U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2

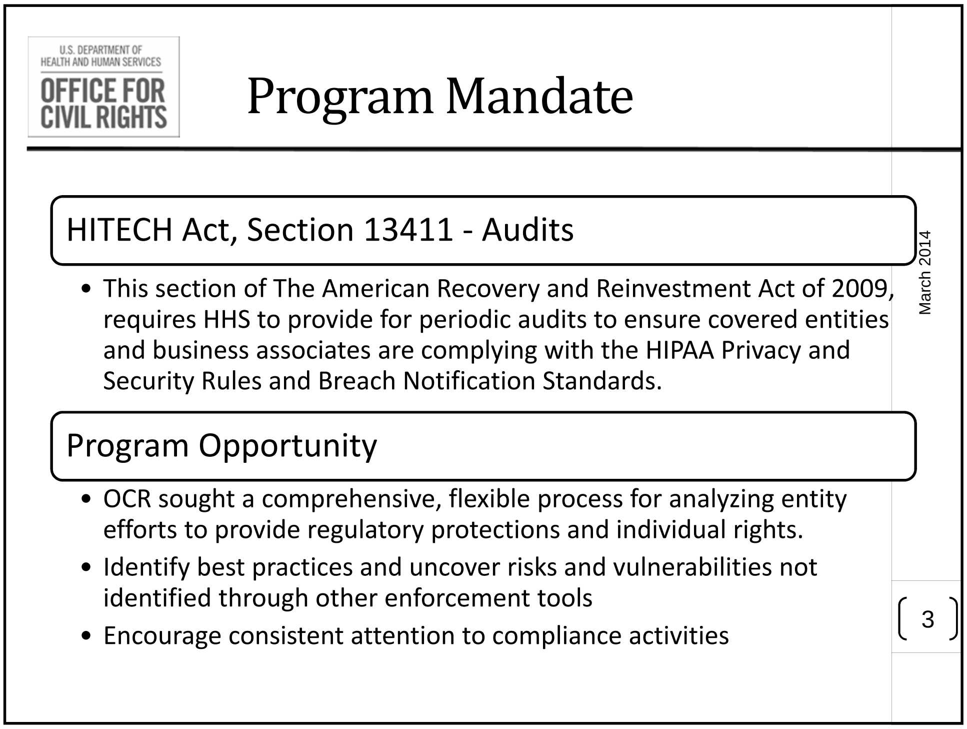
Linda Sanches, MPH
Senior Advisor, Health Information Privacy

HCCA Compliance Institute
March 31, 2014

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Agenda

- Background
- Audit Phase 1
  - Design
  - 2012 Findings
  - Evaluation—major recommendations
- Audit Phase 2
  - Approach
  - Size
  - Timing
  - Focus
  - Entity selection
- Guidance



Program Mandate

HITECH Act, Section 13411 - Audits

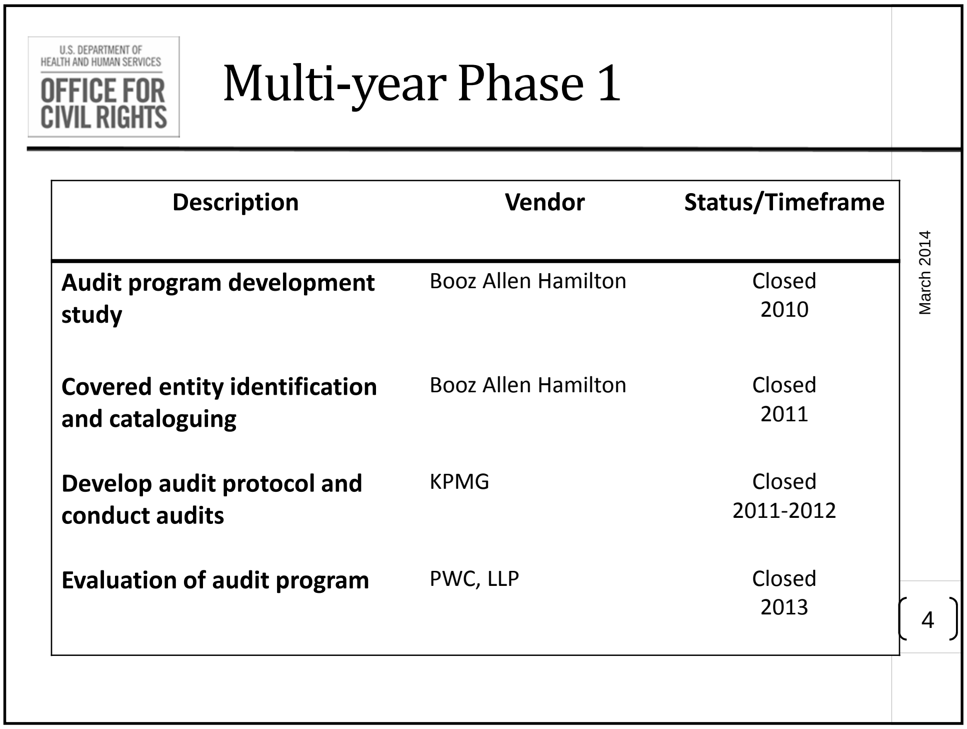
- This section of The American Recovery and Reinvestment Act of 2009, requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification Standards.

Program Opportunity

- OCR sought a comprehensive, flexible process for analyzing entity efforts to provide regulatory protections and individual rights.
- Identify best practices and uncover risks and vulnerabilities not identified through other enforcement tools
- Encourage consistent attention to compliance activities

March 2014

3

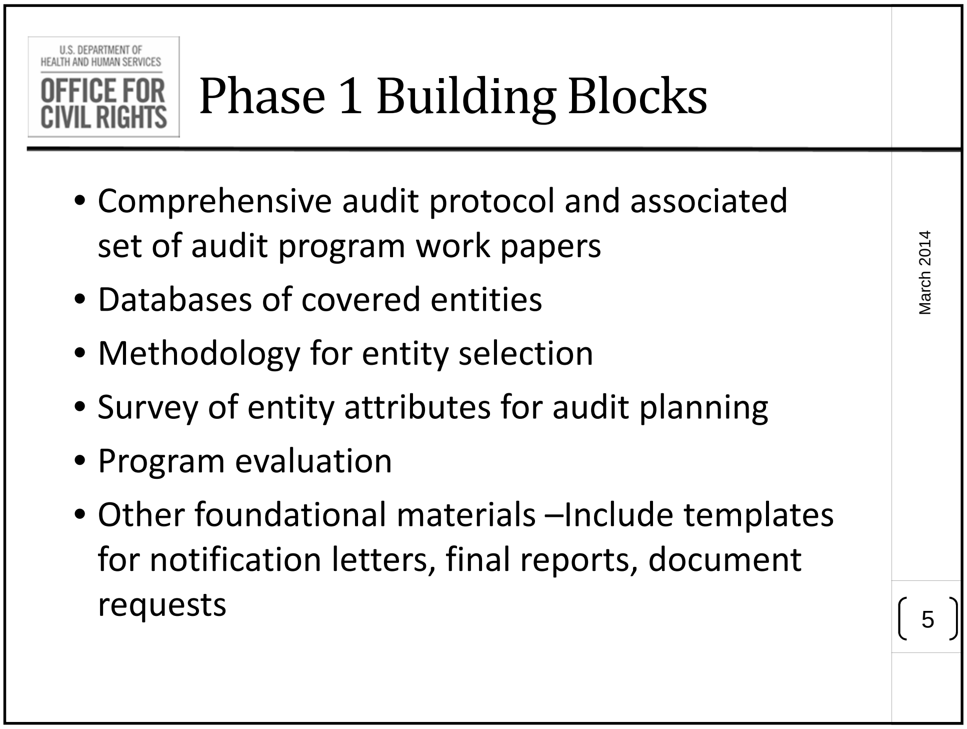


Multi-year Phase 1

Description	Vendor	Status/Timeframe
Audit program development study	Booz Allen Hamilton	Closed 2010
Covered entity identification and cataloguing	Booz Allen Hamilton	Closed 2011
Develop audit protocol and conduct audits	KPMG	Closed 2011-2012
Evaluation of audit program	PWC, LLP	Closed 2013

March 2014

4

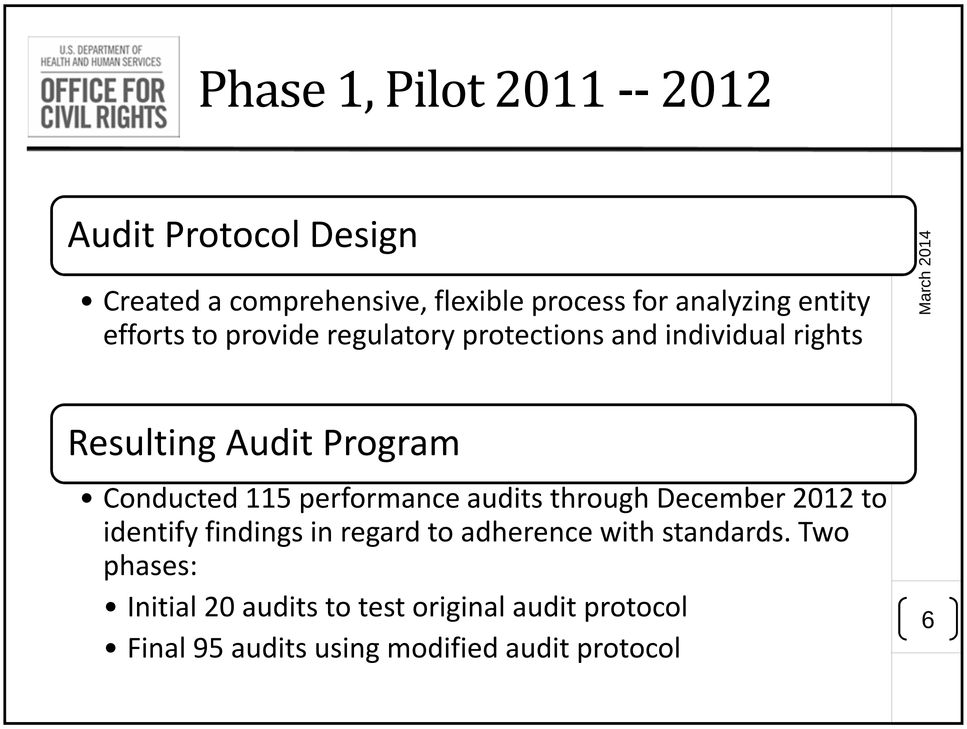


Phase 1 Building Blocks

- Comprehensive audit protocol and associated set of audit program work papers
- Databases of covered entities
- Methodology for entity selection
- Survey of entity attributes for audit planning
- Program evaluation
- Other foundational materials –Include templates for notification letters, final reports, document requests

March 2014

5



Phase 1, Pilot 2011 -- 2012

Audit Protocol Design

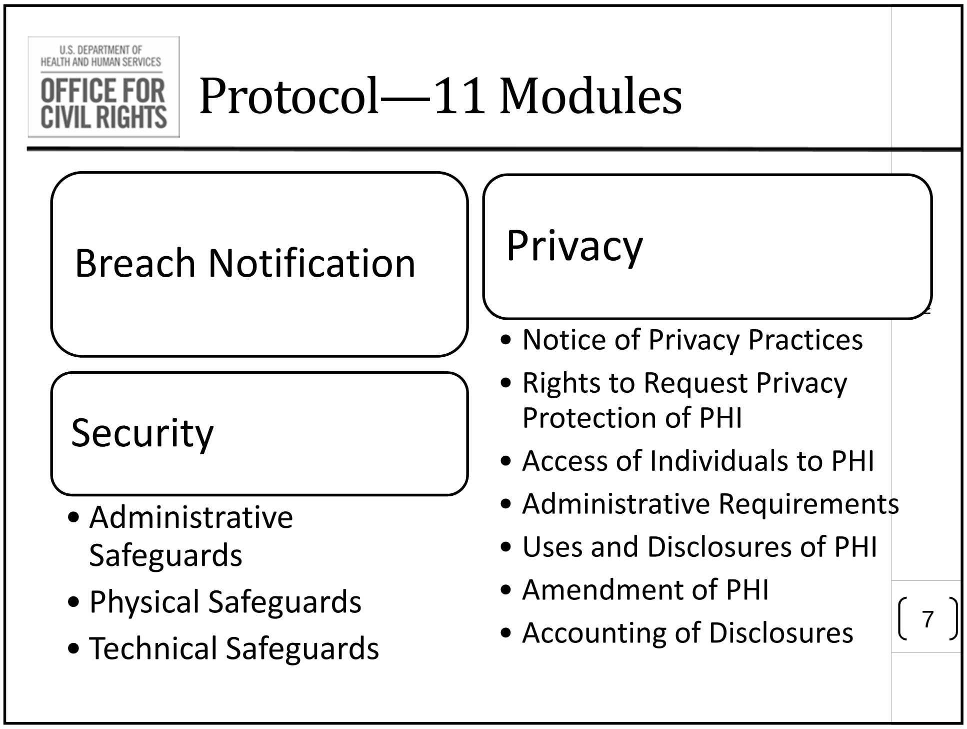
- Created a comprehensive, flexible process for analyzing entity efforts to provide regulatory protections and individual rights

