Preparing for HIPAA and Meaningful Use Compliance Audits

Presented by:
David Holtzman
VP of Compliance, CynergisTek
Today’s Presenter

• Vice President of Compliance Services, CynergisTek, Inc.
• Subject matter expert in health information privacy policy and compliance issues involving the HIPAA Privacy, Security and Breach Notification Rules
• Over 12 years of experience in developing, implementing and evaluating health information privacy and security compliance programs
• Former senior advisor for health information technology and the HIPAA Security Rule, Office for Civil Rights

David Holtzman
CynergisTek, Inc.
Agenda

- What to Expect in OCR Audit Program
- CMS Meaningful Use Audits
- OIG Meaningful Use Audits
- HIPAA Security Risk Analysis
- Tools and Resources
- Questions
OCR HIPAA Audit Program
OCR HIPAA Audit Program

• Permanent audit program slated to begin in 2015
• Pre-audit survey to pre-screen 1200 entities
• ~200 Covered Entities to be selected for desk audits
• Equal number or less BAs selected for desk audits
• Greater number of on-site audits, but no specific number given yet.
• Implementing technology to facilitate data collection phases of audit process
• Carried out by HHS personnel with contractor support
The Audit Steps

- Pre-Audit Survey
- Notification and data request to selected entities
- Desk review and draft findings to entity
- Entity provides management review
- Final Report
Desk Audit Expectations

• Data request will specify content and other electronic document submission requirements

• Only documentation submitted on time is reviewed

• All documentation must be current as of the date of the request

• Auditors will not be able to contact the entity for clarifications or ask for additional information
  – Critical that documentation accurately reflects the program

• Submission of extraneous information increases difficulty for auditor in finding/assessing required items

• Failure to submit responses leads to compliance review
Scope of OCR Desk Audits

2015 Desk Audits of Covered Entities
- Security—Risk Analysis and risk management
- Breach—Content and timeliness of breach notifications
- Privacy—Notice of Privacy Practices and Access

2015 Desk Audits of Business Associates
- Security—Risk Analysis and risk management
- Breach—Breach reporting to covered entities

2015-16 On-site Comprehensive Audits
- Covered entities
- Business associates
Scope of OCR Onsite Audits

Security
- Device and media controls
- Transmission security
- Encryption of data at rest
- Facility access controls

Privacy
- Administrative and physical safeguards
- Workforce training to HIPAA policies & procedures

Other Areas
- High risk areas identified through:
  - 2015 audits
  - Breach reports submitted to OCR
  - Consumer complaints
Meaningful Use Attestation Audits
Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs

- Program established by American Recovery and Reinvestment Act of 2009
- Provides incentive payments to certain eligible professionals (EPs), eligible hospitals (EHs), and critical access hospitals
- *Adopt, implement, upgrade or demonstrate meaningful use* of certified EHR technology

Payments began in 2011 and continue through 2016 (Medicare) or 2021 (Medicaid)

- Over **$28 Billion** paid out since 2011
CMS MU Audits

• Any provider attesting to receive EHR incentive payments for either the Medicare or Medicaid program may be subject to audits.

• Medicaid audits are performed by each state.

• Medicare audits performed by Figliozzi & Company.
MU Audit Process

• Audit Approach
  _ Appropriate Letter and Documentation Request is sent to individual who attested for the organization (letter is specific to whether it is an Eligible Provider or Eligible Hospital engagement).
  _ Client has 10 business days to provide the documentation requested electronically.
  _ Auditor reviews documentation and determines if additional information is needed. (This is the primary review step).
  _ Additional request will be provided via email as necessary.
  _ If documentation is deemed insufficient to support attestation or other data anomalies exist then, an on-site visit/exam is scheduled.
• The source documentation utilized during the attestation process
• Copy of the certification from ONC-CHPL for the EHR application (http://oncchpl.force.com/ehrcert)
• Documentation to support the methodology chosen for achieving measures (i.e. observation services or all emergency department visits)
• The numerators and denominators for each measures
MU Desk Audit Documentation (cont’d)

• The time period the reports cover
• Risk analysis and remediation plans for deficiencies
• Summary level reports for measures
• Screenshots or other evidence to support and measures that require a “YES” answer
• Evidence to support that source information was generated for that eligible professional or eligible hospital
MU Onsite Audit Scope

• Detailed reviews of any of the measures via:
  – Walk-throughs of structured data and functionality in EHRs
  – Walk-throughs of test patients and scenarios
  – Review of medical records and patient records; Detailed data to support summary reports
  – Census reports
  – Billing information
  – Validation of settings or additional detailed information to support reporting as deemed necessary
    • Security screen settings
    • Screen shots of test exchanges of clinical information
    • Audit logs (date for when a feature was enabled, etc.)
• A determination by CMS that a provider or hospital has
  — been denied an EHR incentive payment
  — have been determined to be ineligible for the program
  — received an audit decision believed to be in error, you can appeal the decision.

