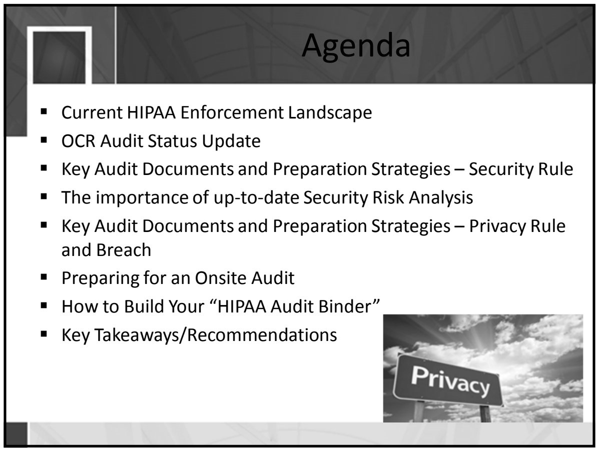
POLSINELLI

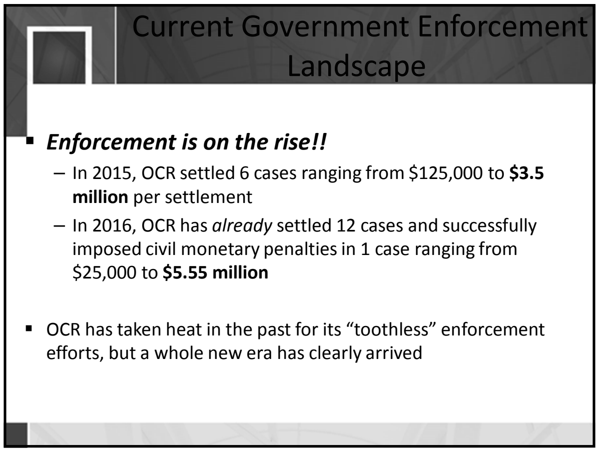
HIPAA Audits Are Here to Stay – Key Preparation Strategies for Business Associates and Covered Entities

Lisa Acevedo | *Shareholder, Polsinelli PC*
Katie Kenney | *Attorney, Polsinelli PC*



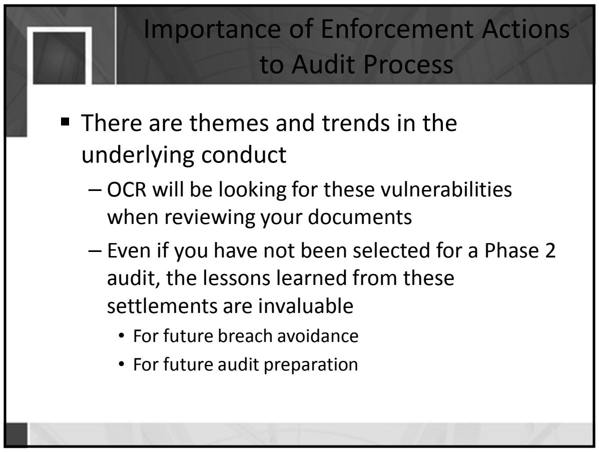
Agenda

- Current HIPAA Enforcement Landscape
- OCR Audit Status Update
- Key Audit Documents and Preparation Strategies – Security Rule
- The importance of up-to-date Security Risk Analysis
- Key Audit Documents and Preparation Strategies – Privacy Rule and Breach
- Preparing for an Onsite Audit
- How to Build Your "HIPAA Audit Binder"
- Key Takeaways/Recommendations



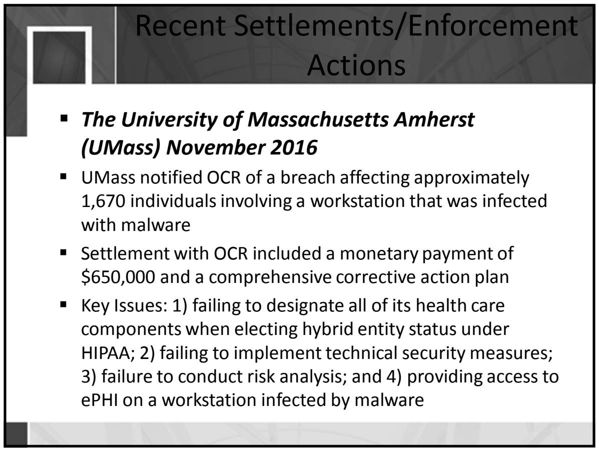
Current Government Enforcement Landscape