Resulting Audit Program

- Conducted 115 performance audits through December 2012 to identify findings in regard to adherence with standards. Two phases:
  - Initial 20 audits to test original audit protocol
  - Final 95 audits using modified audit protocol

March 2014

6



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Protocol—11 Modules

Breach Notification

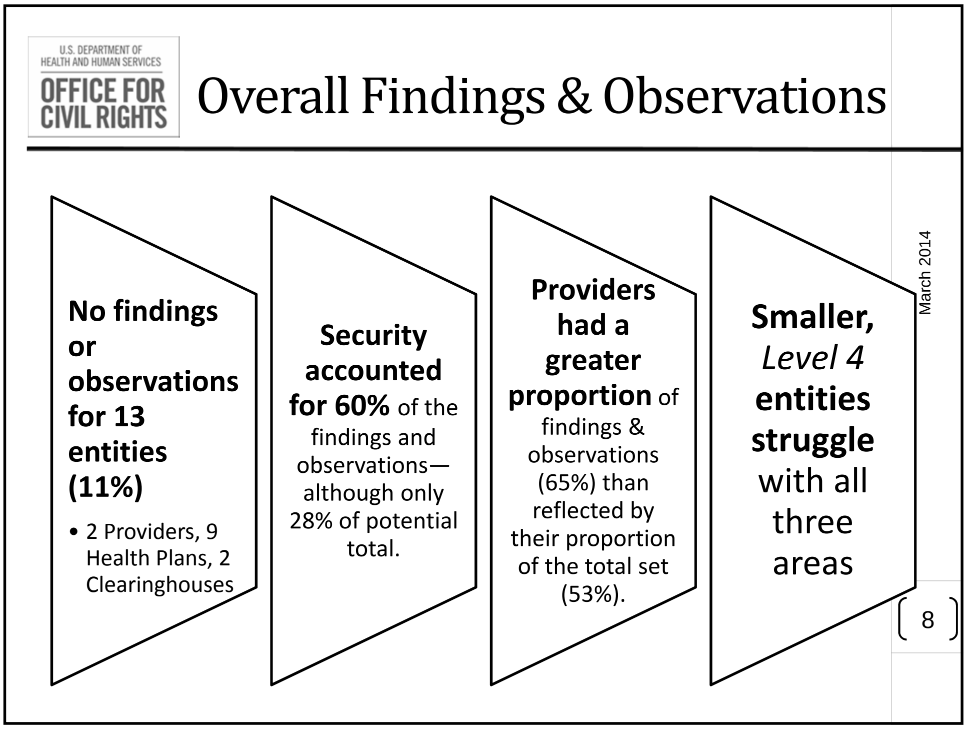
Security

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Privacy

- Notice of Privacy Practices
- Rights to Request Privacy Protection of PHI
- Access of Individuals to PHI
- Administrative Requirements
- Uses and Disclosures of PHI
- Amendment of PHI
- Accounting of Disclosures

7



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Overall Findings & Observations

No findings or observations for 13 entities (11%)

- 2 Providers, 9 Health Plans, 2 Clearinghouses

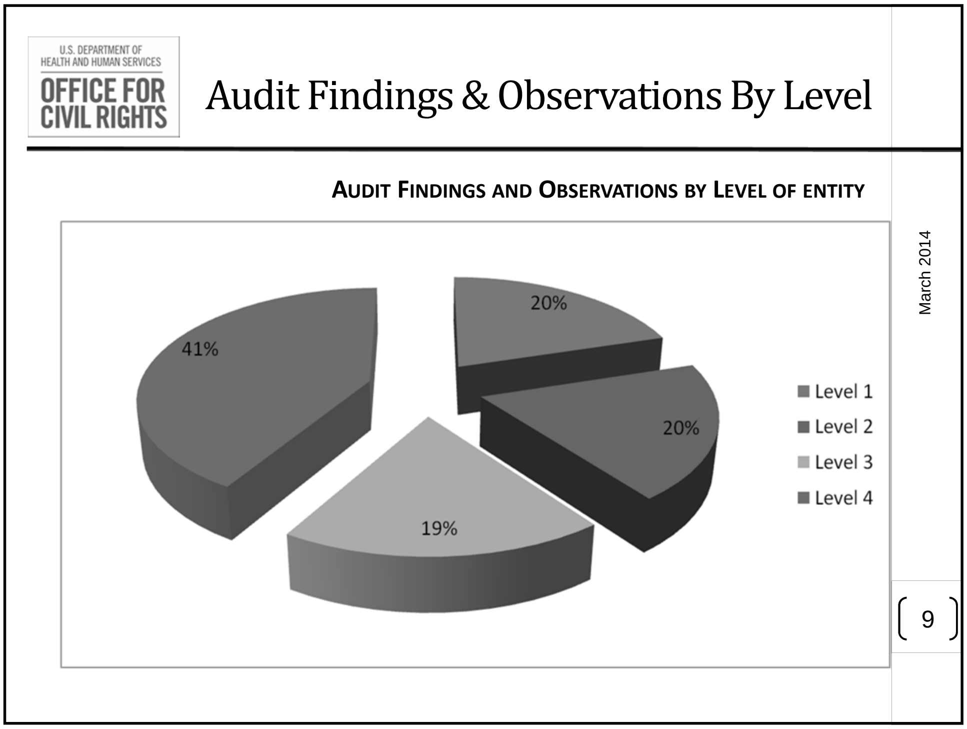
Security accounted for 60% of the findings and observations—although only 28% of potential total.

Providers had a greater proportion of findings & observations (65%) than reflected by their proportion of the total set (53%).

Smaller, *Level 4* **entities struggle** with all three areas

March 2014

8

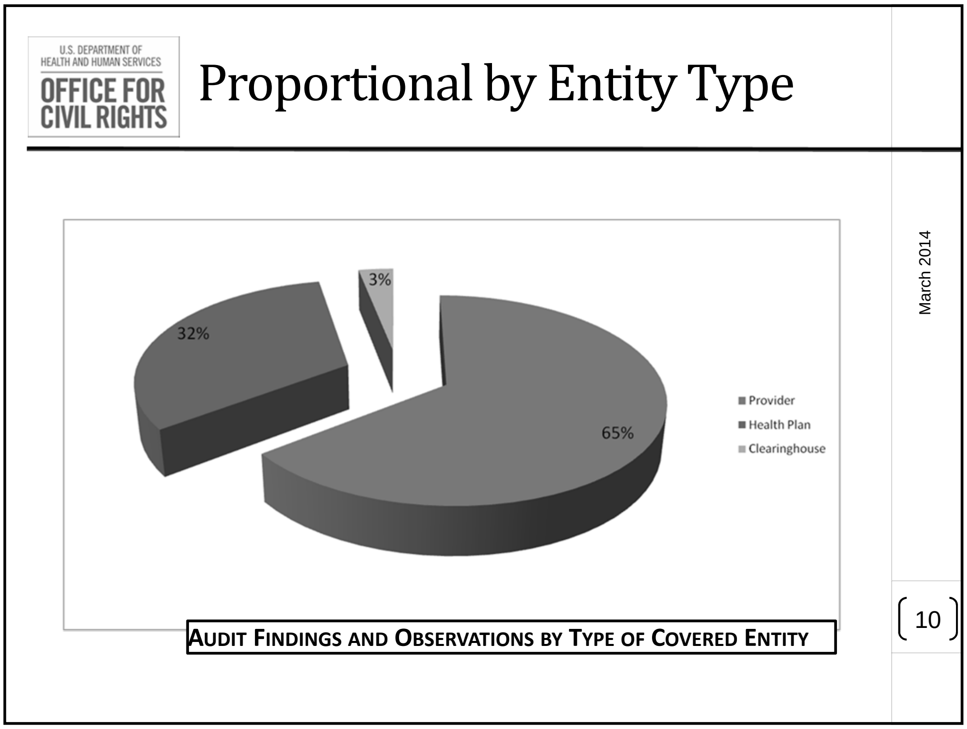


Audit Findings & Observations By Level

AUDIT FINDINGS AND OBSERVATIONS BY LEVEL OF ENTITY

March 2014

9



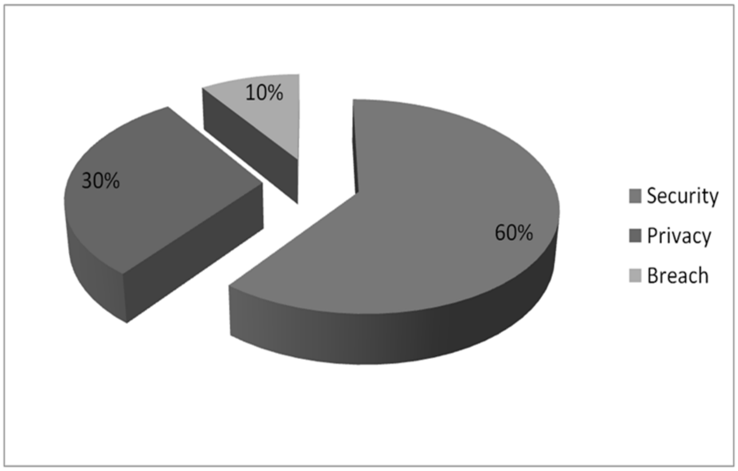
Proportional by Entity Type

AUDIT FINDINGS AND OBSERVATIONS BY TYPE OF COVERED ENTITY

March 2014

10

Proportional Findings by Rule

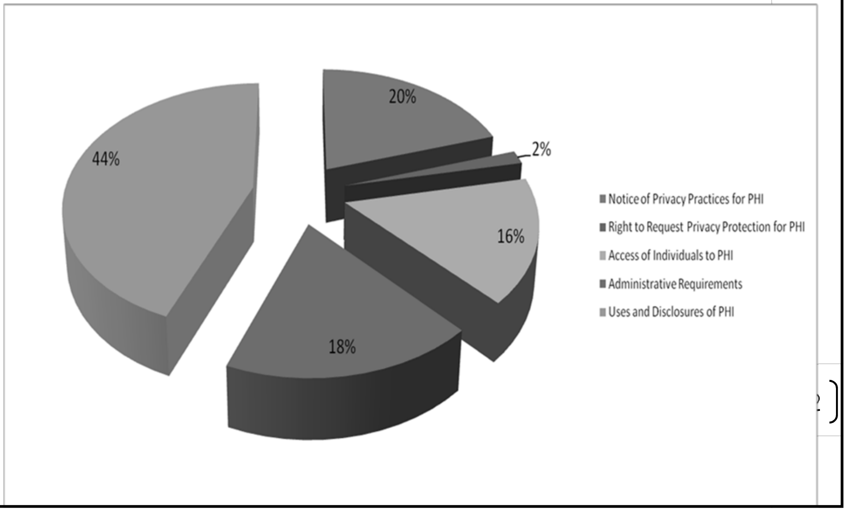


March 2014

Audit Findings and Observations by Rule

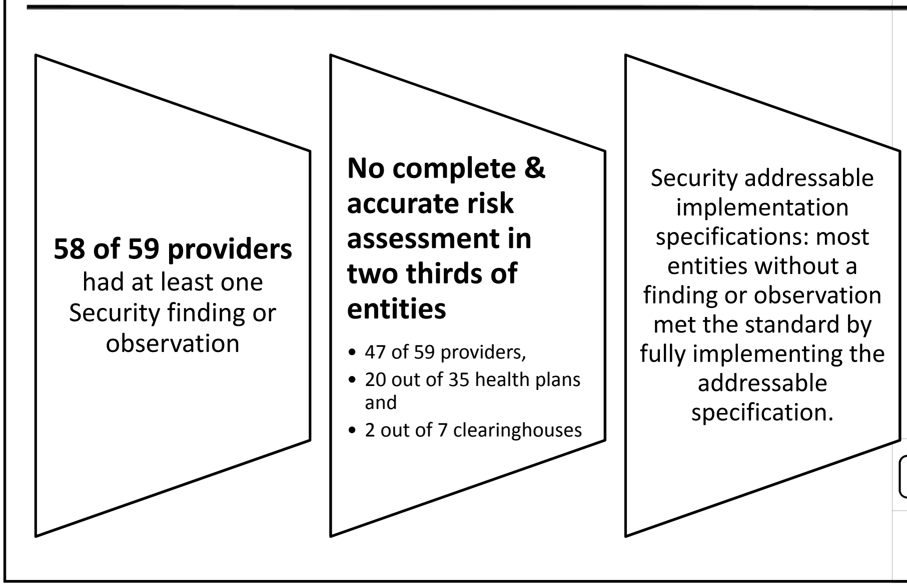
Privacy Findings & Observations

PERCENTAGE OF FINDINGS AND OBSERVATIONS BY AREA OF FOCUS



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Security Results



58 of 59 providers had at least one Security finding or observation

No complete & accurate risk assessment in two thirds of entities

- 47 of 59 providers,
- 20 out of 35 health plans and
- 2 out of 7 clearinghouses

Security addressable implementation specifications: most entities without a finding or observation met the standard by fully implementing the addressable specification.

