United States Department of
Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

Preparing for the Anticipated OCR Privacy and Security Audits

4th National HIPAA West Summit
October 4-6, 2010

Adam Greene, JD, MPH
Senior Health IT and Privacy Specialist

Agenda

- Current enforcement procedures
- Status of audit program
- Challenges for HIPAA audits

Enforcement & Compliance

- Complaints
- Compliance reviews
- Breach reports
- Audits

Complaints

- OCR currently investigates all timely complaints that allege Privacy or Security Rule violations
  - Complaints must be filed within 180 days
  - Administratively resolved when untimely, no jurisdiction, or no violation alleged
- Complaints are investigated by regional office based on location of covered entity
  - Exception based on regional caseload

Compliance Reviews

- Initiated by OCR, often in response to media reports
- Subsequent complaints may be added to compliance review
- Generally focused on specific issue

Breach Reports

- All large breaches (500 or more) are verified and investigated
- Regions have discretion on small breaches
- Summary of results posted on website

Investigation

- Steps include:
  - Notification of covered entity
  - Data request(s) and interviews
  - Corrective action where indications of non-compliance
- Generally focused on complaint allegation, media report, or cause of breach

Audits

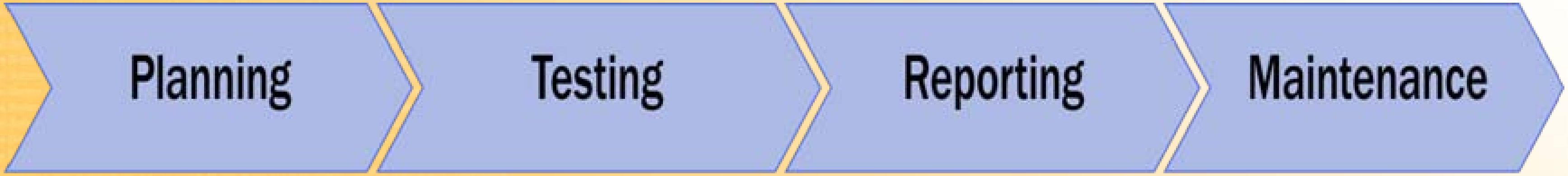
HITECH Act § 13411

The Secretary shall provide for periodic audits to ensure that covered entities and business associates … comply with [the HITECH Act, Privacy, and Security Rules].

OCR HIPAA Audit Contract

- **Purpose:** To evaluate and compare compliance audit program configurations and recommend to OCR several feasible and effective program structure alternatives to implement HITECH § 13411
- **Timeline:**
  - Nov, 2009 – Request for proposal
  - Mar. 2010 - Contract awarded to Booz Allen Hamilton
  - March – Aug. 2010 – BAH research period
  - Aug. 2010 - BAH issues final report to OCR

Audit Program Elements


Planning Testing Reporting Maintenance

• Select Audited Entities • Create Documentation and Analysis Tools • Identify and Train Staff • Establish Level of Effort • Conduct Pre-Audit Planning	• Perform Tests and Evaluate Results • Draft Communications	• Communicate Results of Audit • Report Findings • Permit Dispute of Findings	• Request Corrective Action • Transition from Audit to Enforcement • Conduct Appeals • Encourage Compliance of other Audited Entities

Planning Questions

- Defining universe of covered entities and business associates
  - No central list exists
- Choosing option(s) for selecting audited entities
  - Random selection
  - Statistical representativeness
  - Based on complaints
  - Consideration of geographical data
  - Corrective action plans

Planning Questions

- Determining scope of audits
- Creating audit documentation tools
  - Standardized vs. customized for each covered entity or business associate
- Identifying and training staff
  - Government staff vs. contractors
- Determining frequency of audits
- Allocating resources
  - Number of auditors per audit
  - Duration of site visits

Testing Questions

- Determining amount of advanced notice
- Determining amount of documentation needed
- Organizing documentation (e.g., crosswalks)
- Determining whom to interview

Reporting Questions

- Preparing comprehensive final report
- Preparing recommendations
- Providing a means to dispute findings
- Determining whether to publicly release report
  - Transparency vs. exposure of vulnerabilities

Maintenance Questions

- Ensuring that corrective action is taken
- Determining whether enforcement is appropriate

Want more information?

The OCR website:
http://www.hhs.gov/ocr/privacy/

My contact:
adam.greene@hhs.gov