- ***Enforcement is on the rise!!***
  - In 2015, OCR settled 6 cases ranging from $125,000 to **$3.5 million** per settlement
  - In 2016, OCR has *already* settled 12 cases and successfully imposed civil monetary penalties in 1 case ranging from $25,000 to **$5.55 million**
- OCR has taken heat in the past for its "toothless" enforcement efforts, but a whole new era has clearly arrived



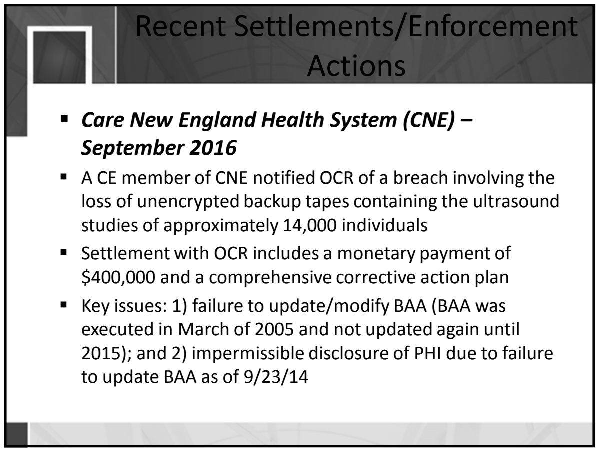
Importance of Enforcement Actions to Audit Process

- There are themes and trends in the underlying conduct
  - OCR will be looking for these vulnerabilities when reviewing your documents
  - Even if you have not been selected for a Phase 2 audit, the lessons learned from these settlements are invaluable
    - For future breach avoidance
    - For future audit preparation



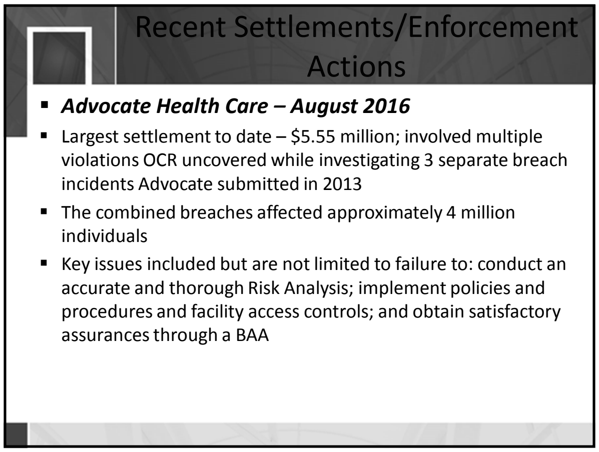
Recent Settlements/Enforcement Actions

- ***The University of Massachusetts Amherst (UMass) November 2016***
- UMass notified OCR of a breach affecting approximately 1,670 individuals involving a workstation that was infected with malware
- Settlement with OCR included a monetary payment of $650,000 and a comprehensive corrective action plan
- Key Issues: 1) failing to designate all of its health care components when electing hybrid entity status under HIPAA; 2) failing to implement technical security measures; 3) failure to conduct risk analysis; and 4) providing access to ePHI on a workstation infected by malware



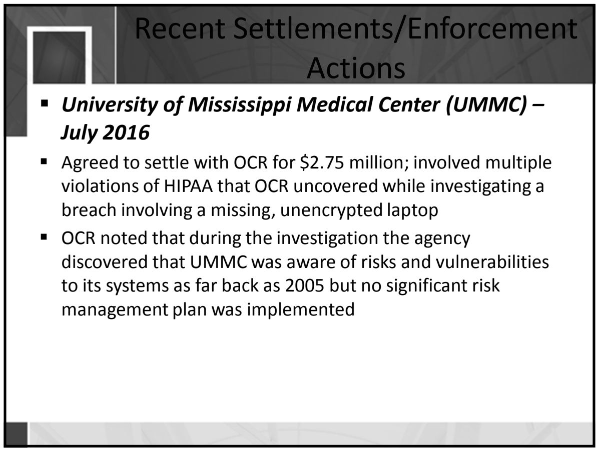
Recent Settlements/Enforcement Actions

- ***Care New England Health System (CNE) – September 2016***
- A CE member of CNE notified OCR of a breach involving the loss of unencrypted backup tapes containing the ultrasound studies of approximately 14,000 individuals
- Settlement with OCR includes a monetary payment of $400,000 and a comprehensive corrective action plan
- Key issues: 1) failure to update/modify BAA (BAA was executed in March of 2005 and not updated again until 2015); and 2) impermissible disclosure of PHI due to failure to update BAA as of 9/23/14