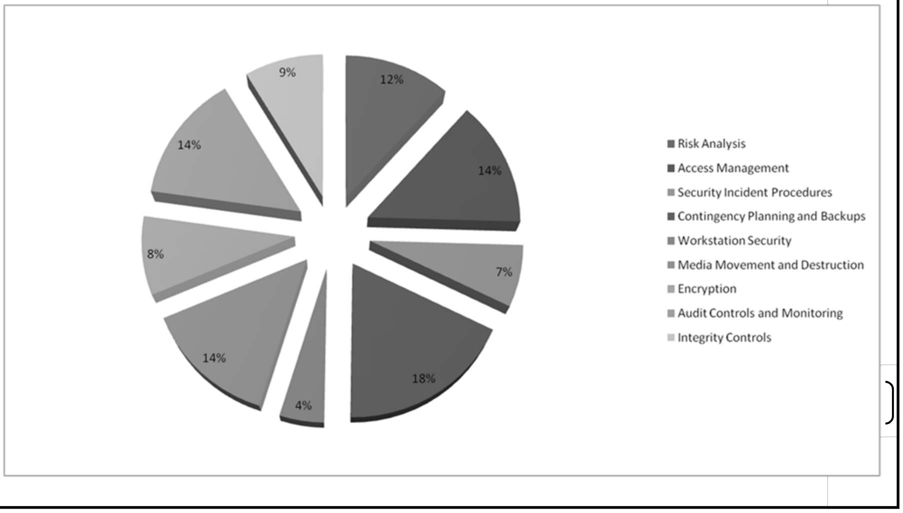
March 2014

13

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

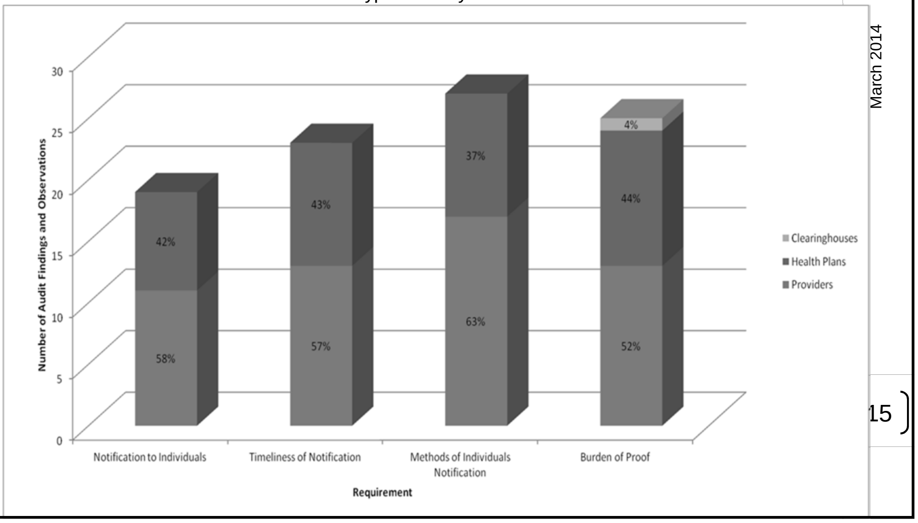
Security Elements

Percentage of Audit Findings and Observations by Area of Focus



Breach Notification by Entity Type

Audit Findings and Observations by Requirement and Type of Entity



Overall Cause Analysis

- For every finding and observation cited in the audit reports, audit identified a "Cause."
- Most common across all entities: **entity unaware of the requirement.**
  - in 30% (289 of 980 findings and observations)
    - **39% (115 of 293) of Privacy**
    - **27% (163 of 593) of Security**
    - **12% (11) of Breach Notification**
  - Most of these related to elements of the Rules that explicitly state what a covered entity must do to comply.
- Other causes noted included but not limited to:
  - Lack of application of sufficient resources
  - Incomplete implementation
  - Complete disregard

Cause Analysis – Top Elements
Unaware of the Requirement

Privacy

- Notice of Privacy Practices;
- Access of Individuals;
- Minimum Necessary; and,
- Authorizations.

Security

- Risk Analysis;
- Media Movement and Disposal; and,
- Audit Controls and Monitoring.

March 2014

17

Objectives

Communications

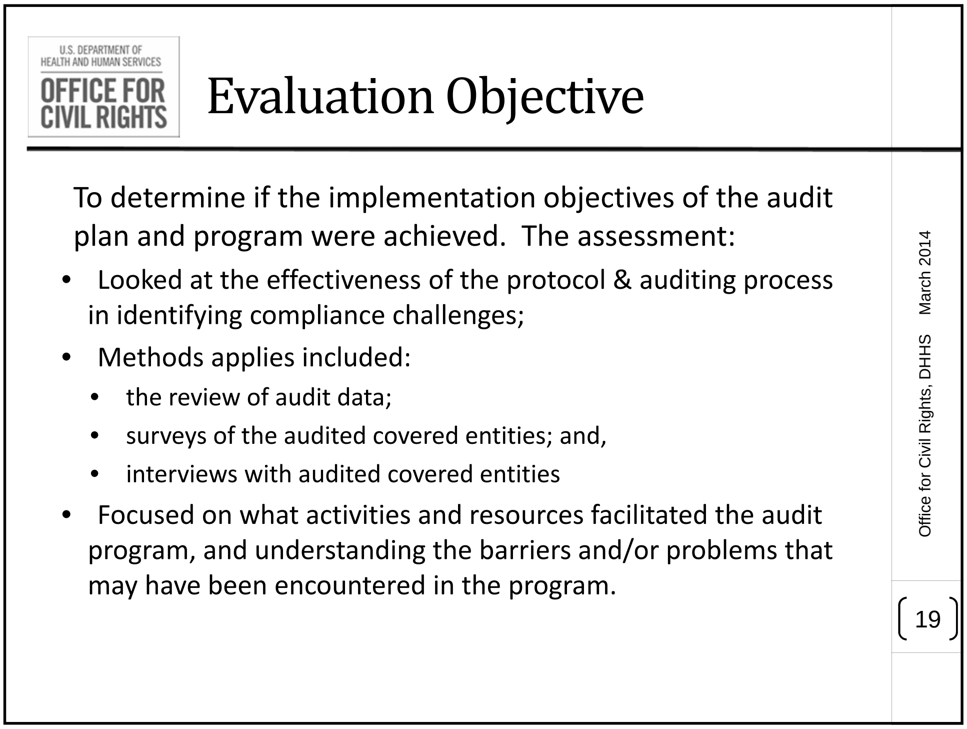
Entity Selection

Protocols

PHASE ONE PROGRAM EVALUATION

March 2014

18



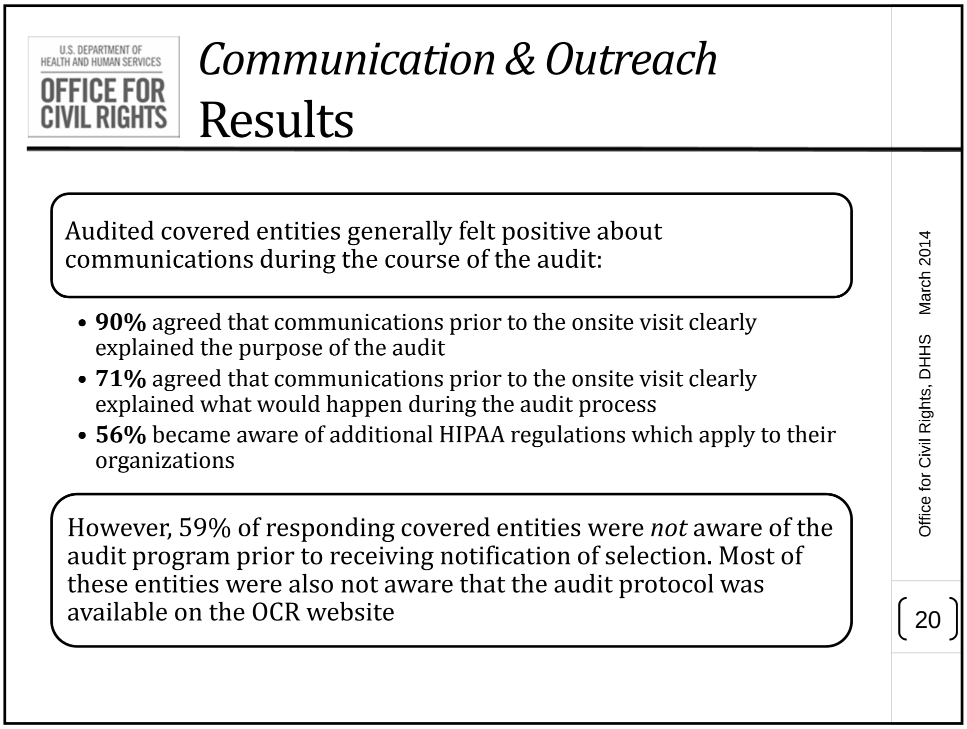
Evaluation Objective

To determine if the implementation objectives of the audit plan and program were achieved. The assessment:

- Looked at the effectiveness of the protocol & auditing process in identifying compliance challenges;
- Methods applies included:
  - the review of audit data;
  - surveys of the audited covered entities; and,
  - interviews with audited covered entities
- Focused on what activities and resources facilitated the audit program, and understanding the barriers and/or problems that may have been encountered in the program.

