“HIPAA Audits: How to Be Prepared”

Lindsey Wiley, MHA, CHTS-IM, CHTS-TS
HIT Manager
Oklahoma Foundation for Medical Quality
An Important Reminder

For audio, you **must** use your phone:

**Step 1**: Call (866) 906-0123.

**Step 2**: Enter code 2071585#.

**Step 3**: **Mute your phone!!!**

= AUDIO
Mission of OFMQ

OFMQ is a not-for-profit, consulting company dedicated to advancing healthcare quality. Since 1972, we’ve been a trusted resource through collaborative partnerships and hands-on support to healthcare communities.
OFMQ Service Lines

- Analytics
- Case Review
- Education
- IT Consulting
- Health Information Technology
- National Quality Measures
- Quality Improvement
HIT Service Lines

- Security Risk Assessment- Level 1, 2, and 3
- Meaningful Use Assistance
- Meaningful Use Audit Support
- Risk Management Consulting and Development
- Staff IT Security Training
- Website Development
- IT Consulting
- Cloud Deployment
Lindsey Wiley, MHA, CHTS-IM, CHTS-TS

Lindsey works with healthcare providers and hospitals to advance the use of electronic health records (EHR) to improve patient care and health outcomes. She consults with physician practices and hospitals to successfully implement and meaningfully use EHRs, including assistance associated with vendor products, hardware, software and system configuration and troubleshooting, staffing considerations, workflow analysis, EHR utilization, security and privacy, and quality data reporting from EHR systems.
What is HIPAA?

• Health Insurance Portability & Accountability Act of 1996
• HIPAA Protects Individually Identifiable Health Information
• Protected Health Information (PHI)
• Individually Identifiable Information
Over the Years

1996 - HIPAA
2003 - Privacy Rule
2005 - Security Rule
2009 - Meaningful Use Core measure 14 (EH) 15 (EP)
2012 - Pilot Program Begins
2013 - Major Update of Rules, HIPAA Omnibus (effective March 26 and enforceable September 23)
2014 HIPAA Audits Resuming
Improved Enforcement
Enforcement of HIPAA Regulations

• Turning it up a notch!

• The US Department of Health and Human Services (HHS) is currently implementing audits to meet requirements in the HITECH Act in the American Recovery and Reinvestment Act of 2009 (ARRA) for performing periodic audits of compliance with the HIPAA Privacy and Security Rules.
Who is responsible for the audits?

- Office for Civil Right’s (OCR)
- Responsible for:
  - Administering and enforcing the HIPAA Privacy and Security Rules
  - Conducts complaint investigations
  - Compliance reviews
  - Audits
- OCR works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA
HIPAA Privacy & Security Rule Complaint Process

Complaint → Intake & Review

Possibility of Criminal Violation → DOJ

Accepted by DOJ

DOJ Declines case & refers back to OCR

Resolution

OCR finds no violation
OCR obtains voluntary compliance, corrective action, or other agreement
OCR issues formal finding of violation

Resolution

The violation did not occur after April 14, 2003
Entity is not covered by the Privacy Rule
Complaint was not filed within 180 days and an extension was not granted
The incident described in the complaint does not violate the Privacy Rule
Complaints Received by Calendar Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>12,915</td>
</tr>
<tr>
<td>2012</td>
<td>10,454</td>
</tr>
<tr>
<td>2011</td>
<td>9,022</td>
</tr>
<tr>
<td>2010</td>
<td>8,764</td>
</tr>
<tr>
<td>2009</td>
<td>7,587</td>
</tr>
<tr>
<td>2008</td>
<td>8,729</td>
</tr>
<tr>
<td>2007</td>
<td>8,221</td>
</tr>
<tr>
<td>2006</td>
<td>7,362</td>
</tr>
<tr>
<td>2005</td>
<td>6,866</td>
</tr>
<tr>
<td>2004</td>
<td>6,534</td>
</tr>
<tr>
<td>Partial 2003</td>
<td>3,742</td>
</tr>
</tbody>
</table>
OCR Audit Process

• First small round of pilot audits conducted in 2012 by KPMG involved on-site visits examining broad list of compliance issues.
• OCR will personally resume their HIPAA compliance audit program in 2015 with narrowly focused “desk audits” plus comprehensive on-site audits.
• Fines may be imposed for failure to comply with the HIPAA Rules.
• In the past, Audits were conducted due to probable cause…..that is not the case anymore!
HIPAA Audits

• Focus both on covered entities and business associates
• Hope to audit 350 covered entities, and 50 Business Associates first go-round
• Audits will focus on real-life application of HIPAA policies and procedures across your entire organization
• Staff must know and understand polices and how they relate to their daily activities
HIPAA Audits

OCR will assess compliance efforts through an updated protocol including HIPAA Omnibus Rule changes

Focus

• Risk Analysis and Risk Management
• Breach Notification Rule (including content and timeliness of notifications)
• Notice of Privacy Practice
• Providing patients with access to protected health information
HIPAA Audits 2015 & 2016

OCR projects another round of covered entity audits in 2015 & 2016

2015 Focus

• Computing device and storage media controls
• Transmission security
• HIPAA Privacy Rule Safeguards (workforce training, policies and procedures)

2016 Focus

• Encryption and decryption
• Facility and Physical Access Control
• Other areas of high-risk as identified by 2014 audits
• Breach Reports and Complaints
Selection Process

• Selected covered entities will receive audit notification and data requests in fall 2014 and will be asked to identify their business associates and provide those vendors’ current contact information.