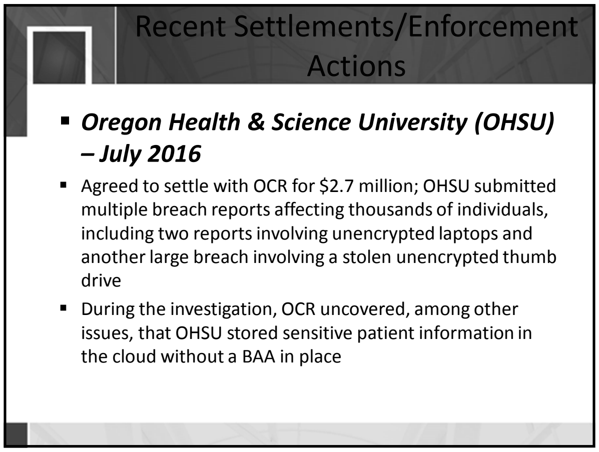
Recent Settlements/Enforcement Actions

- ***Advocate Health Care – August 2016***
- Largest settlement to date – $5.55 million; involved multiple violations OCR uncovered while investigating 3 separate breach incidents Advocate submitted in 2013
- The combined breaches affected approximately 4 million individuals
- Key issues included but are not limited to failure to: conduct an accurate and thorough Risk Analysis; implement policies and procedures and facility access controls; and obtain satisfactory assurances through a BAA



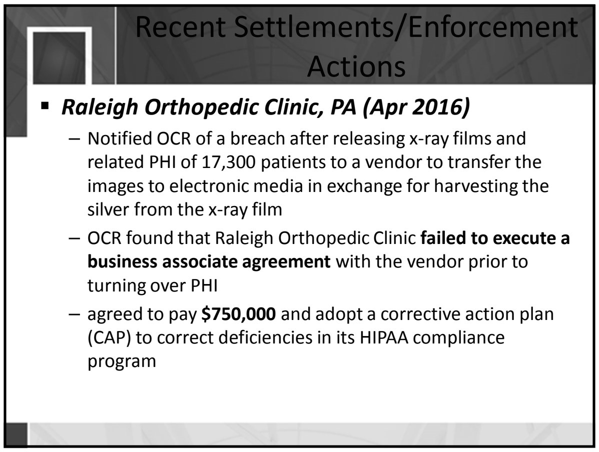
Recent Settlements/Enforcement Actions

- ***University of Mississippi Medical Center (UMMC) – July 2016***
- Agreed to settle with OCR for $2.75 million; involved multiple violations of HIPAA that OCR uncovered while investigating a breach involving a missing, unencrypted laptop
- OCR noted that during the investigation the agency discovered that UMMC was aware of risks and vulnerabilities to its systems as far back as 2005 but no significant risk management plan was implemented



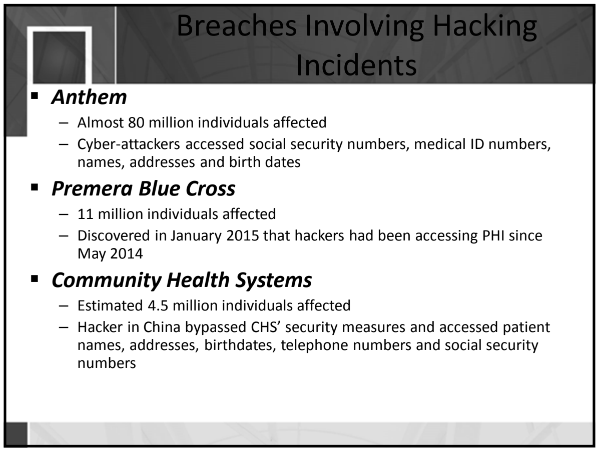
Recent Settlements/Enforcement Actions

- ***Oregon Health & Science University (OHSU) – July 2016***
- Agreed to settle with OCR for $2.7 million; OHSU submitted multiple breach reports affecting thousands of individuals, including two reports involving unencrypted laptops and another large breach involving a stolen unencrypted thumb drive
- During the investigation, OCR uncovered, among other issues, that OHSU stored sensitive patient information in the cloud without a BAA in place