Office for Civil Rights, DHHS March 2014

19



Communication & Outreach Results

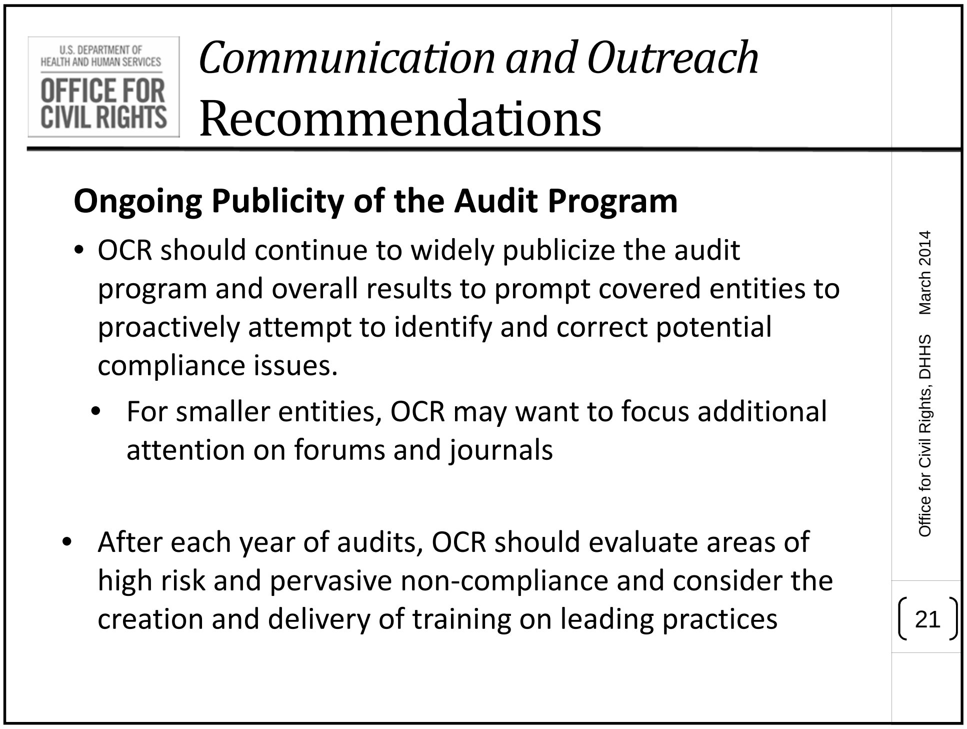
Audited covered entities generally felt positive about communications during the course of the audit:

- **90%** agreed that communications prior to the onsite visit clearly explained the purpose of the audit
- **71%** agreed that communications prior to the onsite visit clearly explained what would happen during the audit process
- **56%** became aware of additional HIPAA regulations which apply to their organizations

However, 59% of responding covered entities were *not* aware of the audit program prior to receiving notification of selection. Most of these entities were also not aware that the audit protocol was available on the OCR website

Office for Civil Rights, DHHS March 2014

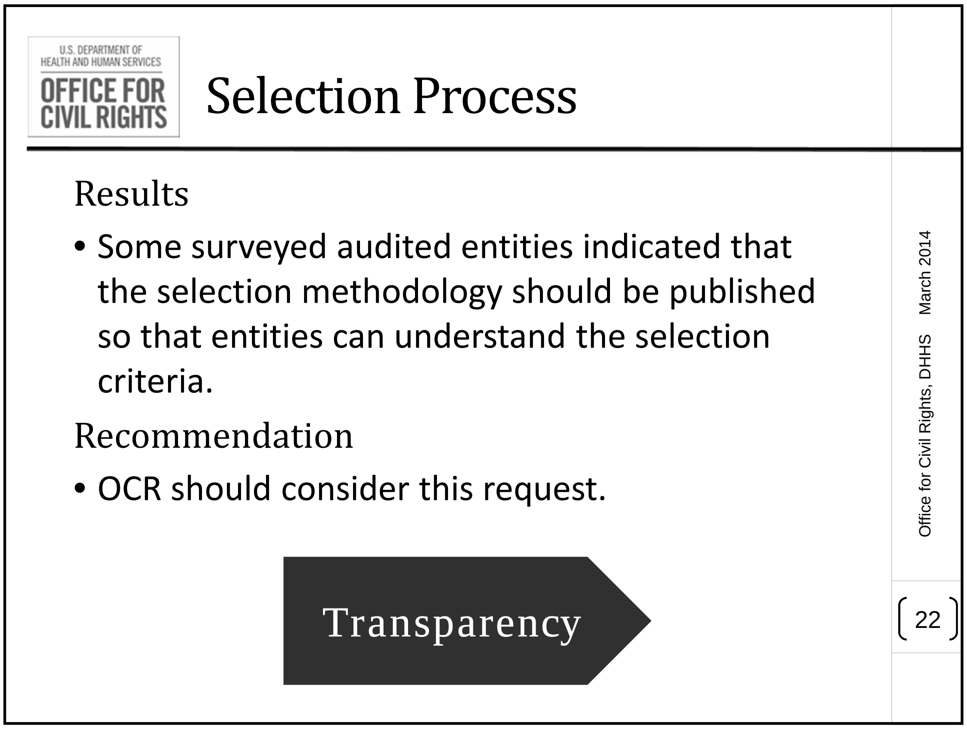
20



Communication and Outreach Recommendations

Ongoing Publicity of the Audit Program

- OCR should continue to widely publicize the audit program and overall results to prompt covered entities to proactively attempt to identify and correct potential compliance issues.
  - For smaller entities, OCR may want to focus additional attention on forums and journals
- After each year of audits, OCR should evaluate areas of high risk and pervasive non-compliance and consider the creation and delivery of training on leading practices



Selection Process

Results

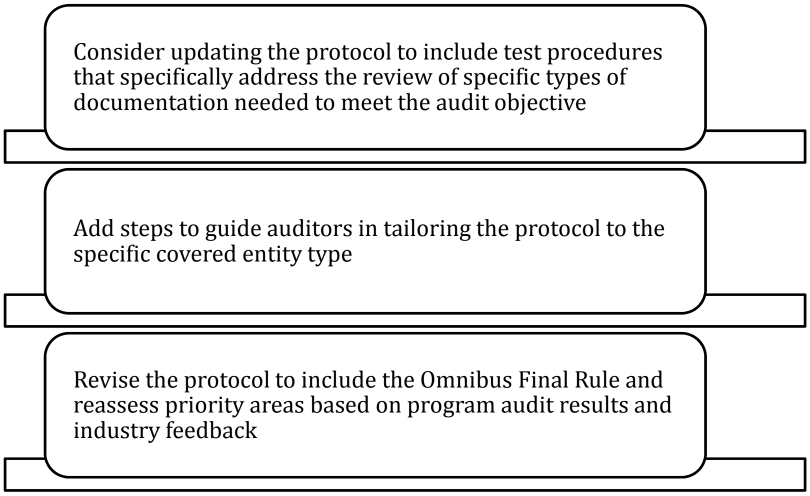
- Some surveyed audited entities indicated that the selection methodology should be published so that entities can understand the selection criteria.

Recommendation

- OCR should consider this request.

Transparency

Recommendations: Protocol Modifications



Consider updating the protocol to include test procedures that specifically address the review of specific types of documentation needed to meet the audit objective

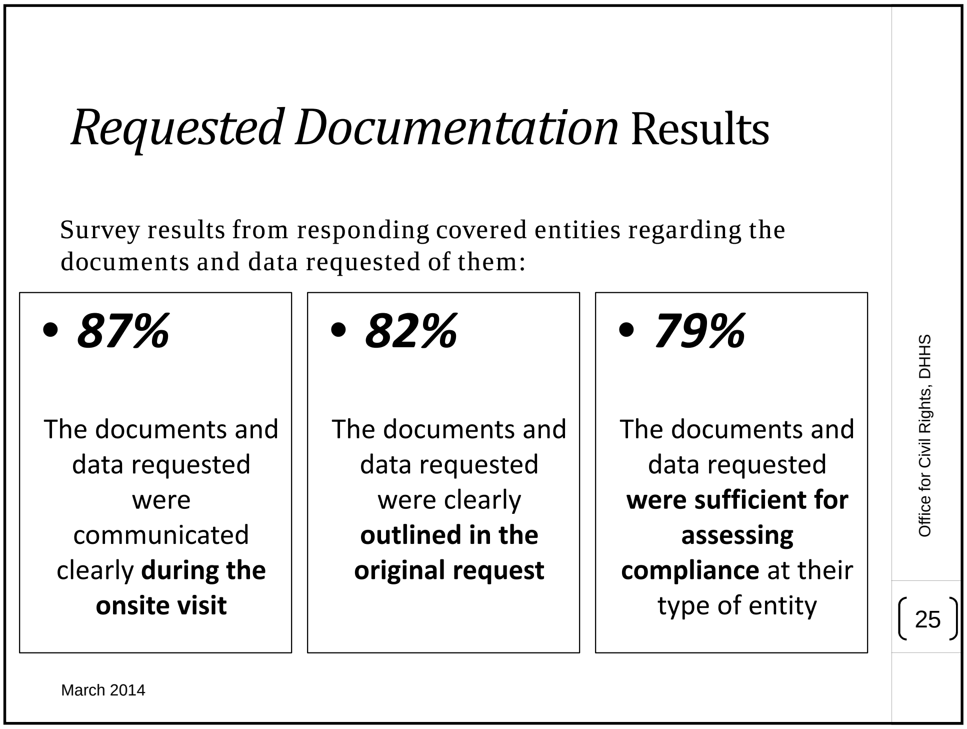
Add steps to guide auditors in tailoring the protocol to the specific covered entity type

Revise the protocol to include the Omnibus Final Rule and reassess priority areas based on program audit results and industry feedback

Selection of Requirements to Audit-- Recommendations

Implement a Risk-Based Approach

- A risk-based approach for applying audit protocols would allow OCR to determine areas of the Rules which require implementation of controls which, if not implemented effectively, pose the greatest risk to the protection of PHI.
- OCR should consider a multi-tiered audit approach which can be tailored based on entity type, area or a hybrid.



Requested Documentation Results

Survey results from responding covered entities regarding the documents and data requested of them:

- ***87%***

  The documents and data requested were communicated clearly **during the onsite visit**

- ***82%***

  The documents and data requested were clearly **outlined in the original request**

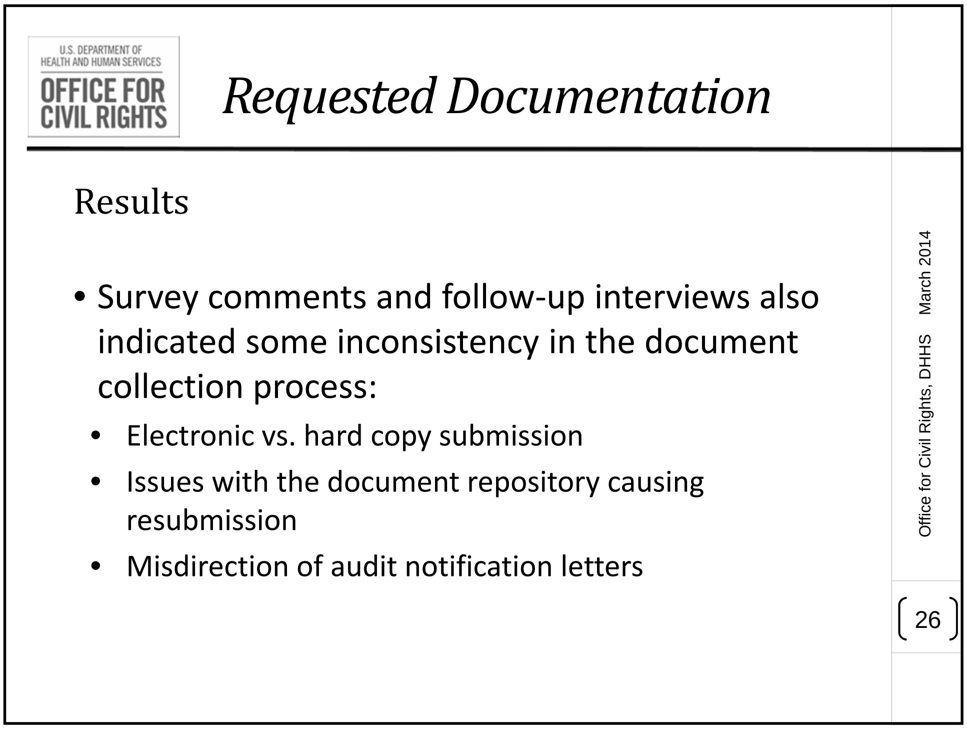
- ***79%***

  The documents and data requested **were sufficient for assessing compliance** at their type of entity

