KPMG

cutting through complexity

2012 HIPAA Privacy and Security OCR Audits

Mark M. Johnson

National HIPAA Security Director

Overview of HIPAA Compliance High Interest Areas

Administrative Requirements

Uses and Disclosures (U&D)

Notice of Privacy Practices (NPP)

Rights to Request Privacy Protection

Access of Individuals to PHI

Breach Notification Requirements

Security

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Program Objectives

The objectives for the audit program are to improve covered entity compliance with the HIPAA privacy and security standards, through two approaches.

•OCR anticipates that widely publicizing both the audit program and the results of particular audits will spur covered entities and their business associates to assess and calibrate their privacy and security protections.

•In addition, OCR post on its web site and broadly share best practices gleaned through the audit process and guidance targeted to observed compliance challenges. Such technical assistance will assist those entities that are seeking information to frame their ongoing compliance efforts.

It is the intent of OCR to publish results that were obtained from these reviews as a broader guidance set to the industry (de-identified).

What is a Performance Audit?

- **An audit service conducted in accordance with Generally Accepted Government Auditing Standards, GAGAS (The Yellow Book)**
- **Provides findings, observations, or conclusions based on an evaluation of sufficient, appropriate evidence against established audit criteria**
- **Can include a limitless range of objectives driven by the needs of the program sponsor**
- **Can entail objective assessments of a variety of attributes:**
  - Program effectiveness, economy, and efficiency
  - Internal control
  - Compliance
  - Questions of interest to the program sponsor, but within the realm of the scope and industry requirements

Who Is Audited?

- **All covered entities are subject to be audited**
- **Covered entities range in size and complexity**
- **Covered Entities were identified in the following categories to allow for specific application of the rule:**
  - Provider
  - Health Plan
  - Group Health Plan (GHP)
  - Clearinghouse

Timeline for the Audit Program

The contract with KPMG to create audit protocols and field the pilot audits went into effect the end of June 2011, so we are now completing the program activities. The pilot audit, which consisted of a 115 audits was a three step process.

1. The first step entailed working with OCR to develop the audit protocols.

2. An initial round of audits were fielded to test the protocol. The results of the field testing were used to adjust the final protocol design.

3. The last step included rolling out the full range of audits and an evaluation process, as well as publishing the final audit protocol. All audits are field complete with final reporting being completed by December, 2012.

Audit Process

Performance Audit Objective

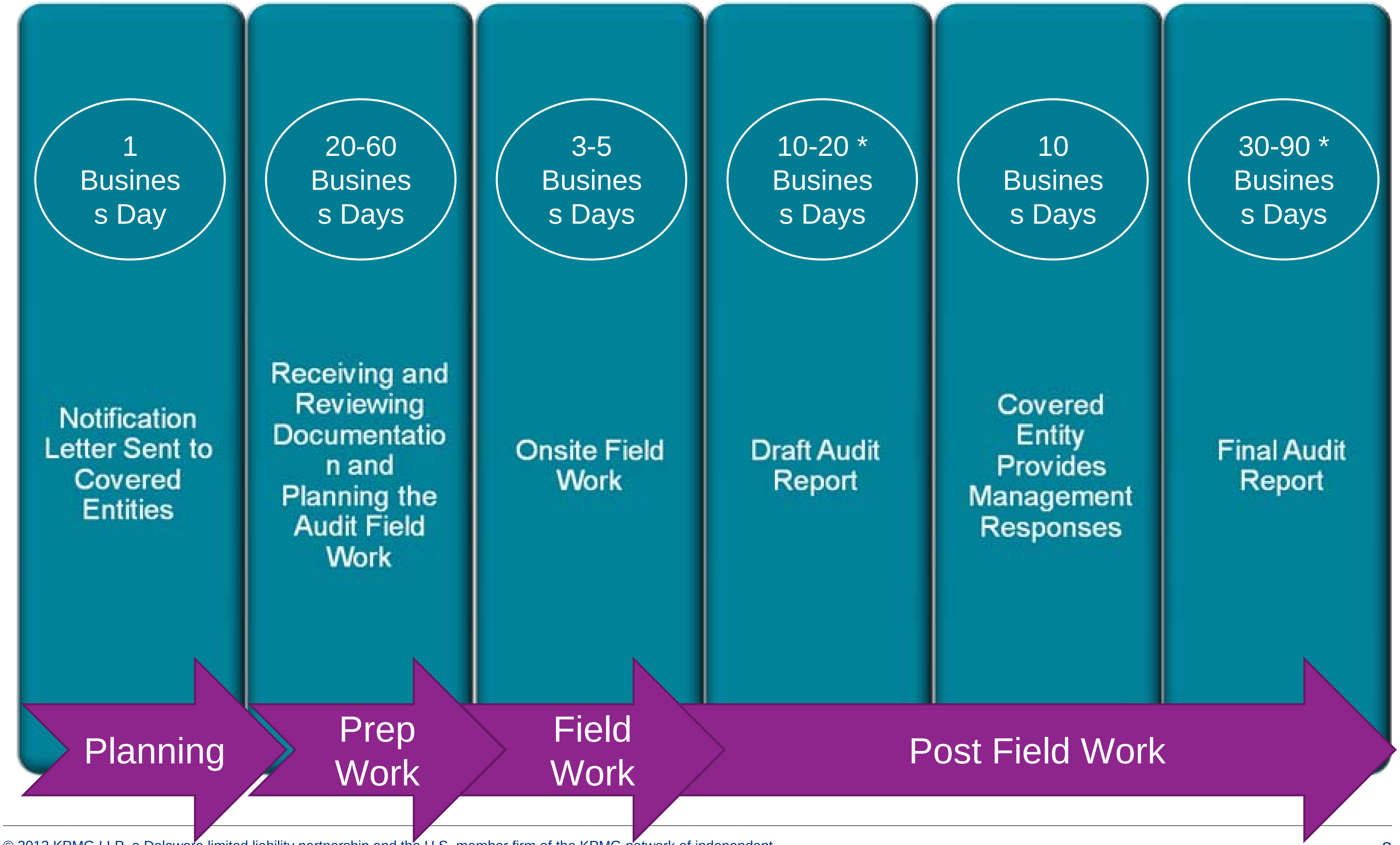
The objective of this performance audit was to 1) analyze the key processes, controls, and policies of the auditee relative to selected requirements of the Rules as specified in an audit protocol established by the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS), and 2) to provide our findings or observations. The audit objective did not include a determination of the effectiveness of implementation of the selected requirements in OCR's audit protocol.