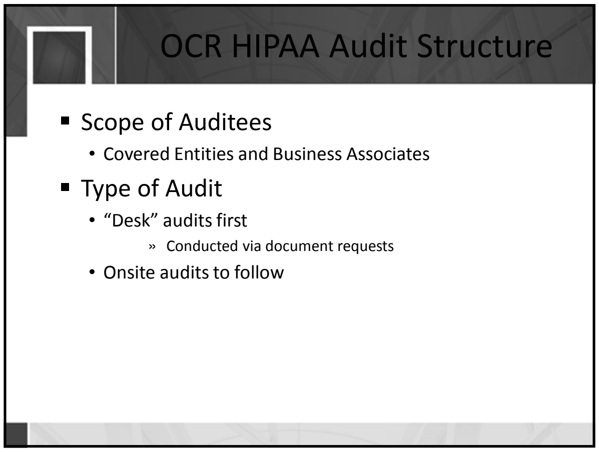
Recent Settlements/Enforcement Actions

- ***Raleigh Orthopedic Clinic, PA (Apr 2016)***
  - Notified OCR of a breach after releasing x-ray films and related PHI of 17,300 patients to a vendor to transfer the images to electronic media in exchange for harvesting the silver from the x-ray film
  - OCR found that Raleigh Orthopedic Clinic **failed to execute a business associate agreement** with the vendor prior to turning over PHI
  - agreed to pay **$750,000** and adopt a corrective action plan (CAP) to correct deficiencies in its HIPAA compliance program



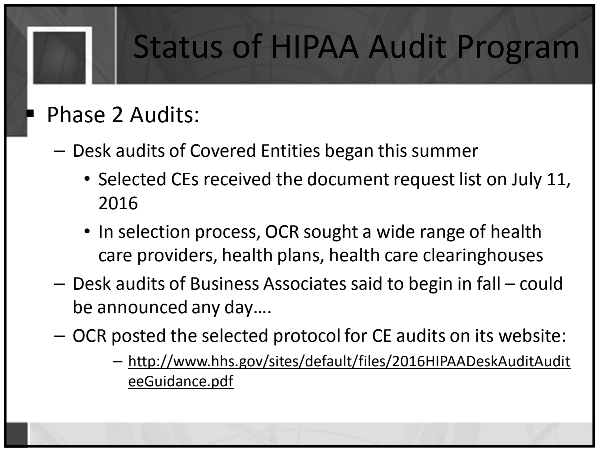
Breaches Involving Hacking Incidents

- ***Anthem***
  - Almost 80 million individuals affected
  - Cyber-attackers accessed social security numbers, medical ID numbers, names, addresses and birth dates
- ***Premera Blue Cross***
  - 11 million individuals affected
  - Discovered in January 2015 that hackers had been accessing PHI since May 2014
- ***Community Health Systems***
  - Estimated 4.5 million individuals affected
  - Hacker in China bypassed CHS' security measures and accessed patient names, addresses, birthdates, telephone numbers and social security numbers



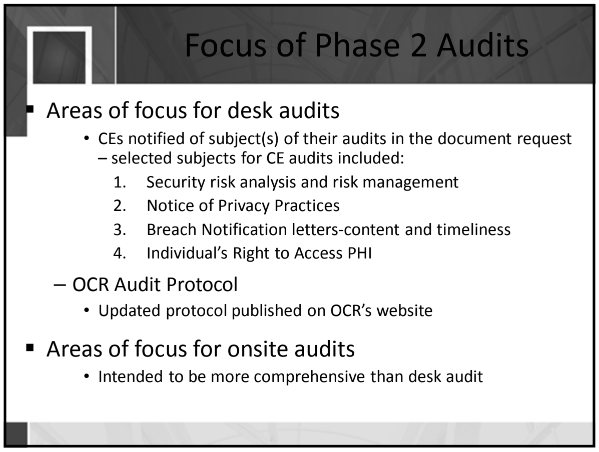
OCR HIPAA Audit Structure

- Scope of Auditees
  - Covered Entities and Business Associates
- Type of Audit
  - "Desk" audits first
    - Conducted via document requests
  - Onsite audits to follow



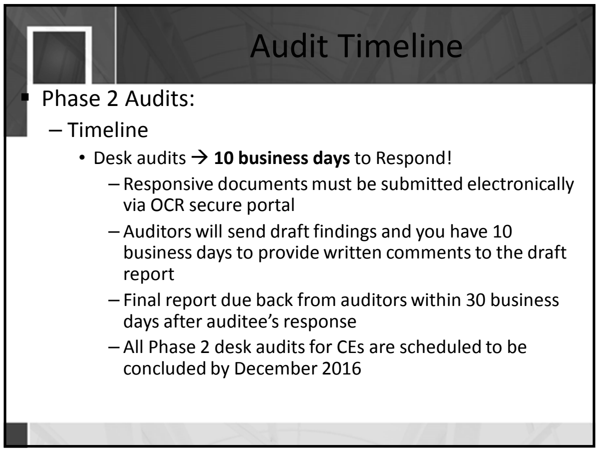
Status of HIPAA Audit Program

- Phase 2 Audits:
  - – Desk audits of Covered Entities began this summer
    - Selected CEs received the document request list on July 11, 2016
    - In selection process, OCR sought a wide range of health care providers, health plans, health care clearinghouses
  - – Desk audits of Business Associates said to begin in fall – could be announced any day….
  - – OCR posted the selected protocol for CE audits on its website:
    - – http://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf



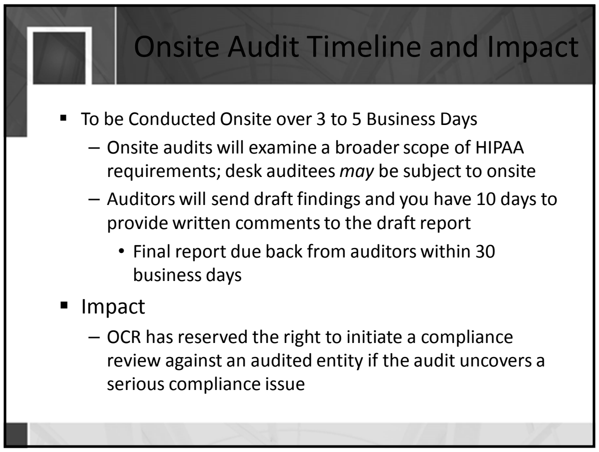
Focus of Phase 2 Audits

- Areas of focus for desk audits
  - CEs notified of subject(s) of their audits in the document request – selected subjects for CE audits included:
    1. Security risk analysis and risk management
    2. Notice of Privacy Practices
    3. Breach Notification letters-content and timeliness
    4. Individual's Right to Access PHI
  - – OCR Audit Protocol
    - Updated protocol published on OCR's website
- Areas of focus for onsite audits
  - Intended to be more comprehensive than desk audit



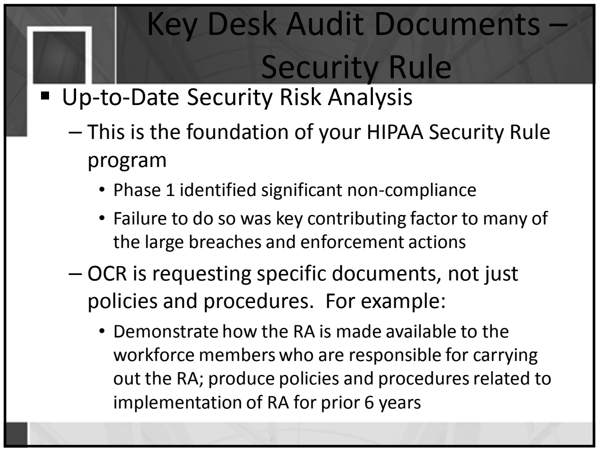
Audit Timeline

- Phase 2 Audits:
  - – Timeline
    - Desk audits → **10 business days** to Respond!
      - – Responsive documents must be submitted electronically via OCR secure portal
      - – Auditors will send draft findings and you have 10 business days to provide written comments to the draft report
      - – Final report due back from auditors within 30 business days after auditee's response
      - – All Phase 2 desk audits for CEs are scheduled to be concluded by December 2016



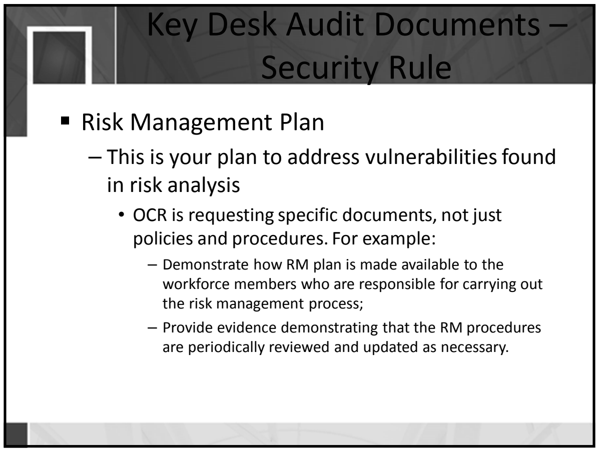
Onsite Audit Timeline and Impact

- To be Conducted Onsite over 3 to 5 Business Days
  - Onsite audits will examine a broader scope of HIPAA requirements; desk auditees *may* be subject to onsite
  - Auditors will send draft findings and you have 10 days to provide written comments to the draft report
    - Final report due back from auditors within 30 business days
- Impact
  - OCR has reserved the right to initiate a compliance review against an audited entity if the audit uncovers a serious compliance issue