March 2014

Office for Civil Rights, DHHS

25



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS

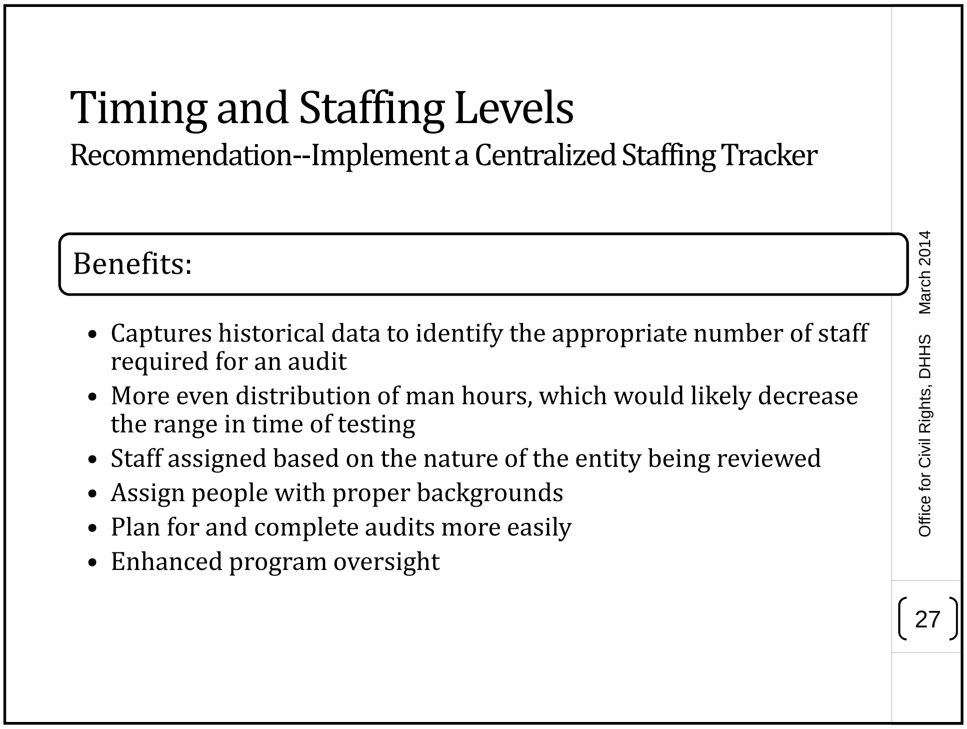
Requested Documentation

Results

- Survey comments and follow-up interviews also indicated some inconsistency in the document collection process:
  - Electronic vs. hard copy submission
  - Issues with the document repository causing resubmission
  - Misdirection of audit notification letters

Office for Civil Rights, DHHS March 2014

26

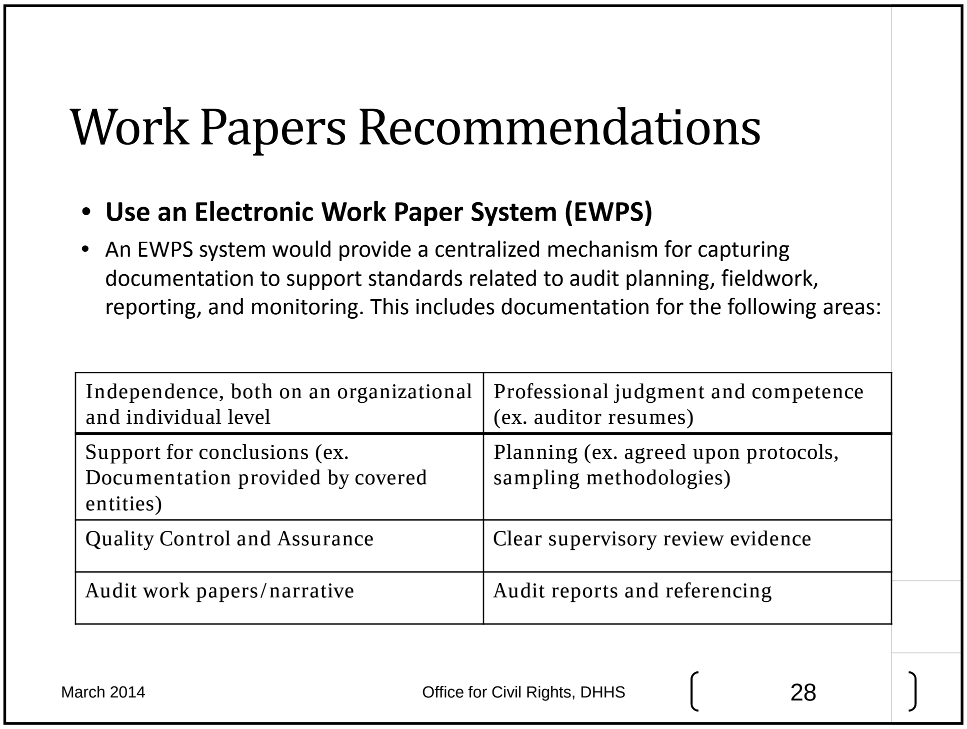


Timing and Staffing Levels

Recommendation--Implement a Centralized Staffing Tracker

Benefits:

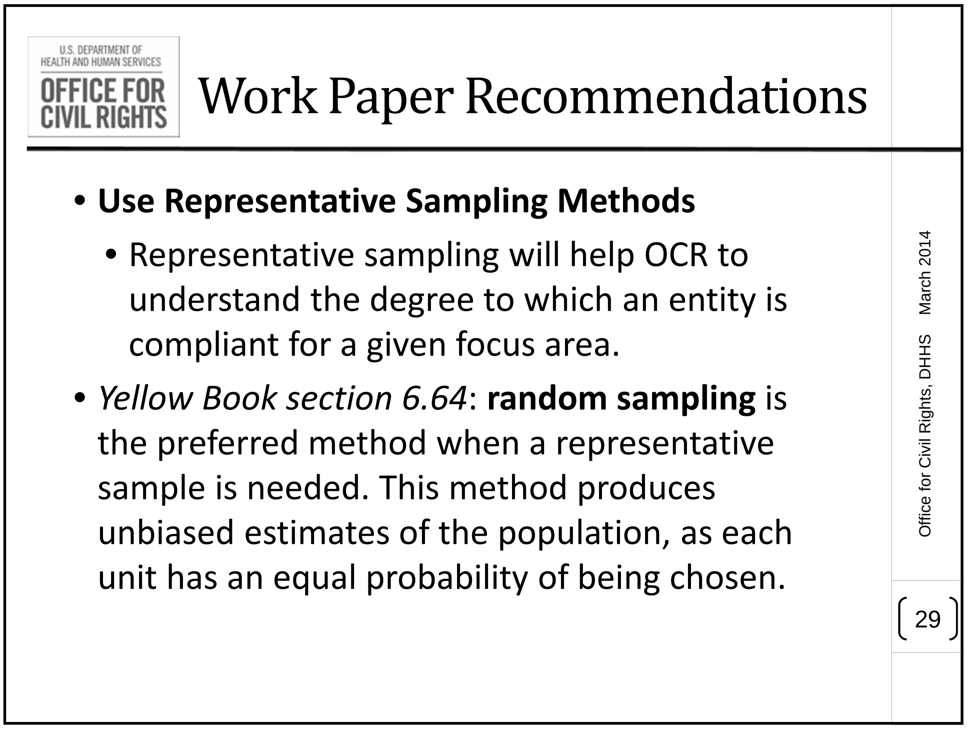
- Captures historical data to identify the appropriate number of staff required for an audit
- More even distribution of man hours, which would likely decrease the range in time of testing
- Staff assigned based on the nature of the entity being reviewed
- Assign people with proper backgrounds
- Plan for and complete audits more easily
- Enhanced program oversight



Work Papers Recommendations

- **Use an Electronic Work Paper System (EWPS)**
- An EWPS system would provide a centralized mechanism for capturing documentation to support standards related to audit planning, fieldwork, reporting, and monitoring. This includes documentation for the following areas:

Independence, both on an organizational and individual level	Professional judgment and competence (ex. auditor resumes)
Support for conclusions (ex. Documentation provided by covered entities)	Planning (ex. agreed upon protocols, sampling methodologies)
Quality Control and Assurance	Clear supervisory review evidence
Audit work papers/narrative	Audit reports and referencing

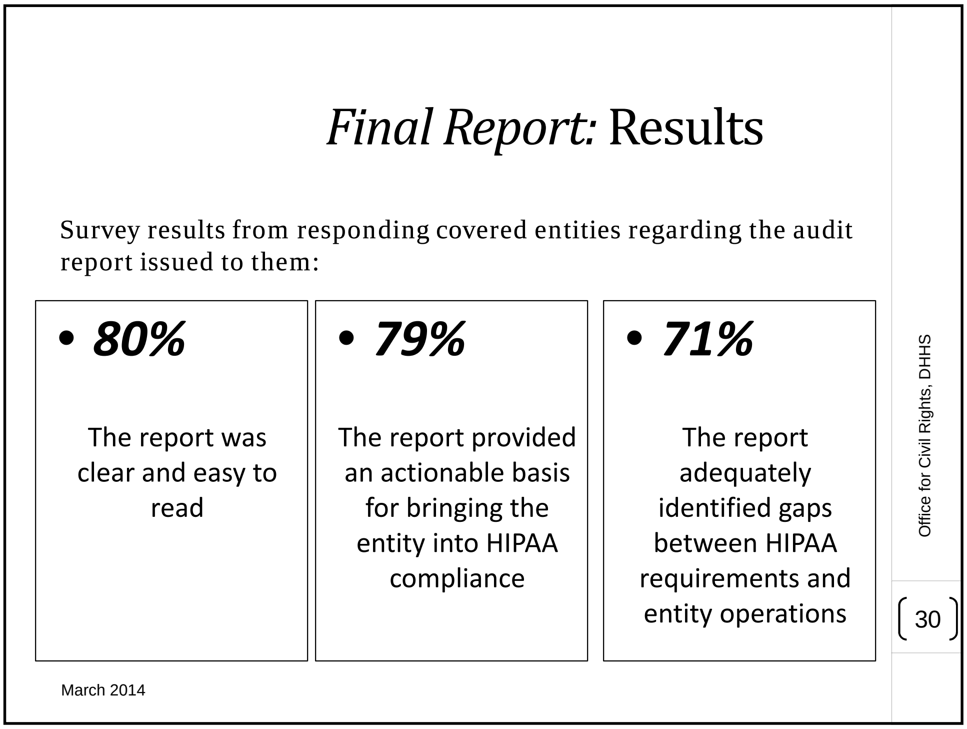


Work Paper Recommendations

- **Use Representative Sampling Methods**
  - Representative sampling will help OCR to understand the degree to which an entity is compliant for a given focus area.
- *Yellow Book section 6.64*: **random sampling** is the preferred method when a representative sample is needed. This method produces unbiased estimates of the population, as each unit has an equal probability of being chosen.

Office for Civil Rights, DHHS March 2014

29



Final Report: Results

Survey results from responding covered entities regarding the audit report issued to them:

- ***80%***

  The report was clear and easy to read

- ***79%***

  The report provided an actionable basis for bringing the entity into HIPAA compliance

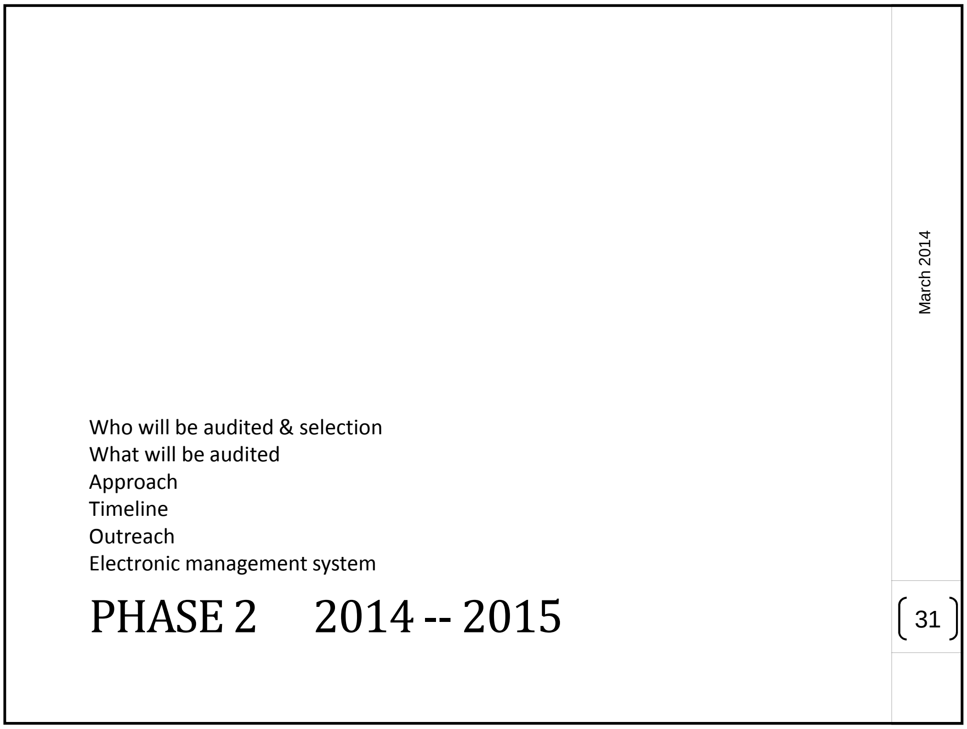
- ***71%***

  The report adequately identified gaps between HIPAA requirements and entity operations

