Today's Topics

1. Background: OCR's Phase 2 Audit Program
2. Key Compliance Areas Under OCR's Scrutiny
3. Tips for Undergoing an OCR Phase 2 Audit
4. Recent OCR Enforcement Actions: Lessons Learned

Background: OCR's Phase 2 Audit Program

OCR's Compliance and Enforcement Tools

- Education and Outreach
- Investigations
  - Complaint investigations
  - Compliance reviews
    - Triggered by breach reports, news reports, referrals, etc.
    - Automatically opened for breaches affecting 500 or more individuals
- Audits
  - HITECH Act of 2009, Section 13411 requires HHS to conduct *periodic audits* of covered entities' and business associates' compliance with HIPAA Rules

OCR's Audit Program: Phase 1

- OCR conducted pilot audit program in 2011 and 2012
- Audited 115 covered entities for compliance with all aspects of HIPAA Rules
  - 61 health care providers, 47 health plans, 7 health care clearinghouses
- Every audit involved an on-site review
- OCR used results, in part, to improve audit program design

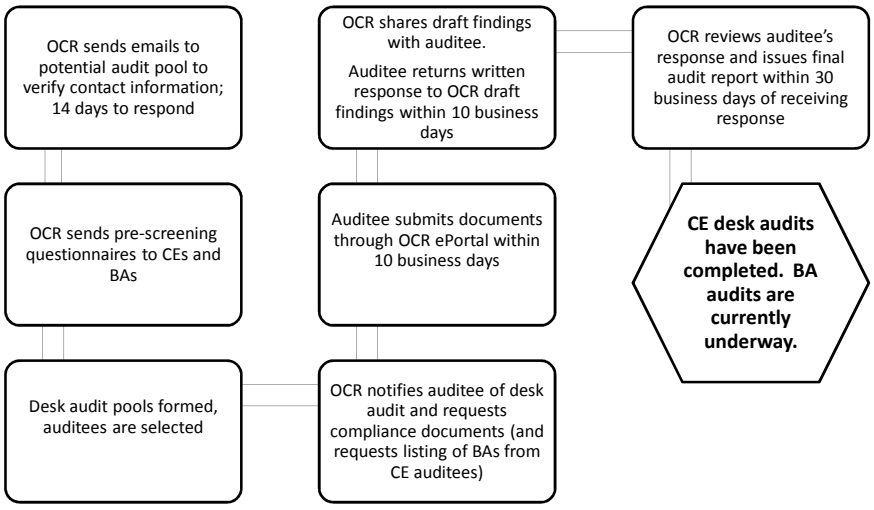
OCR's Audit Program: Phase 2

- OCR launched Phase 2 in Summer 2016
- Phase 2 consists of both desk audits and on-site reviews
- Stated goal of Phase 2:
  - "[E]xamine mechanisms for compliance, identify best practices, discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews, and enable us to get out in front of problems before they result in breaches"
- OCR may open up compliance review, which may lead to enforcement action, if (1) entity is uncooperative, or (2) egregious compliance concerns uncovered.