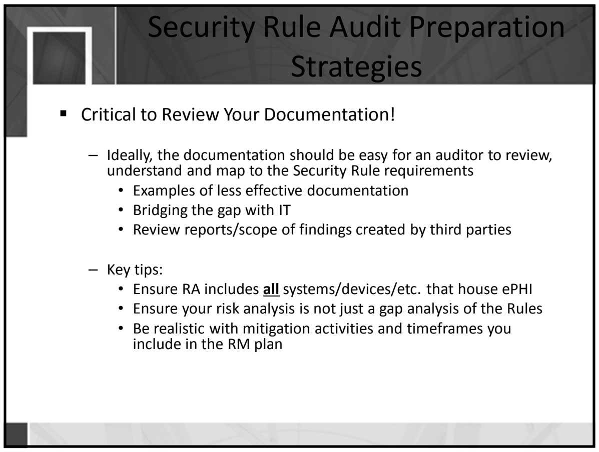
Key Desk Audit Documents – Security Rule

- Up-to-Date Security Risk Analysis
  - This is the foundation of your HIPAA Security Rule program
    - Phase 1 identified significant non-compliance
    - Failure to do so was key contributing factor to many of the large breaches and enforcement actions
  - OCR is requesting specific documents, not just policies and procedures. For example:
    - Demonstrate how the RA is made available to the workforce members who are responsible for carrying out the RA; produce policies and procedures related to implementation of RA for prior 6 years



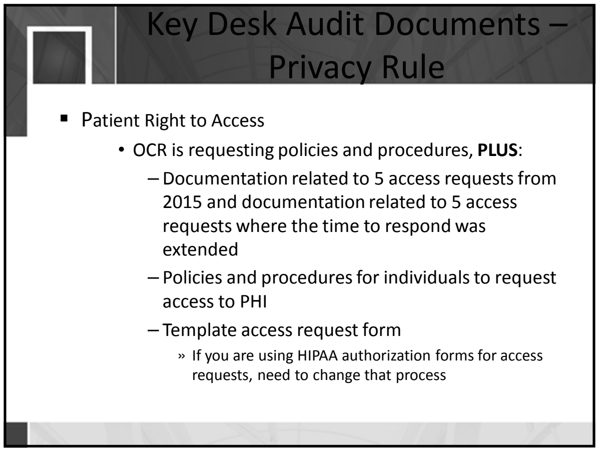
Key Desk Audit Documents – Security Rule

- Risk Management Plan
  - This is your plan to address vulnerabilities found in risk analysis
    - OCR is requesting specific documents, not just policies and procedures. For example:
      - Demonstrate how RM plan is made available to the workforce members who are responsible for carrying out the risk management process;
      - Provide evidence demonstrating that the RM procedures are periodically reviewed and updated as necessary.



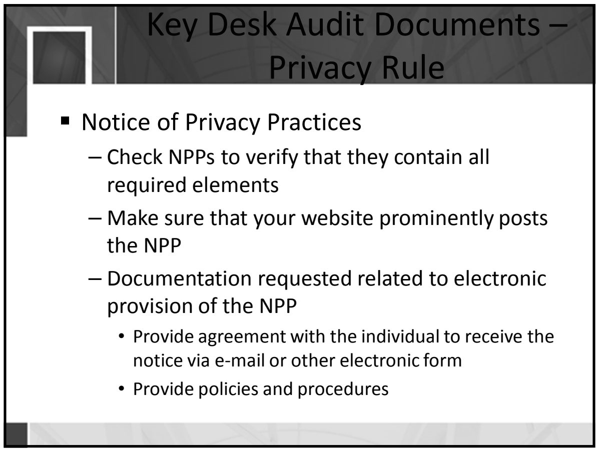
Security Rule Audit Preparation Strategies

- Critical to Review Your Documentation!
  - Ideally, the documentation should be easy for an auditor to review, understand and map to the Security Rule requirements
    - Examples of less effective documentation
    - Bridging the gap with IT
    - Review reports/scope of findings created by third parties
  - Key tips:
    - Ensure RA includes **all** systems/devices/etc. that house ePHI
    - Ensure your risk analysis is not just a gap analysis of the Rules
    - Be realistic with mitigation activities and timeframes you include in the RM plan



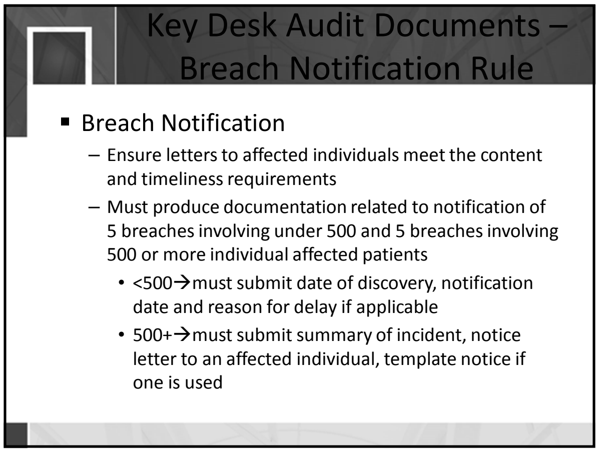
Key Desk Audit Documents – Privacy Rule

- Patient Right to Access
  - OCR is requesting policies and procedures, **PLUS**:
    - Documentation related to 5 access requests from 2015 and documentation related to 5 access requests where the time to respond was extended
    - Policies and procedures for individuals to request access to PHI
    - Template access request form
      - » If you are using HIPAA authorization forms for access requests, need to change that process