March 2014

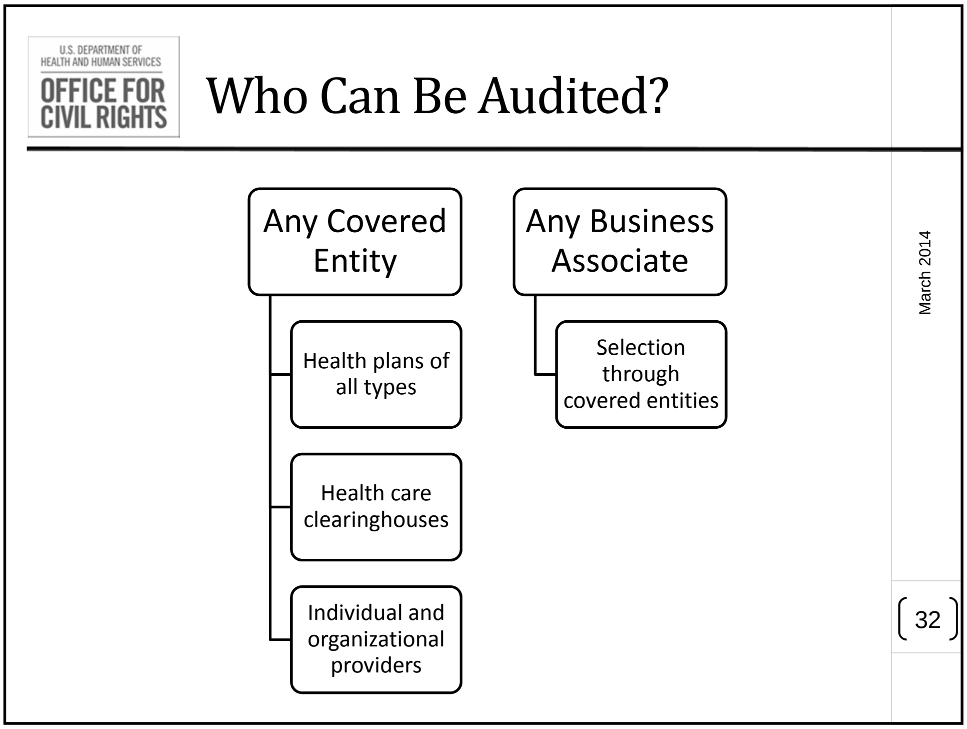
Office for Civil Rights, DHHS

30



Who will be audited & selection
What will be audited
Approach
Timeline
Outreach
Electronic management system

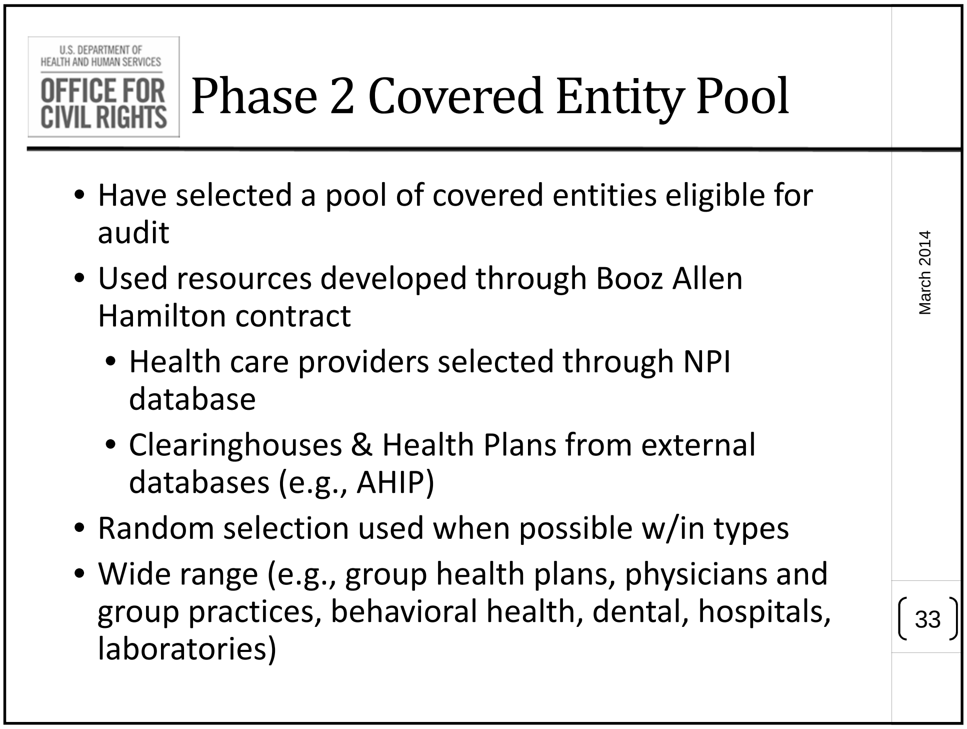
PHASE 2   2014 -- 2015



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS

Who Can Be Audited?

- Any Covered Entity
  - Health plans of all types
  - Health care clearinghouses
  - Individual and organizational providers
- Any Business Associate
  - Selection through covered entities

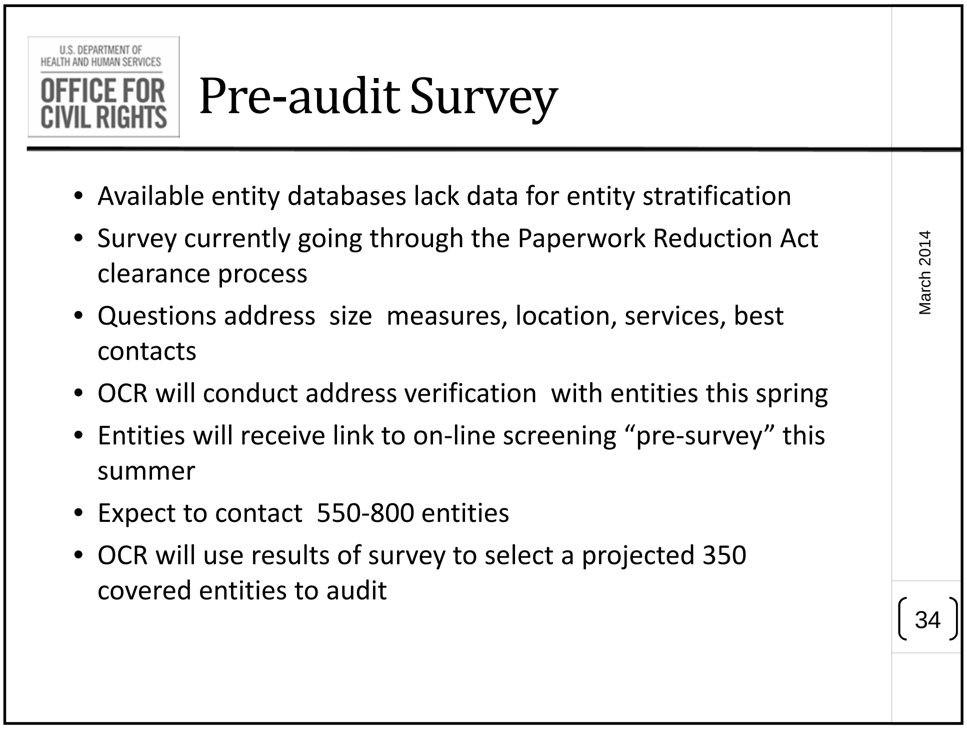


Phase 2 Covered Entity Pool

- Have selected a pool of covered entities eligible for audit
- Used resources developed through Booz Allen Hamilton contract
  - Health care providers selected through NPI database
  - Clearinghouses & Health Plans from external databases (e.g., AHIP)
- Random selection used when possible w/in types
- Wide range (e.g., group health plans, physicians and group practices, behavioral health, dental, hospitals, laboratories)

March 2014

33



Pre-audit Survey

- Available entity databases lack data for entity stratification
- Survey currently going through the Paperwork Reduction Act clearance process
- Questions address size measures, location, services, best contacts
- OCR will conduct address verification with entities this spring
- Entities will receive link to on-line screening “pre-survey” this summer
- Expect to contact 550-800 entities
- OCR will use results of survey to select a projected 350 covered entities to audit

March 2014

34

Audit Phase 2 Approach

- Primarily internally staffed
- Selected entities will receive notification and data requests in fall 2014
- Entities will be asked to identify their business associates and provide their current contact information
- Will select business associate audit subjects for 2015 first wave from among the BAs identified by covered entities
- Desk audits of selected provisions
- Comprehensive on-site audits as resources allow

DHHS, OCR April 2014

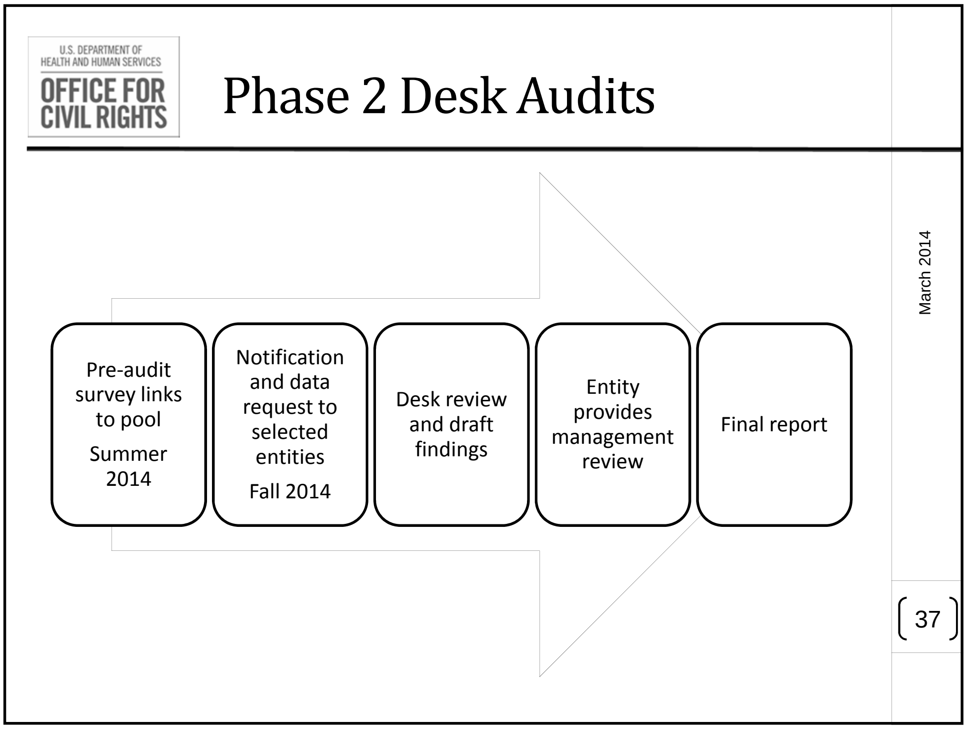
35

Phase 2 Audit Distribution Projections

Entity Type	Privacy	Breach	Security
Covered Entities	100	100	150
• **Health Plans**	33	31	45
• **Providers**	67	65	100
• **Clearinghouses**	-	4	5
Business Associates	0	0	50
• **IT Related**	-	-	35
• **Non-IT Related (eg, TPAs, claims)**	-	-	15
Total Audits by Protocol	100	100	200