• BA’s will then be selected from those that were identified by the covered entities.
First Round Findings

• Found that a significant number of healthcare providers and healthcare facilities had not completed the risk assessment required by HIPAA Security Rule or taken appropriate measures to address the threats and vulnerabilities identified through their risk assessments

• These foundational issues in safeguarding electronic health information were widespread in smaller health care providers and hospitals
**Improved Enforcement**

- HITECH 13410 Sections:
  - (a), (b): “Willful Neglect” violations
    - Must be investigated, penalties mandatory
    - Interim Final Rule now used in enforcement
  - (c): Distribution of Penalties
    - To provide more enforcement
    - Portion will go to those harmed
Improved Enforcement

• (d): Higher penalties effective for violations after 2/17/09
  – New, four-tier penalty structure with up to $1.5 million maximum for all violations of the same provision in a calendar year
• (e): State Attorneys General may bring HIPAA action
• (f): Continued corrective action allowed, even if no penalty
Tiered Penalty Structure 1 of 4

- 160.404 Penalty Amounts
  Tier 1: Didn’t know and, with reasonable diligence, would not have known (Accident)
  - $100-$50,000 per violation
  - $1.5 Million max for all violations of a similar type in a calendar year
  - Reasonable Diligence: Different person under same circumstances would have created same outcome
Tiered Penalty Structure 2 of 4

• Tier 2: Violation due to reasonable cause and not willful neglect (Accident but knew right away what happened)
  – $1000-$50,000 per violation
  – $1.5 million maximum for all violations of a similar type in a calendar year
  – Reasonable Cause: Circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated
Tiered Penalty Structure 3 of 4

• Tier 3: Violation due to willful neglect AND CORRECTED within 30 days of when known or should have been known with reasonable diligence
  – $10,000-$50,000 per violation
  – $1.5 million maximum for all violations of a similar type in a calendar year

  – Willful Neglect: Conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated
Tiered Penalty 4 of 4

• Tier 4: Violation due to willful neglect and **NOT CORRECTED within 30 days** of known or should have been known with reasonable diligence
  – $50,000 per violation
  – $1.5 Million maximum for all violations of a similar type in a calendar year
  – Note: Penalties can be levied on a daily basis so adding up to 1.5 Million is easy
Teeth in Enforcement

• $4.3 Million fine for Cignet health of Maryland for multiple HIPAA violations, INCLUDING ignoring OCR investigators
• $4.8 Million fine for New York and Presbyterian Hospital and Columbia University for failing to secure thousands of patients electronic ePHI held on their network.
• $865,000+ settlement with UCLA Medical Center for snooping in celebrity records
• Multiple Multi-million dollar settlements with pharmacies
• $100,000 settlement with physician’s office for Security Rule Violations
• $1.5 Million settlement with BCBS of Tennessee for lost hard drives
• $1.7 million settlement with Alaska Medicaid for laptop and security compliance issues
Audit Prep

• Do it NOW, not when you are called upon
• Be ready to answer their questions
• Monitor for additional questions and requests as they are released; the process will evolve!
• Consider partnering with an entity who can provide third-party review of your processes
Audit Nuts and Bolts

• Show you have in place all the policies and procedures required by HIPAA
• Show you have been using them
• Three week notice – you must be prepared in advance or it is too late – you have 15 days to provide any paper requests
SAMPLE Security Audit Content

• Below is a list of items that auditors wanted information on within 10 days. Specifically, asked to provide policies and procedures for:
  – Prevention, detection, containment and correction of security violations (incident reports)
  – Background checks, confidentiality agreements
  – Authentication methods used to ID users
  – List of individuals with access to system(s) (updated regularly)
  – Physical, workstation, and network security
  – Data encryption
  – Wireless networking
  – Internet usage
SAMPLE Security Audit Content

- Sanctions (what happens to an employee who makes a mistake)
- Session termination (timeouts)
- Password management
- Disposal of media/devices
- Wireless security
- Computer patch management
- Anti-virus software
- Security Plan
- Baseline Risk Analysis
- Vulnerability Scans, configuration standards
- Network diagram
SAMPLE Security Audit Content

• Additional Documents/Lists:
  – Terminated employees
  – New hires
  – Encryption mechanisms used for ePHI
  – Software used to manage and control access to the internet
  – Users with remote access
  – Database security requirements and settings
Approaching the Audit

