Disclaimer

- The information provided in this presentation does not constitute legal advice and is intended to be used for guidance.
- If you require legal advice, please consult with a healthcare attorney

Message

I am here for your benefit. If you have questions, please ask.
1. Background
2. The Audit
3. Lessons Learned
Background

S.M.O.G.
November 15, 2011
- Senior Management Operations Group
- Catching up on email
- November 9th email from OCR listserv:

OCR Listserv
The email

From: Privacy Officer
Date: 11/15/11, 3:30 p.m.
Subject: Are you sitting down?
“We are scheduled for a KPMG audit on 12/5. We did not receive the letter mailed on Nov. 4. I just received a phone call from Tim XXXX who is e-mailing me the letter. Cancel my vacation request for Friday.”

Timeline

• November 4, 2011 – Certified Letter from OCR/KPMG addressed to “Privacy Office” 800 Rose St.
• November 8/9, 2011: OCR Listserve notification of audit program
• November 15th – Call from KPMG: “Did you get our letter?” (What letter?)
• “10 days are up tomorrow.”

“Submit”
OCR News Release

- The information about OCR HIPAA Audits is very accurate. [http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html](http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html)
- KPMG is very professional.
- Communication about expectations are very clear.

Background

- American Recovery and Reinvestment Act – HITECH Act §13411 Audits and Breach Notification
- Booz Allen Hamilton
- KPMG
  - Develop, assess, pilot program
  - Business Associates

Background

- 20 HIPAA Covered Entities for pilot
- Including:
  - Health plans
  - Clearinghouses
  - Big and small providers
  - Business Associates
Background

• Four levels
  – Large Provider Payer
  – Large Regional Hospital System
  – Community hospitals, outpatient clinics
  – Small providers, community or rural

The Audit

OCR Audit Program

• Press release/website is very accurate
• KPMG does an excellent job of communicating expectations
• Periodic meetings to discuss findings
• No surprises
• Two teams:
  – Privacy
  – Security
Performance Audit

“The overall objective of the audit is to gain an understanding as to whether your organization has key processes or controls to facilitate reasonable adherence with the HIPAA Privacy and Security Rules.”

Performance Audit

Professional standards require:
• Obtain sufficient evidence, which must support findings based on the criteria (HIPAA Privacy and Security Rules)
• Request documentation,(x3)
• Reviews of policies and procedures
• Interview officials
• Observe activities
• Document findings
• Discuss Fraud awareness and processes

Process

• Notification Letter
• Information submission
• Notification of on-site review (x3)
• On-site meeting to discuss scope
• Privacy Meeting Agendas
• Security Meeting Agendas
• Review and observation of controls
Request for Information

- Policies and Documentation
  - Privacy
  - Security
- Documentation of complaints
- Documentation of audit plan
- Documentation of compliance work plan
- Compliance/Privacy structure

On-Site

- Room for the team, lockable, for 10 members
- Printer
- Network access/WWW/Wireless
- Security badges
- Contact information for key officials

On-Site

- Documentation requests
  - Same advice, please number and track
  - Email, not hardcopy,
  - Plan for managing information*
Planning Meeting

• All members, KPMG, Institution
• Privacy breakout
• Security breakout

Privacy Agenda

• NPP
• Requests for Privacy Protection
• Access
• Breach Notification
• Administrative Requirements
  — Policies and Procedures
  — Sanctions
  — Mitigation
  — Retaliation Acts

Security Agenda

• Administrative Safeguards
• Physical Safeguards
• Technical Safeguards
Expectations

• Data requests are everything you would expect (only one surprise)

Lessons Learned

Documentation Requests

• The initial request is not numbered
  − Recommend that you number them and refer to them by request number
• On site request are not numbered
  − Recommend that you number them and refer to them by request number
Documentation Requests

- Keep track of what you send them
  - Time date
  - Recipient (2 teams, multiple individuals)
  - Multiple requests for the same item

Interaction

- Privacy/Security Officer accompany auditors on all interviews.
- Take notes during the interview

Breach Notification

- They will ask you for an “incident” or a Breach
- Be prepared to walk them through the analysis
- Document your process
- Document your analysis
- Document all of your actions and circumstances
The Surprise

Fraud and Awareness Processes

“Professional standards require us to consider fraud and abuse in the design of our audit procedures and to inquire about the organization’s fraud awareness and anti-fraud procedures.”

- Risks and risk assessment.
- Procedures to identify fraud.
- How are reports fraud handled/communicated?
- How are employees made alert to the possibilities of fraud?

FRAUD

- Risks and risk assessment?
- Procedures to identify fraud?
- How is fraud treated when reported and communicated?
- How are employees made alert to the possibilities of fraud and how to identify and prevent it?
The Representation Letter

- 4 pages
- 12 affirmations
- “no violations”
- “unasserted claims”
- “no deficiencies”
- “we have no knowledge of any fraud or suspected fraud...”

General Impressions

- Scope is interesting (hospital vs. system)
- Integrated medical records
- Depth of health care operations
- Don’t assume
- Be prepared to “paper” your entire program
- Lack of activity? Document it. (denial medical records, de-identification)
- Are you different? State laws, etc.

Recommendations

- Paper your program
- Validate your program
- Document your audit plan
- Defend your program/audit plan (benchmark, peers, HCCA, HFMA, etc)
- Investigations/Mitigations
- HR: New employees, terminated employees
**Recommendations**

- Remind workforce/compliance personnel of policy on inquiries/investigations
- Be truthful
- Don’t assume they know your operations
- Be mindful of the scope: hospital vs. ambulatory, etc.

**Other Considerations**

- Let all potential parties know what to expect and the importance (HR, IA, IT, etc)
- Conduct a robust assessment...Regularly
- Diagrams
  - Flow of information
  - Organization
  - Compliance program structure
  - Affiliates

**Other Considerations**

- Overarching ERM / Compliance Plan
- Vendors
- Business Associates
- Track changes:
  - Education
  - Change in policy or business direction
The List

- Policies and Procedures
- Workforce training, new and regular
- Audit program, check effectiveness, regularly
- Risk Analysis and mitigation
- Incident response:
  - Compliance
  - Breach/Incident

Recommendations

- Beware vendor stories
- Business Associates
  - Survey the landscape

Resources

- Mark M. Johnson, National HIPAA Services Director: “2012 HIPAA Privacy and Security Audit Readiness”
- ID Experts: Prepared for HIPAA Audit?
- HIPAA COW
- 2012 HIPAA Privacy and Security Audits (http://csrc.nist.gov/news_events/hipaa_june2012/day2/day2-2_banches_ocr-audit.pdf)
OCR Data

- Linda Sanches:
  - 65% Security
  - 26% Privacy
  - 9% Breach

Thank You

Roger Brett Short
Chief Compliance Officer
University of Kentucky
UK HealthCare
Brett.short@uky.edu

Questions?