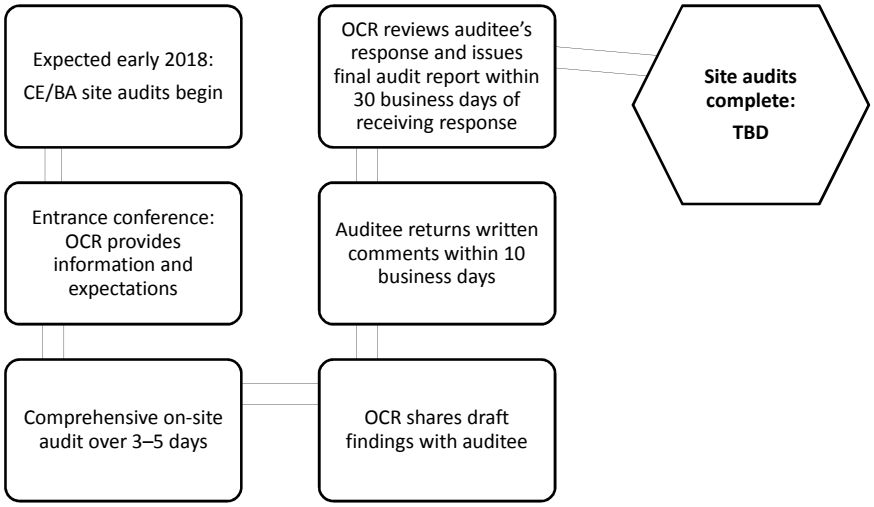
OCR's Audit Program: Phase 2

- Phase 2 covers both covered entities (CEs) and business associates (BAs)
- CE selection pool criteria:
  - Size and type of entity (public or private, affiliation with other health care organizations, etc.)
  - Geographic factors
  - Present enforcement activity with OCR
- BA selection pool largely based on CE auditees' lists of BAs
- Random sampling used to select auditees from audit pools
  - 167 CEs selected for desk audits

Desk Audit Process



Site Audit Process



IceMiller® LEGAL COUNSEL

9

icemiller.com

Conclusion of Phase 2 Audits

- OCR will aggregate and analyze Phase 2 findings and issue high-level report to public
- OCR does not intend to publicize auditees' identities or auditee-specific findings.
- FOIA exception may apply, but OCR but may be required to disclose "audit notification letters and other information about these audits upon request by the public"
- OCR will use Phase 2 results to (1) develop targeted guidance, (2) strengthen permanent audit program, (3) open compliance reviews when it deems necessary

IceMiller® LEGAL COUNSEL

10

icemiller.com

OCR Audit Reports: Compliance Ratings

Compliance Effort Ratings—Legend*

Rating	Description
1	The audit results indicate the entity is in compliance with both goals and objectives of the selected standards and implementation specifications.
2	The audit results indicate that the entity substantially meets criteria; it maintains appropriate policies and procedures, and documentation and other evidence of implementation meet requirements.
3	Audit results indicate entity efforts minimally address audited requirements; analysis indicates that entity has made attempts to comply, but implementation is inadequate, or some efforts indicate misunderstanding of requirements.
4	**Audit results indicate the entity made negligible efforts to comply with the audited requirements (e.g. policies and procedures submitted for review are copied directly from an association template; evidence of training is poorly documented and generic).**
5	**The entity did not provide OCR with evidence of serious attempt to comply with the Rules and enable individual rights with regard to PHI.**

* Source: OCR/NIST Conference, Sept. 6, 2017, Washington D.C.

Key Compliance Areas Under OCR's Scrutiny

Covered Entities: Desk Audits

Requirements Selected for CE Desk Audit Review	
Privacy Rule	Notice of Privacy Practices and Content Requirements [§164.520(a)(1) & (b)(1)]
	Provision of Notice – Electronic Notice [§164.520(c)(3)]
	Right to Access [§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)]
Breach Notification Rule	Timeliness of Notification [§164.404(b)]
	Content of Notification [§164.404(c)(1)]
Security Rule	Security Management Process – Risk Analysis [§164.308(a)(1)(ii)(A)]
	Security Management Process – Risk Management [§164.308(a)(1)(ii)(B)]

Business Associates: Desk Audits

Requirements Selected for BA Desk Audit Review	
Breach Notification Rule	Notification by a Business Associate [§164.410]
	Content of Notification [§164.404(c)(1)]
Security Rule	Security Management Process – Risk Analysis [§164.308(a)(1)(ii)(A)]
	Security Management Process – Risk Management [§164.308(a)(1)(ii)(B)]

Tips for Undergoing an OCR Phase 2 Audit

Tip 1: Documentation

- Respond to OCR's document requests with documentation that became effective *prior to* date of request
  - Cannot create new documentation within 10-day response period
- Remember HIPAA Rules' 6-year retention period for compliance documentation
  - OCR may request documents generated during the past 6 years
- Know where your documentation is located in order to meet 10-day deadline for response
- Policies and procedures must be tailored to entity's unique environment

