Today’s Topics

1. OCR Phase 2 Audits
2. Lessons from OCR Enforcements
3. Risk Analysis and Risk Management
4. Ransomware
5. Cyber Insurance
6. Implementing Guardrails – Stopping Compliance Issues Before They Begin
Phase 2 Audits Underway

- OCR currently desk-auditing 167 CEs
- HIPAA Rule requirements selected for review
- OCR released audit schedule
- Recent OCR guidance documents

Desk Audit Flow Cycle

- OCR sends prescreening questionnaire (CEs requested to identify BA) Desk pool formed, auditees selected
- OCR notifies audit and requests documents (July 11, 2016: 167 CEs notified of selection)
- Auditee returns written comments on OCR draft report within 10 business days
- OCR reviews auditee’s documents; issues draft compliance report (October 2016: 40-50 BAs notified of desk audits)
- Auditee submits documents through OCR ePortal within 10 business days
- OCR issues final audit report within 30 days of auditee response
- Desk audit pools formed, auditees selected
- OCR notifies auditee of desk audit and requests documents
- Auditee returns written comments on OCR draft report within 10 business days
- OCR issues final audit report within 30 days of auditee response

Site Audit Flow Cycle

- Expected early 2017: CE/BA site audits begin
- Entrance conference: OCR provides information and expectations
- 3-5 day on-site audit
- OCR issues draft findings
- Site audits complete: ???
Public Postings?

- OCR does not intend to publicize auditees’ identities or auditee-specific findings.
- OCR believes there is a FOIA exception, but “may” be required to disclose “audit notification letters and other information about these audits ...”

Will Audits Lead to Fines/Enforcement?

- What is OCR’s stated purpose for audits?*
- What is OCR’s stated objective for audits?**
- But ... what does OCR say about enforcement?*

* From OCR’s July 13, 2016 webinar for CE desk auditees
** From OCR’s Q&A set

Lessons from OCR Enforcements
Lesson 1: Protect Paper
Cornell Prescription Pharmacy – April 2015 (RA/CAP and $125,000 resolution amount)
PHI disposed of in open container on CEs’ premises

Lesson 2: Consider Encryption/Manage Offsite PHI
QCA Health Plan, Inc. – April 2014 (RA/CAP and $250,000 resolution amount)

Lesson 3: Perform an Enterprise-Wide Risk Analysis
Lesson 4: Properly Manage and Use SaaS and Cloud Storage Options

Security Rule: Ensure confidentiality, integrity, availability of ePHI
CE/BA “creates, receives, maintains, or transmits”

St. Elizabeth’s Medical Center – June 2015 (RA/CAP and $218,000 resolution amount)

Lesson 5: Ensure Proper Access Management

Former workforce members employed by a competitor accessed proprietary database containing ePHI (access rights not terminated upon leaving employment)

Triple-S Management Corporation – Nov. 2015 (RA/CAP and $3.5M resolution amount)

OCR’s SMALL BREACH INITIATIVE

“Initiative to more widely investigate breaches affecting fewer than 500 individuals.” (August 18, 2016)

Lesson 6: Size Doesn’t Matter (Much)
Phoenix Cardiac Surgery – April 2012 (RA/CAP, $100,000 resolution amount)

One-location, two-physician practice

“This case is significant because it highlights a multi-year, continuing failure on the part of this provider to comply with the requirements of the Privacy and Security Rules … We hope that health care providers pay careful attention to this resolution agreement and understand that the HIPAA Privacy and Security Rules have been in place for many years, and OCR expects full compliance no matter the size of a covered entity.”

Catholic Health Care Services – June 2016 (RA/CAP and $650,000 resolution amount)

• First settlement directly with a BA
• BA employee’s unencrypted iPhone, containing 412 individuals’ “extensive” ePHI, stolen
• OCR investigation: (1) failure to perform SR risk analysis; (2) failure to implement SR risk management plan; (3) no policies/procedures addressing removal of mobile devices from premises

Lesson 7: Emphasize Access

• Access Rule
• Top “Pilot Audit” finding
• 2016 OCR Guidance
• Phase 2 area of inquiry
• Document requests to Phase 2 CE desk auditees?
Risk Analysis and Risk Management

Risk Analysis and Risk Management Plan

- **Risk Analysis:** “accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of” PHI
- **RMP:** “security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level”
- Security Rule builds flexibility into RA process
- Start with a data inventory/map (location and flows)

Ransomware
What Does It Look Like?

From: 
Sent: 
To: 
Subject: 
Attachment: 

Dear [Recipient],

Your personal files are encrypted!

Your personal files are encrypted and cannot be opened using standard file decryption techniques. To recover your files, you must install the recommended decryption tool by accessing the file located at [Encrypted File Location].

Please contact [Contact Information] for further assistance.

Thank you,

Joe

Malware: Most Used Email Lures

Source: ProofPoint, The Human Factor 2016
How to Prevent?

Suggestions for Businesses

• Enforce an effective password policy
• Use two-factor authentication for remote access
• Use regular, out-of-band backups
• Have an incident response plan
• Protect mobile devices
• Educate employees

How to Prevent?

Suggestions for Individuals

• Do not open email messages or attachments from unknown individuals.
• Be cautious of clicking links within emails from unknown individuals.
• Implement technical safeguards.
• Think before you click!

HHS FACT SHEET: Ransomware and HIPAA

• HIPAA Security Rule requires implementation of security measures to help prevent ransomware
• The HIPAA Security Rule requires policies and procedures to recover from a ransomware attack

“Unless the covered entity or business associate can demonstrate that there is a ‘...low probability that the PHI has been compromised,’ based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred.” – OCR Fact Sheet
Basic “Cyber” or “Tech” Insurance

Third-Party Coverages
- Tech E&O
- Network Security
- Data Breach
- Computer Crime
- Computer Fraud & FTF

First-Party Coverages
- Data Restoration
- Network Interruption
- Extortion

Implementing Guardrails – Stopping Compliance Issues Before They Begin
IMPLEMENTING GUARDRAILS

• Perform an enterprise-wide risk analysis, and follow up with an appropriate risk management plan.
• Mind your Ps and Qs – and PEDs
• Ensure individuals’ access to their own PHI – and mind what you charge!
• “Minimum necessary” is maximally important. Think through role-based access and uses, disclosures, and requests.
• Train and train again. Changes in law, organizational structure, and risks/vulnerabilities may require immediate re-training. Document efforts.

What Can Your Organization Do Now?

1. Keep Momentum Strong: It Doesn’t Stop With Phase 2
2. Learn From Enforcements – And Beyond:
   a. Security Management Process (RA + RMP)
   b. Portable Electronic Device Security
   c. Access Rights
   d. Business Associates
3. Ensure Buy-In:
   a. Engage C-suite and board
   b. Build culture of compliance – Keep privacy and security fresh
4. Train Your Workforce: Issue in almost every enforcement
5. Learn From Your Peers: Find opportunities to connect

Questions

TWENTY QUESTIONS

IceMiller.com

icemiller.com
Thank You!

- Stephen Reynolds
  - Stephen.Reynolds@icemiller.com
- Kim Metzger
  - metzger@icemiller.com