 4%

The information above is from the US Department of Health & Human Services Presentation: OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2 (Linda Sanches, March 2014)
OMNIBUS REFRESH
HIPAA Final Omnibus Rule Overview
The final omnibus rule strengthens and expands patient rights as well as enforcement and is comprised of the following four components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Key Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Privacy &amp; Security Rules</td>
<td>- Definition expanded to include “any entity that creates, receives, or transmits” PHI on behalf of a covered entity (“business associate”)</td>
</tr>
<tr>
<td></td>
<td>- Limitations on the use and disclosure of PHI for marketing and fundraising</td>
</tr>
<tr>
<td></td>
<td>- Prohibition on the sale of PHI without authorization</td>
</tr>
<tr>
<td></td>
<td>- Expand rights to receive electronic copies of health information</td>
</tr>
<tr>
<td></td>
<td>- Requirement to modify and redistribute notice of privacy practices</td>
</tr>
<tr>
<td>2. Enforcement Rule</td>
<td>Increased tiered civil penalties:</td>
</tr>
<tr>
<td>Violation</td>
<td>Penalty</td>
</tr>
<tr>
<td>Did not know</td>
<td>$100 - $50,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 - $50,000</td>
</tr>
<tr>
<td>Willful neglect / corrected</td>
<td>$10,000 - $50,000</td>
</tr>
<tr>
<td>Willful neglect / uncorrected</td>
<td>$50,000</td>
</tr>
<tr>
<td>3. Breach Notification Rule</td>
<td>Final rule adopts the Breach Notification for Unsecured PHI created under the HITECH Act, replacing the breach notification rule’s “harm” threshold.</td>
</tr>
<tr>
<td>4. Privacy of Genetic Information</td>
<td>Final rule modifies the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to increase privacy protections for genetic information by prohibiting most health plans from using or disclosing genetic information for underwriting purposes.</td>
</tr>
</tbody>
</table>
What is considered Protected Health Information (“PHI”)?

1. The information relates to:
   i. A physical or mental health condition of an individual;
   ii. The provision of health care to an individual; or
   iii. The payment for the provision of health care to an individual; and

2. The information is individually identifiable; meaning:
   i. It identifies the individual; or
   ii. There is a reasonable basis to believe that the information can be used to identify the individual.
10 THINGS TO FOCUS ON
#1 – Know the scope

- All covered entities and BAs
- Individual and group providers
- Demographic criteria not differentiating
- Privacy, Security and Breach Notification Rules
- Required HIPAA documentation including P&Ps, training documentation and Security Risk Assessments
- Updated to reflect Omnibus
#2 – Logistics and mechanics

- Desk audits primarily
- Select on-site audits
- Estimated completion of 12/31/16
- Results will determine enforcement actions
- Results feed into Phase 3 onsite audits
#3 – Notifications and documentation

- Initial data verification questionnaire (14 days)
- Business Associate listing (CEs)
- Document request list (10 days only electronic)
- Draft findings report (10 days)
- Final audit report (30 days from response)
- Not publically posted/distributed
- Reminder – Watch Spam Filtering!!!
#4 – Comprehensive Risk Assessment

- Must include Omnibus considerations
- Should have been refreshed within the last 12 months
- Ideally performed against a framework
- Risk acceptance or CAP documented
- Vendor risk consideration included
#5 – Data encryption of portable devices

- No excuses from the regulator.
- Laptops and portable media
- Check your vendors!
- Data classification can help
#6 – Business Associate inventory

• Readily provide BA listing (consider template)
• Updated agreements better be in place with each BA
• Population for BA specific audit requests
• High area for non-compliance recently
#7 – Business Associate diligence

- Negligence in selecting BAs
- Monitoring against agreements
- Data inventory mapping
- Third party assurance from BAs
- Consider those with “potential” to access PHI
#8 – You can’t hide!

- Lack of response to questionnaire almost guarantees inclusion in audit pool
- Spam filtering is not an excuse
- A late response = a non-response
- Public information will be leveraged
- Cross referenced information available
- On-site compliance audits more likely
#9 – It’s all about the behavior

- Do you take it seriously
- Are you actively monitoring your Risk Assessment
- Does your Risk Acceptance cadence make sense
- Do you have a robust breach analysis process
- Accountability of vendors
#10 – Use as a catalyst to drive change

- It's here and for real
- Enforcement actions are increasing
- Board level attention
- Integration opportunities
- Implementation of a framework and program
HOW TO PREPARE
What can I do immediately to get ready?

- Determine if you are in scope
- Ensure documentation is updated (P&Ps, training documentation, etc).
- Review OCR templates
- Revisit Risk Assessment to ensure its “comprehensive”
- Have a complete and updated BA list
- Review recent resolution agreements
What else should I consider?

• Educate internal and external stakeholders
• Execute a mock audit (internal or external)
• Demanding proof of compliance from Bas, sub-Bas, etc.
• Implementing a repeatable program leveraging a framework
• Drive further change in the organization
CONTINUED SUCCESS
It needs to be sustainable!

- Compliance does not equal security
- Integration is key
- Leveraging a program and framework
- Periodic check-points
- Robust vendor due diligence program
- Revisit third party assurance approach
Thank you!
Michael Parisi – PwC
Michael.P.Parisi@pwc.com
860-241-7194

Q&A