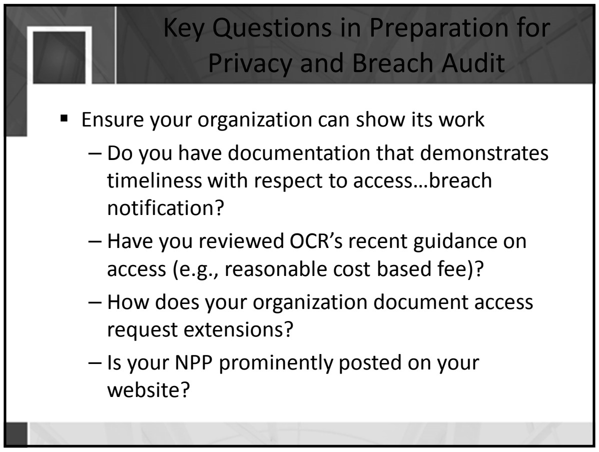
Key Desk Audit Documents – Privacy Rule

- Notice of Privacy Practices
  - Check NPPs to verify that they contain all required elements
  - Make sure that your website prominently posts the NPP
  - Documentation requested related to electronic provision of the NPP
    - Provide agreement with the individual to receive the notice via e-mail or other electronic form
    - Provide policies and procedures



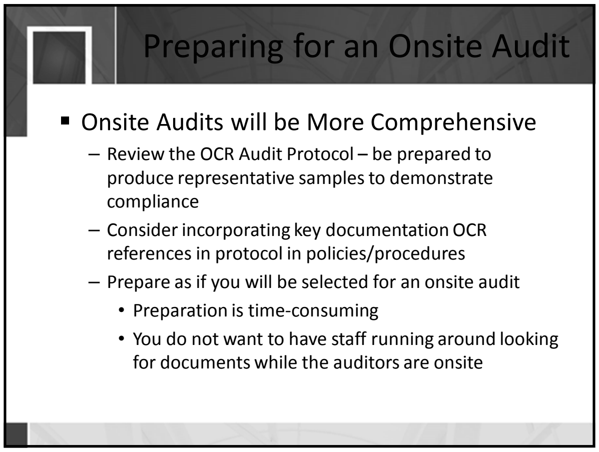
Key Desk Audit Documents – Breach Notification Rule

- Breach Notification
  - Ensure letters to affected individuals meet the content and timeliness requirements
  - Must produce documentation related to notification of 5 breaches involving under 500 and 5 breaches involving 500 or more individual affected patients
    - <500→must submit date of discovery, notification date and reason for delay if applicable
    - 500+→must submit summary of incident, notice letter to an affected individual, template notice if one is used



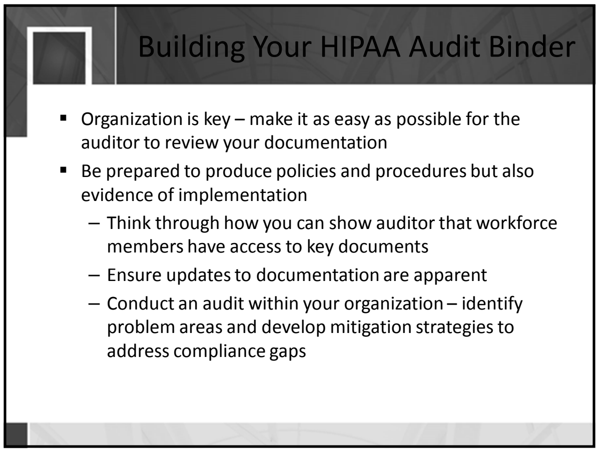
Key Questions in Preparation for Privacy and Breach Audit

- Ensure your organization can show its work
  - Do you have documentation that demonstrates timeliness with respect to access…breach notification?
  - Have you reviewed OCR's recent guidance on access (e.g., reasonable cost based fee)?
  - How does your organization document access request extensions?
  - Is your NPP prominently posted on your website?