March 2014

36



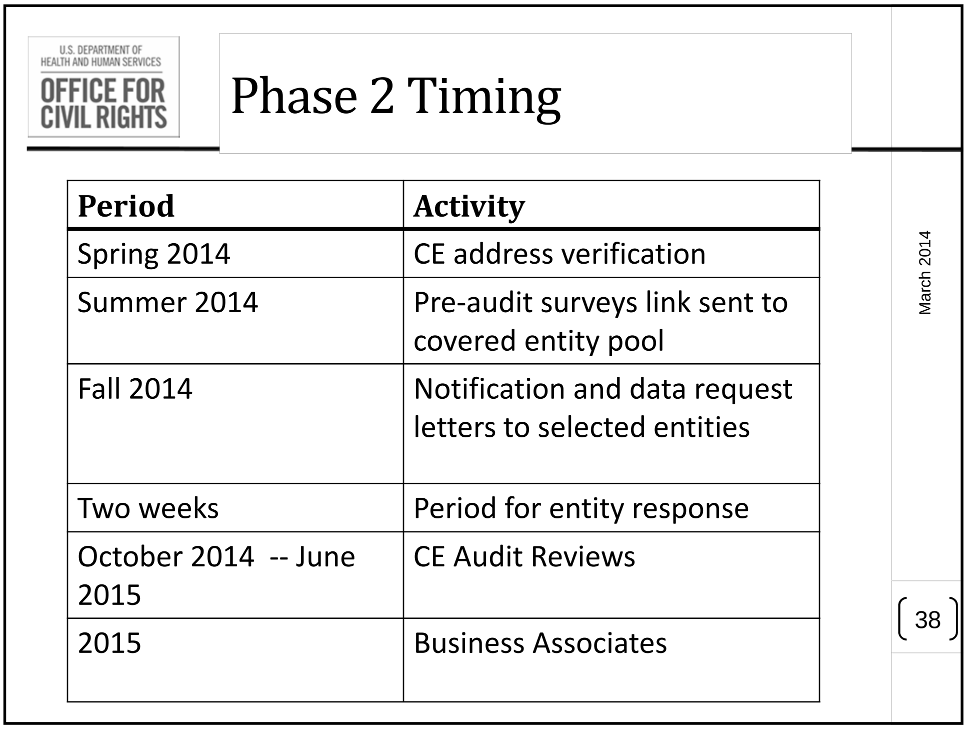
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS

Phase 2 Desk Audits

- Pre-audit survey links to pool
Summer 2014
- Notification and data request to selected entities
Fall 2014
- Desk review and draft findings
- Entity provides management review
- Final report

March 2014

37



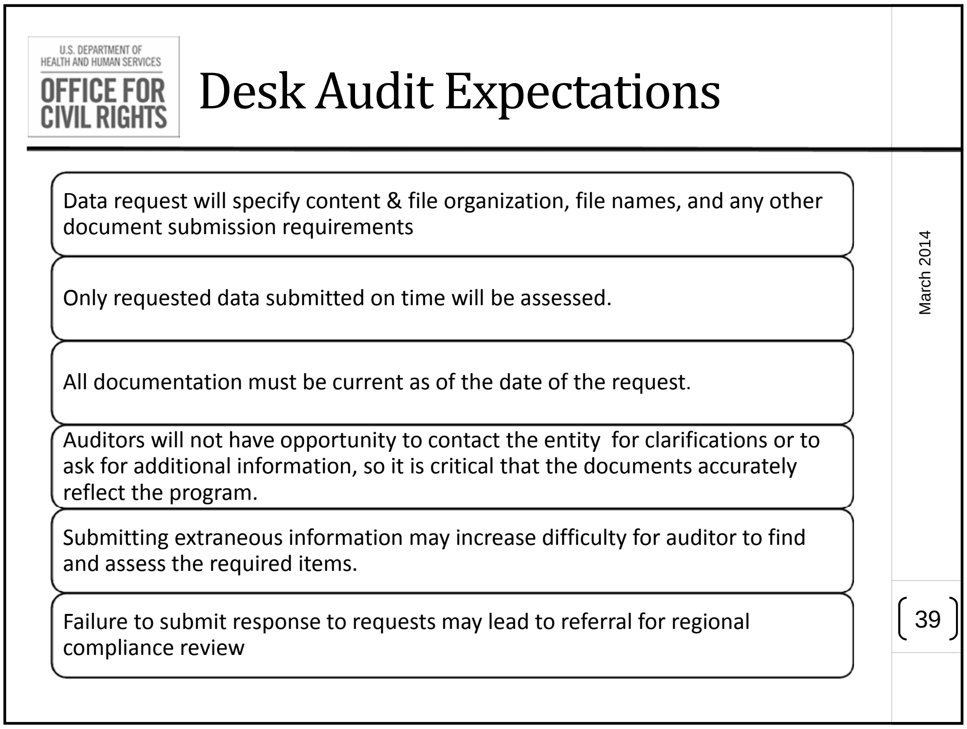
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS

Phase 2 Timing

Period	**Activity**
Spring 2014	CE address verification
Summer 2014	Pre-audit surveys link sent to covered entity pool
Fall 2014	Notification and data request letters to selected entities
Two weeks	Period for entity response
October 2014 -- June 2015	CE Audit Reviews
2015	Business Associates

March 2014

38



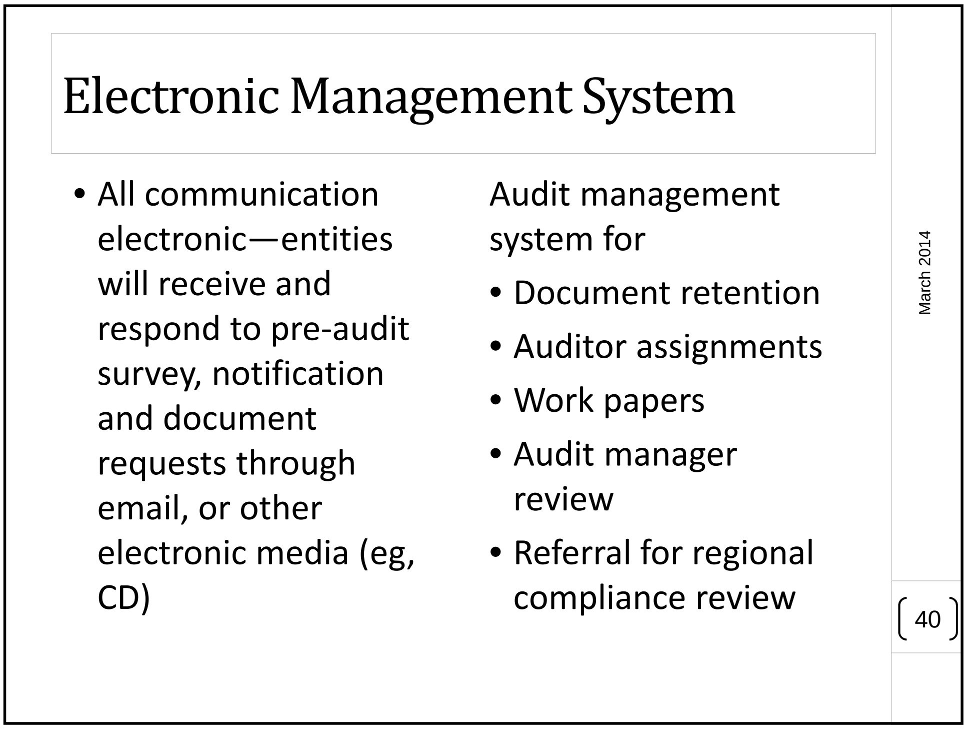
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS

Desk Audit Expectations

- Data request will specify content & file organization, file names, and any other document submission requirements
- Only requested data submitted on time will be assessed.
- All documentation must be current as of the date of the request.
- Auditors will not have opportunity to contact the entity for clarifications or to ask for additional information, so it is critical that the documents accurately reflect the program.
- Submitting extraneous information may increase difficulty for auditor to find and assess the required items.
- Failure to submit response to requests may lead to referral for regional compliance review

March 2014

39



Electronic Management System

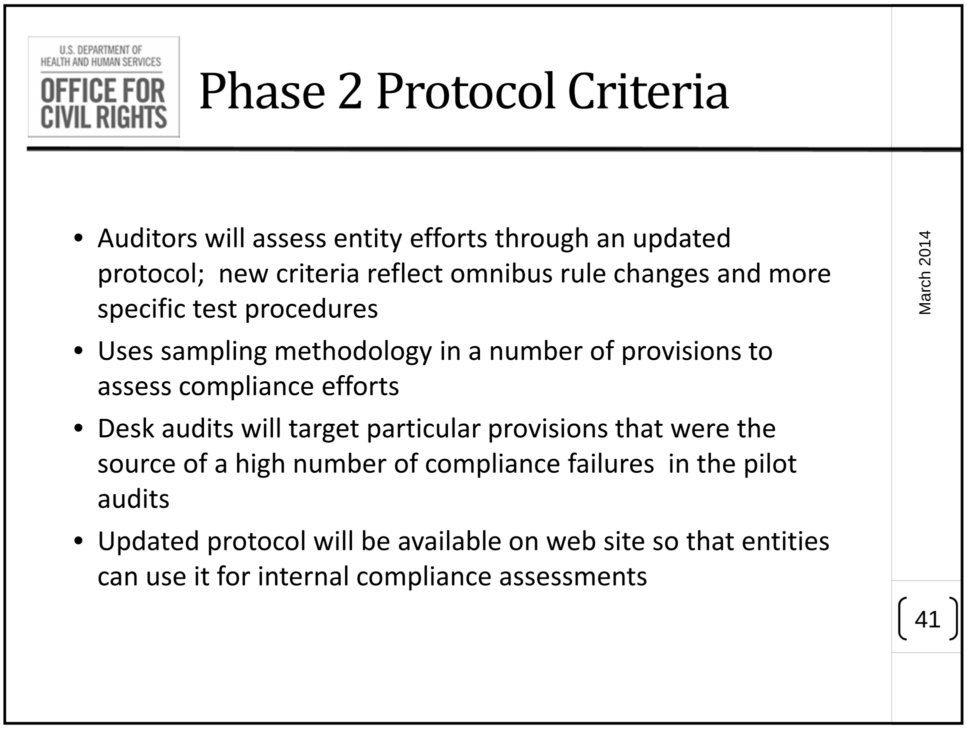
- All communication electronic—entities will receive and respond to pre-audit survey, notification and document requests through email, or other electronic media (eg, CD)

Audit management system for

- Document retention
- Auditor assignments
- Work papers
- Audit manager review
- Referral for regional compliance review

March 2014

40



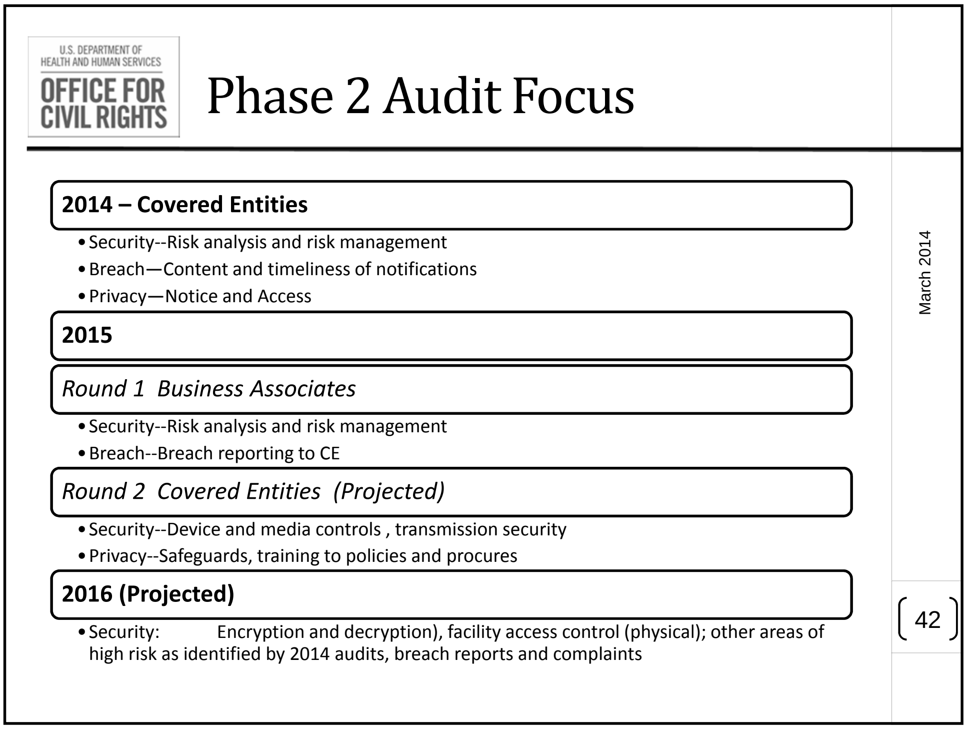
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Phase 2 Protocol Criteria