• Don’t Panic
• Seek guidance (don’t tackle it alone)
• Get policies and procedures in place
• Get documentation in place
• Tackle a self-audit only if you are ready – an outside perspective is helpful
Top 5 Issues in Investigated Cases Closed with Correction Action
<table>
<thead>
<tr>
<th>Year</th>
<th>Issue 1</th>
<th>Issue 2</th>
<th>Issue 3</th>
<th>Issue 4</th>
<th>Issue 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Mitigation</td>
</tr>
<tr>
<td>2012</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Mitigation</td>
</tr>
<tr>
<td>2011</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Mitigation</td>
</tr>
<tr>
<td>2010</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Complaints</td>
<td>Minimum Necessary</td>
</tr>
<tr>
<td>2009</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Complaints to Covered Entity</td>
</tr>
<tr>
<td>2008</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Complaints to Covered Entity</td>
</tr>
<tr>
<td>2007</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Notice</td>
</tr>
<tr>
<td>2006</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Notice</td>
</tr>
<tr>
<td>2005</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Mitigation</td>
</tr>
<tr>
<td>2004</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Safeguards</td>
<td>Access</td>
<td>Minimum Necessary</td>
<td>Authorizations</td>
</tr>
<tr>
<td>partial year 2003</td>
<td>Safeguards</td>
<td>Impermissible Uses &amp; Disclosures</td>
<td>Access</td>
<td>Notice</td>
<td>Minimum Necessary</td>
</tr>
</tbody>
</table>
Wait... Does Complying With Standards Really Ensure Compliance?

- Standards MUST be used but do NOT ensure compliance in and of themselves
- PEOPLE ensure compliance, interpret your policies and procedures, and are your first line of defense in security
- An Institutional Culture of Privacy and Security is required to ensure compliance with the Privacy and Security Rules
Perspective

• As the Audit noose tightens, providers must BALANCE through acts of judgment:
  • Confidentiality of Information - how secure is your information
  • Integrity of Information - how valid and correct is your information
  • Availability of Information - who can see it who can’t
Risk-Based Process

- Risk Management Program
  - the big picture view, needed for planning
- Risk Assessment is REQUIRED
  - the micro view, assess each system and flow
- Both
  - Provides basis for decision-making
  - Cornerstone of the compliance process
How are others preparing for Audit?

• HIPAA IS A PROJECT, FOREVER
  – Plan the work, schedule it, follow-up
  – Committing staff and getting outside help
  – Getting support from all levels of facility

• Community Strategies
  – Sharing experiences
  – Working on community solutions
  – Conducting DRILLS
Conducting Drills

• WHY...to prepare for the unknown
  – You must be prepared for incidents to occur
  – You will not have time to figure out what to do
  – People will be upset and confused
  – You need to call on experience gained in practice
Recommendations
Recommendations

**Establish a Team:**

- Who will assume the role of Risk Management and Mitigation moving forward?
- A team approach to Risk Management has proven to be the most successful
- Determine your subject matter experts who can best contribute to the improvement of Risk Management processes
Recommendations

Review the results:

• The team needs to focus efforts on impacts and threats rated as HIGH, then MEDIUM.

• MUST TAKE ACTION on the results.

• Policy and organizational standards must be taken into consideration, and in some cases the recommendations made by the OFMQHIT team become unattainable.
Recommendations

Empower the team:
• Encourage your Risk Mitigation team to verbalize all ideas on problem resolution.
• Developing controls for threats and vulnerabilities should be a group task.

Document:
• Dates, times, agendas, meeting minutes, and of course updates directly to the report and results provided to you by OFMQHIT.
Consider decisions: Will you Mitigate, Transfer, or Accept Risk that has been reported to you?

– Mitigate: Reduction of risk by implementing the recommended controls
– Transfer: Outsource the issue, or insure against any possible loss
– Accept: The team has considered and discussed the reported issue and consider the risk to be acceptable
Your To-Do List

• Don’t be in denial – willful neglect will cost you
• Ignorance is no longer an excuse or option
• Prepare for breach notification
• Review your policies and procedures per rules
• Do Risk Analysis, use a third party if you can
• Don’t use generic policy – customize!
• DOCUMENT
• Conduct drills in audit and breach response
• Make corrections based on results
• Always have a plan for moving forward, AND FOLLOW IT
Opportunities for OFMQ’s Help

OFMQ has received several grant opportunities to help Oklahoma primary care practices. If you are seeking to improve patient care while utilizing your EHR, contact us to sign up!

Send an email to OFMQHIT@OFMQ.COM
Questions & Answers

If you’re interested in improving your practice and office efficiency through EHR software use or our service lines, contact us!

Email: ofmjqhit@ofmq.com
Call: (877) 963-6744
Visit: www.OFMQ.com
Upcoming WebEx Seminar

Wed, May 13 | 12:15pm (Central Time)
“Stage 3 Meaningful Use for Providers & Hospitals”

Register at www.ofmq.com/event-month
Thank you!