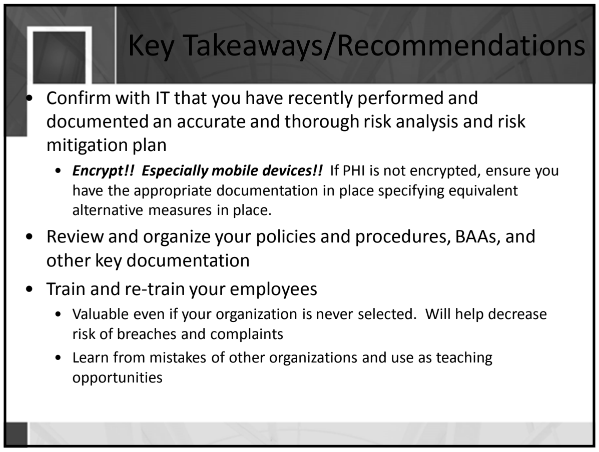
Preparing for an Onsite Audit

- Onsite Audits will be More Comprehensive
  - Review the OCR Audit Protocol – be prepared to produce representative samples to demonstrate compliance
  - Consider incorporating key documentation OCR references in protocol in policies/procedures
  - Prepare as if you will be selected for an onsite audit
    - Preparation is time-consuming
    - You do not want to have staff running around looking for documents while the auditors are onsite



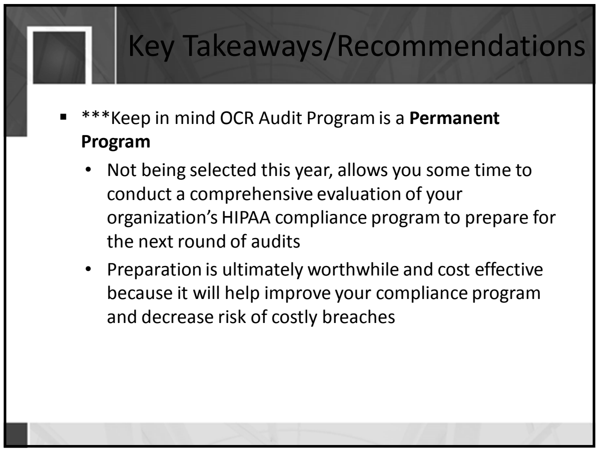
Building Your HIPAA Audit Binder

- Organization is key – make it as easy as possible for the auditor to review your documentation
- Be prepared to produce policies and procedures but also evidence of implementation
  - Think through how you can show auditor that workforce members have access to key documents
  - Ensure updates to documentation are apparent
  - Conduct an audit within your organization – identify problem areas and develop mitigation strategies to address compliance gaps



Key Takeaways/Recommendations

- Confirm with IT that you have recently performed and documented an accurate and thorough risk analysis and risk mitigation plan
  - ***Encrypt!! Especially mobile devices!!*** If PHI is not encrypted, ensure you have the appropriate documentation in place specifying equivalent alternative measures in place.
- Review and organize your policies and procedures, BAAs, and other key documentation
- Train and re-train your employees
  - Valuable even if your organization is never selected. Will help decrease risk of breaches and complaints
  - Learn from mistakes of other organizations and use as teaching opportunities



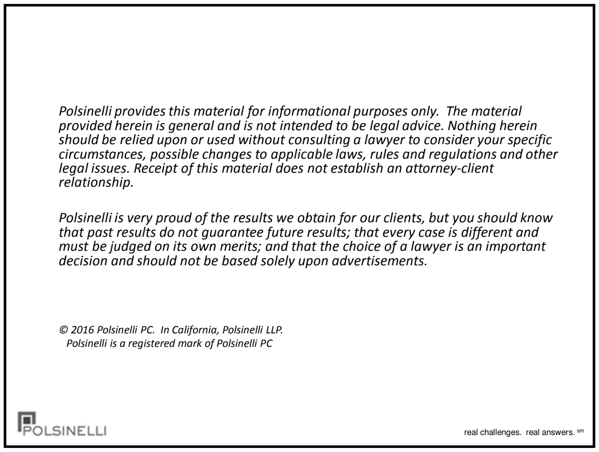
Key Takeaways/Recommendations

- ***Keep in mind OCR Audit Program is a **Permanent Program**
  - Not being selected this year, allows you some time to conduct a comprehensive evaluation of your organization's HIPAA compliance program to prepare for the next round of audits
  - Preparation is ultimately worthwhile and cost effective because it will help improve your compliance program and decrease risk of costly breaches

Questions?

- Feel free to contact us for more information:
  - Lisa Acevedo lacevedo@polsinelli.com
  - Katie Kenney: kdkenney@polsinelli.com

Exposed record
Data breach
Protection
DATA
law
anonymous
Metadata
digital
classification
PRIVACY
Patient privacy
Privacy
Regulations
Risk
Sensitive information
Authentication
compliance



Polsinelli provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

POLSINELLI

real challenges. real answers. sm