Ensure the confidentiality, integrity, and availability of Electronic Protected Health Information (ePHI) that it creates, receives, maintains, or transmits;

Protect against any reasonably anticipated threats and hazards to the security or integrity of ePHI; and

Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

Audit Timeline



1 Business Day

Notification Letter Sent to Covered Entities

20-60 Business Days

Receiving and Reviewing Documentation and Planning the Audit Field Work

3-5 Business Days

Onsite Field Work

10-20 * Business Days

Draft Audit Report

10 Business Days

Covered Entity Provides Management Responses

30-90 * Business Days

Final Audit Report

Planning

Prep Work

Field Work

Post Field Work

Planning the Audit

1. **Complete Covered Entity selection process to:**

   Determine auditee universe;

   Determine independence from entity;

   Determine entity size and type; and

   Select the entity.

2. **Send notification letter to the selected Covered Entity including:**

   Information Request List; and

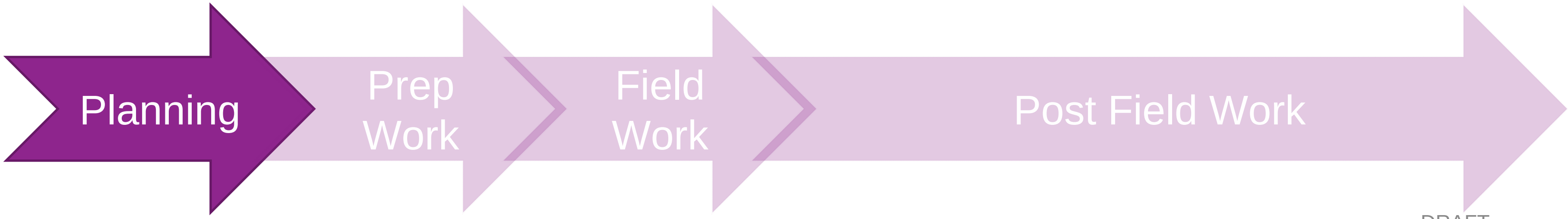
   HIPAA Privacy and Security Performance Audit Survey.

3. **Make Initial contact to:**

   Confirm Notification Letter receipt;

   Respond to any questions/concerns; and

   Confirm due date for documentation requests.



Preparation Work

1. **Conduct kick-off call to:**

    Confirm Covered Entity type (provider, clearinghouse, fully insured group health plan, etc.), applicable scope, and audit location(s); and

    Discuss on-site visit and logistics.

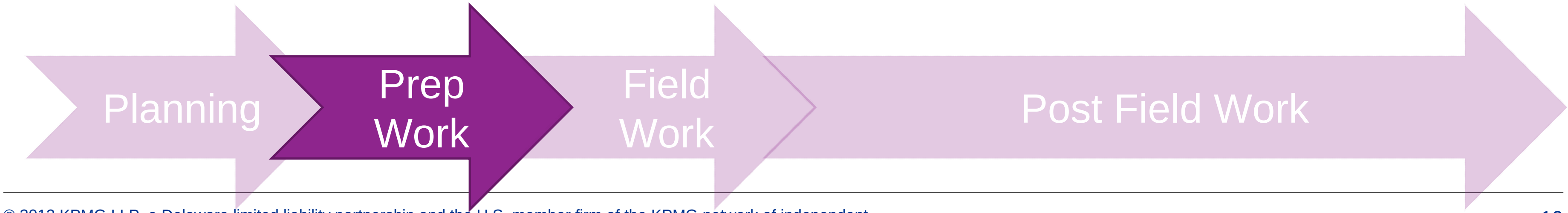
2. **Perform analysis of documentation provided by the Covered Entity to determine:**

    What documents have been received; and

    What documents are missing, if any.