• A provision of ACA provides that there is no right of due process for review of CMS determinations
ACA Ups Ante on Exposure

• Affordable Care Act of 2010 (ACA):
  – If a person has “received an overpayment,” the person shall “report and return the overpayment to the Secretary, the State, an intermediary, a carrier, or a contractor as appropriate and provide notice of the reason for the overpayment
  – Overpayments must be reported and returned within 60 days after the date on which the overpayment was identified
  – Any overpayment retained by a person after the deadline for reporting and returning the overpayment is an “obligation” under the False Claims Act
Post Payment Audits of EPs

• 4601 Completed Audits

• 24% Failed to Meet MU Standards
  – 99% of the failure did not meet MU objectives and measures
  – Average proposed returned incentive amount $16,863 per provider

(CMS Data as of September 15, 2014)
Pre-Payment Audits of EPs

• 3820 Completed Audits
• 21.5% Failed Pre-payment Audit
  – 7% of failures because did not use CEHRT
  – 93% of failures did not meet MU objectives and measures

(CMS Data as of September 15, 2014)
Post-Payment Audits of EHs

- 613 Completed Post-Payment Audits
- 4.7% Failed Post-Payment Audits
  - Average proposed returned incentive payment $1.13 million per hospital
  - $33 million total proposed EH returned incentive payments

(CMS Data as of September 15, 2014)
OIG Meaningful Use Audits
OIG Focus on Meaningful Use

- OIG FY 2015 Workplan
  - Security of certified electronic health record technology
  - Perform audits of various covered entities receiving EHR incentive payments from CMS and their business associates, such as EHR cloud service providers, to determine whether they adequately protect electronic health information created or maintained by certified EHR technology
  - Engagements in each OIG region through the Office of Audit Services
Case Study in OIG Audit Process

- **Document Preparation**
  - 18 areas in which documentation requested prior to onsite engagement
  - Covers prior year attestation period and more recent information

- **Audit Team Onsite Visit – 2 weeks**
  - Exit interview with preliminary Notification of Findings
  - Opportunity for Remediation that can be reflected in final report
  - Interviews with staff involved in IT Security

- **Draft report (about 3 months after onsite visit)**

- **Covered entity comment/response to findings**

- **Final report is shared with CMS and OCR**

- **Rollup report summarizing all provider audits is posted to OIG Website**
OIG Audit Process

• Areas of Focus
  – Organizational Risk Analysis
  – Access Controls
  – Audit of alerts and logs from EHR
  – Patch Management
  – Encryption Security
  – System Scans
OIG System Scanning Tools

• OIG employs an appliance to perform database scanning for security safeguards
  – App Detective is optimized to scan
    • Oracle
    • Sybase
    • SQL Server
    • DB2
    • Not effective on Cache
  – Reading for critical patches & updates
  – Effective access controls
Enforcement Outlook

• Takeaways from recent HCCA Regional Conference in Dallas:
  
  — OIG DC HQ Assoc. Counsel said OIGs approach to audit attestations has moved to a tool for incentive funds recovery
  
  — Asst. US Atty from Dallas said its office is working with the OIG to investigate/prosecute Medicare fraud for knowing/false MU attestations
HIPAA Security Risk Analysis
HIPAA Security Risk Assessment

- Required element for Security Rule and Meaningful Use
- An assessment of threats and vulnerabilities to information systems that handle e-PHI.
- This provides the starting point for determining what is ‘appropriate’ and ‘reasonable’.
- Organizations determine their own technology and administrative choices to mitigate their risks.
- The risk analysis process should be ongoing and repeated as needed when the organization experiences changes in technology or operating environment.
Performing a Risk Analysis

Gather Information
- Prepare inventory lists of information assets—data, hardware, and software.
- Determine potential threats to information assets.
- Identify organizational and information system vulnerabilities.
- Document existing security controls and processes.
- Develop plans for targeted security controls.

Analyze Information
- Evaluate and measure risks associated with information assets.
- Rank information assets based on asset criticality and business value.
- Develop and analyze multiple potential threat scenarios.

Develop Remedial Plans
- Prioritize potential threats based on importance and criticality.
- Develop remedial plans to combat potential threat scenarios.
- Repeat risk analysis to evaluate success of remediation and when there are changes in technology or operating environment.
Resources & Tools
• OCR HIPAA Privacy & Security
  – http://hhs.gov/ocr/privacy

• HIPAA Security Rule Risk Assessment
  – HHS Risk Assessment Tool for Small Providers
    • http://www.healthit.gov/providers-professionals/security-risk-assessment
  – NIST HIPAA Security Risk Assessment Tool
    • http://www.scap.nist.gov/HIPAA

• ONC-Certified Electronic Health Technology Product List
  – http://oncchpl.force.com/ehrcert
Questions?

David Holtzman
david.holtzman@cynergistek.com
512.405.8550 x7020