- Auditors will assess entity efforts through an updated protocol; new criteria reflect omnibus rule changes and more specific test procedures
- Uses sampling methodology in a number of provisions to assess compliance efforts
- Desk audits will target particular provisions that were the source of a high number of compliance failures in the pilot audits
- Updated protocol will be available on web site so that entities can use it for internal compliance assessments

March 2014

41



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Phase 2 Audit Focus

2014 – Covered Entities

- Security--Risk analysis and risk management
- Breach—Content and timeliness of notifications
- Privacy—Notice and Access

2015

Round 1 Business Associates

- Security--Risk analysis and risk management
- Breach--Breach reporting to CE

Round 2 Covered Entities (Projected)

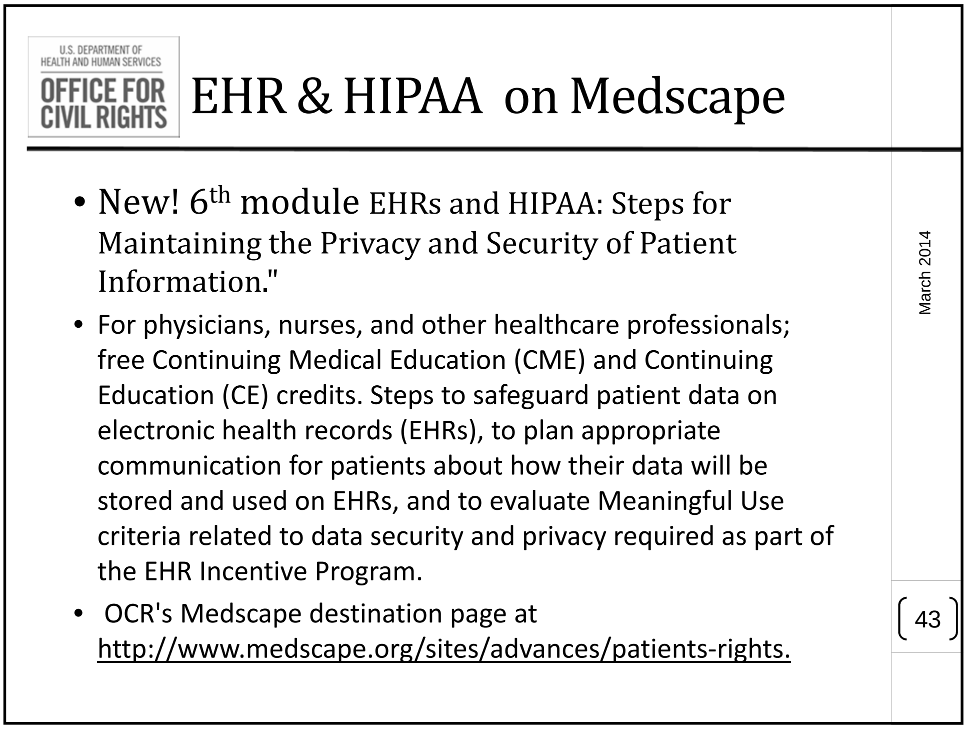
- Security--Device and media controls , transmission security
- Privacy--Safeguards, training to policies and procures

2016 (Projected)

- Security: Encryption and decryption), facility access control (physical); other areas of high risk as identified by 2014 audits, breach reports and complaints

March 2014

42



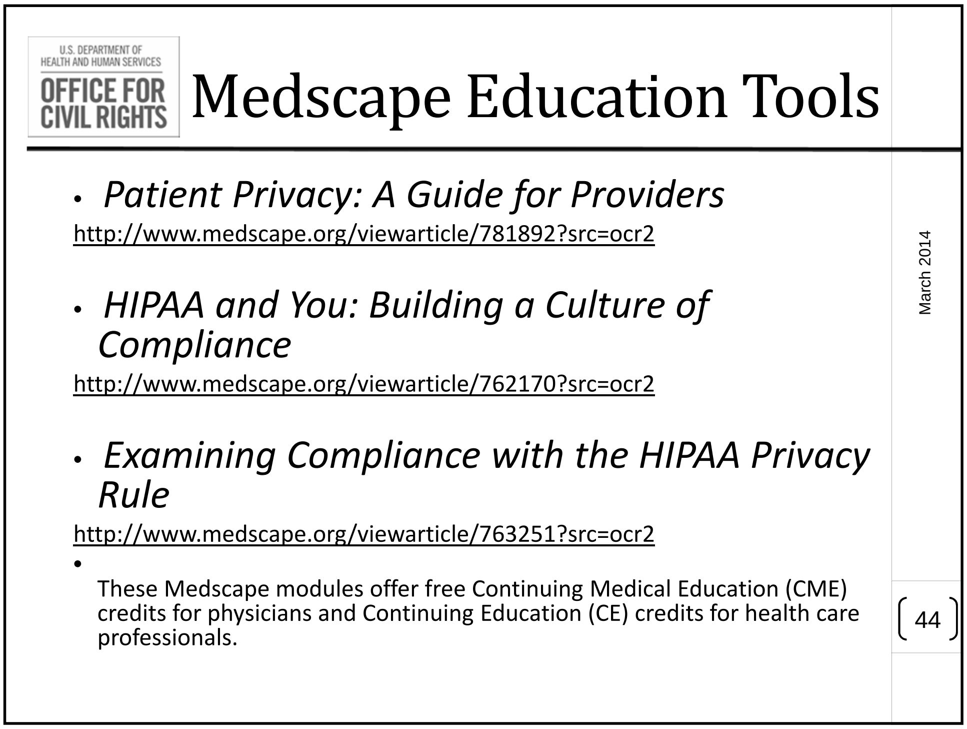
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS

EHR & HIPAA on Medscape

- New! 6th module EHRs and HIPAA: Steps for Maintaining the Privacy and Security of Patient Information."
- For physicians, nurses, and other healthcare professionals; free Continuing Medical Education (CME) and Continuing Education (CE) credits. Steps to safeguard patient data on electronic health records (EHRs), to plan appropriate communication for patients about how their data will be stored and used on EHRs, and to evaluate Meaningful Use criteria related to data security and privacy required as part of the EHR Incentive Program.
- OCR's Medscape destination page at http://www.medscape.org/sites/advances/patients-rights.

March 2014

43



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS

Medscape Education Tools

- *Patient Privacy: A Guide for Providers*

http://www.medscape.org/viewarticle/781892?src=ocr2

- *HIPAA and You: Building a Culture of Compliance*

http://www.medscape.org/viewarticle/762170?src=ocr2

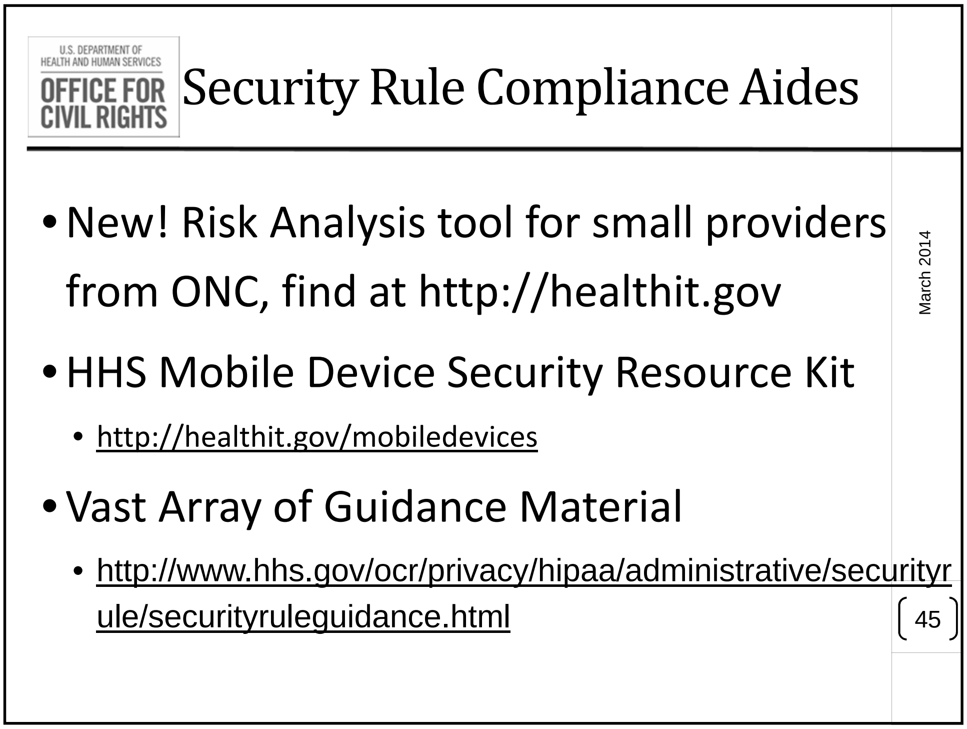
- *Examining Compliance with the HIPAA Privacy Rule*

http://www.medscape.org/viewarticle/763251?src=ocr2

- These Medscape modules offer free Continuing Medical Education (CME) credits for physicians and Continuing Education (CE) credits for health care professionals.

March 2014

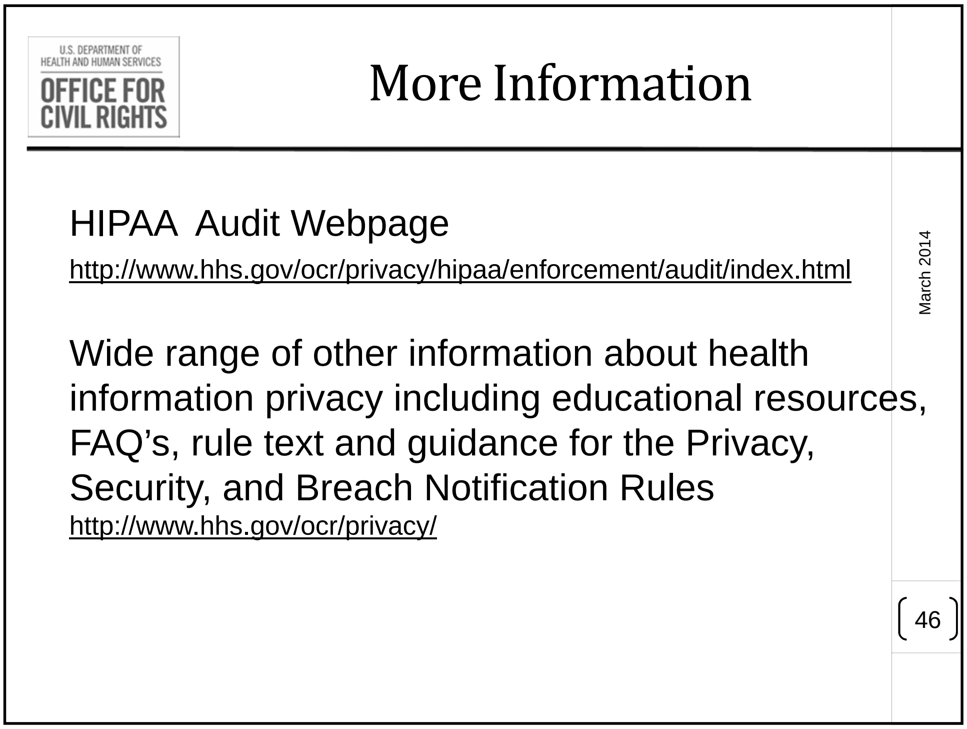
44



Security Rule Compliance Aides

- New! Risk Analysis tool for small providers from ONC, find at http://healthit.gov
- HHS Mobile Device Security Resource Kit
  - http://healthit.gov/mobiledevices
- Vast Array of Guidance Material
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

March 2014



More Information

HIPAA Audit Webpage

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html

Wide range of other information about health information privacy including educational resources, FAQ’s, rule text and guidance for the Privacy, Security, and Breach Notification Rules
http://www.hhs.gov/ocr/privacy/

March 2014