Tip 2: Cooperate with OCR Auditors

- Meet all deadlines
- If you are unable to meet a request, explain rationale for not having the requested documentation
- Provide thoughtful responses to OCR's initial audit findings
- Don't make false or misleading statements to OCR or backdate compliance documentation
- Ensure that the on-site audit process will run smoothly

Tip 3: Evidence of Implementation

- Ensure that you have documentation sufficient to demonstrate *implementation* of HIPAA policies and procedures
- In addition to policies and procedures, OCR may request copies of NPP receipt acknowledgements, training materials, evidence of workforce training, access request forms, Breach Notification Rule risk assessments, etc.
- During on-site audits, OCR may interview workforce members to determine sufficiency of training

Tip 4: Security Rule Compliance

- At a minimum, OCR will request the following Security Rule compliance documentation:
  - Risk analysis (identify potential risks and vulnerabilities to ePHI)
  - Risk management plan (implement security measures to reduce identified risks to reasonable and appropriate level)
- Ensure you are able to produce: (1) current and previous versions; (2) policies and procedures for conducting risk analysis; (3) evidence risk analysis is periodically reviewed and updated; (4) procedures for making risk analysis and risk management plan available to appropriate workforce members

Tip 5: Know Your Business Associates

- Be prepared to provide an inventory of all your BAs to OCR
- Ensure that you have entered into compliant BA agreements with all identified BAs
- Incorporate risks and vulnerabilities introduced by BA use of your ePHI into Security Rule risk analysis
- BAs should take same measures with respect to subcontractors

Lessons Learned from Recent OCR Enforcement Actions

Presence Health (January 2017)

- $475,000 settlement and corrective action plan
- First OCR enforcement action focusing exclusively on untimely breach reporting
- Lessons Learned:
  - Need clear policies and procedures for responding to both large and small breaches
  - Important for breach notifications to be provided in timely manner

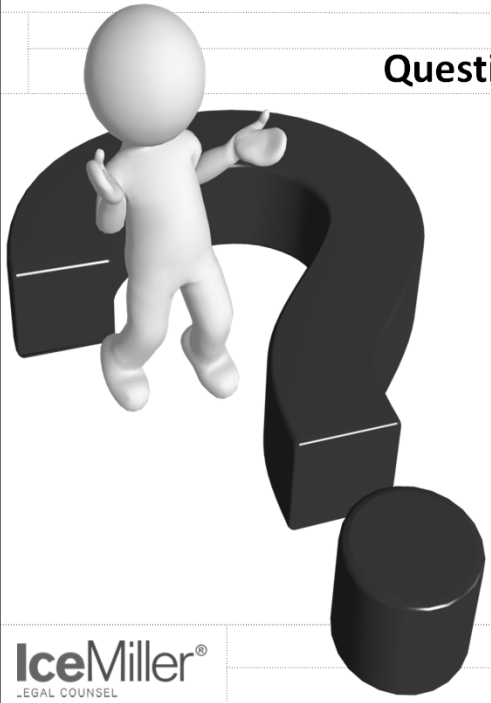
St. Joseph Health (October 2016)

- $2.14 million settlement and corrective action plan
- Newly purchased server included file-sharing application with a default setting allowing "anyone with an Internet connection" to access files. Public had unrestricted access to 31,000 individuals' ePHI.
- Lessons Learned
  - HIPAA Security Rule *evaluation standard* required CE to evaluate impact of new server to security of ePHI before using server
  - Risk analysis may need to be updated if evaluation standard is triggered

North Memorial Health Care (March 2016)

- $1.55 million settlement and corrective action plan
- Breach occurred at BA, triggering OCR investigation into CE. CE failed to enter into BAA with BA before disclosing PHI to BA. CE also failed to conduct a comprehensive, enterprise-wide risk analysis.
- Lessons Learned:
  - Vendor management is critical—OCR is carefully looking into whether compliant BAAs are in place
  - Risk analyses are often deficient because they are not comprehensive in scope

Questions?



Deepali Doddi
(312) 726-7134
deepali.doddi@icemiller.com