OCR's Phase 2 Audit Program:
Preparing your Organization

Jonathan R. Friesen, JD
Kaiser Foundation Health Plan of Colorado
Privacy and Security Officer

Audit Scope

- The Known Universe: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
  - OCR will review the policies and procedures adopted and employed by covered entities and business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules.
- Desk audit scope is limited to a total of 7 controls drawn from the Security Rule, the Privacy Rule, and the Breach Notification Rule
- Entities will either be audited on SR controls or PR & BNR compliance
- Onsite audits will begin in early 2017
  - A desk audit entity may be subject to an onsite audit

Audit Scope - Continued

- Phase 2 Audits will include both covered entities and business associates
- Comprised of 200-250 audits in total
  - Over 200 desk audits
  - Smaller number of comprehensive on-site audits
- OCR identified pools of CEs that represent a wide range of health care providers, health plans, health care clearinghouses, to better assess HIPAA compliance across the industry
  - Sampling criteria included size, affiliations, location, public or private
- Under OCR's separate, broad authority to open compliance reviews, OCR could decide to open a separate compliance review in a circumstance where significant threats to the privacy and security of PHI are revealed through the audit

Areas of Focus and Risk

- Privacy
  - Focused on Access, Notice of Privacy Practices, Electronic Notice
  - Challenging Areas: Deceased Individuals, Personal Representatives, Confidential Communications
- Security:
  - Focused on Security Management Processes – Risk Analysis and Risk Management
  - Challenging Areas: Clinical Technology, Vendor Assessments, Enterprise Risk Analysis
- Breach Notification:
  - Focused on Timeliness and Content of Notifications
  - Challenging Areas: Incident Risk Assessments (When is PHI compromised?), Policies and Procedures

Preparing Your Organization

- An OCR audit is different from a traditional OCR investigation or compliance review
- Practice Makes Perfect
  - Don't get stuck responding without practicing first!
    - 10 Business Days to Respond – You only get one shot – no opportunity to amend or add
    - Policy Collection and Organization Takes Time
      - Evidence of Policies and Procedures takes even longer
      - CEs must extract the relevant language from larger compendiums of policies and procedures if needed
    - Make it easy for the investigator/auditor through document organization
    - Touch base with all areas of the business that will be responsible for responding to particular sections
    - Gather and Conduct Interviews of Key Stakeholders
    - Use Internal and/or External Auditors to Assess Readiness
  - For large organizations, coordination and communication is key – particularly between IT/Security and Privacy

Working Through Pain Points

- Relationships and Responsiveness
  - Internal relationships and communication ensures you get what you need, when you need it
  - In a larger organization, early escalation of issues can help
- How Do We Prepare for Follow-Up?
  - Don't be afraid of the difficult questions, but try to anticipate them and ensure the stakeholders are prepared to provide a response
  - Transparency and trust are important – You have the opportunity to tell your company's story

Questions?