3. **Begin audit testing procedures surrounding the review of documentation.**

4. **Send field work start date reminder email.**



Field Work

1. Conduct an entrance conference with the Covered Entity to discuss:

Performance audit concept, scope, objective, and approach; and

Set expectations with the auditee.

2. Execute and document all applicable audit procedures:

Complete onsite testing;

Conduct interviews;

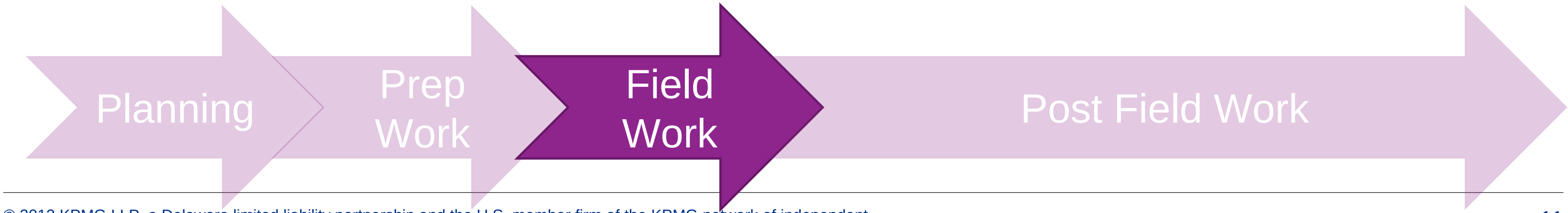
Review documentation; and

Observe appropriate facilities/workstations.

3. Conduct an exit conference with the Covered Entity to discuss:

Preliminary identified issues; and

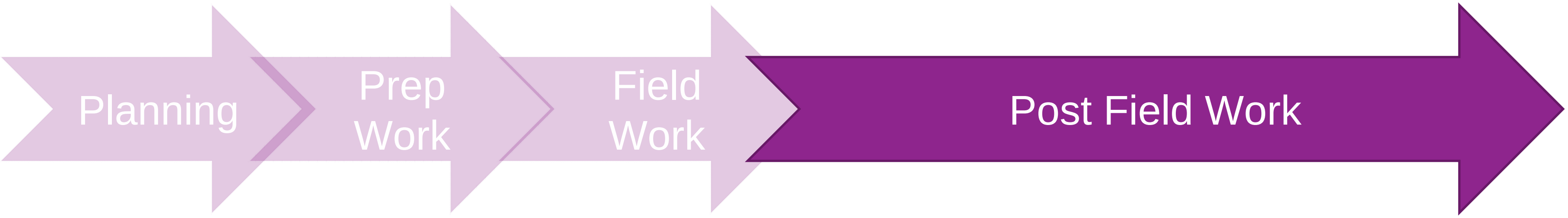
Discuss next steps for the audit process.



Post Field Work

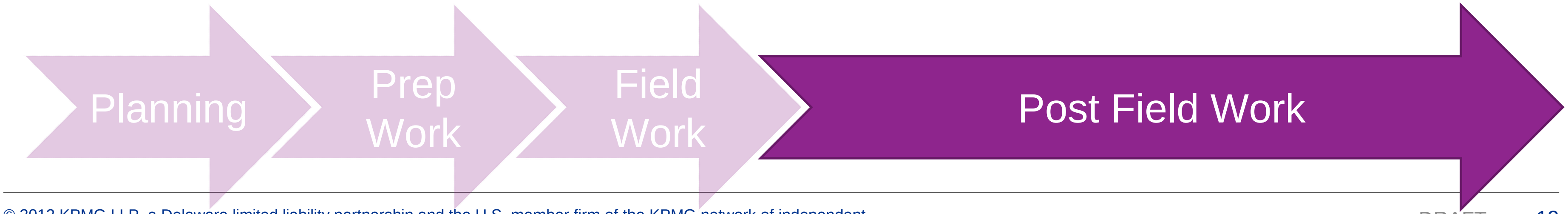
1. **Document results of the audit.**
2. **Finalize draft identified findings.**
3. **Draft performance audit report.**
4. **Submit documents for review:**

   Submit audit results and draft audit report for initial Quality Assurance (QA) Review



Post Field Work (cont'd)

6. Provide draft findings to Covered Entity for management response.
7. Incorporate findings with management responses into draft report and Clarify management responses with Covered Entity.
8. Submit draft audit report and results for secondary QA Review.
9. Provide OCR with draft audit report for comments.
10. Obtain signed Representation Letter from Covered Entity.
11. Issue the final audit report.



Planning

Prep Work

Field Work

Post Field Work

What will be the Outcome of an Audit?

Audits are a type of review that serves more as a compliance improvement tool then an investigation of a particular violation that may lead to sanctions and penalties. An audit may uncover vulnerabilities and weaknesses that can be appropriately addressed through corrective action on the part of the entity.

It is possible that an audit could indicate serious compliance issues that may trigger a separate enforcement investigation by OCR.

KPMG

cutting through complexity

Mark M. Johnson

mmjohnson@kpmg.com