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

HIPAA Privacy, Security and Breach Notification Audits

Program Overview & Initial Analysis

Verne Rinker JD, MPH

2013 NIST / OCR Security Rule Conference

May 21-22, 2013

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

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

- Examine mechanisms for compliance
- Identify best practices
- Discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews
- Encourage renewed attention to compliance activities

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

Multi-year Audit Plan

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, Inc.	Closed 2011-2012
Evaluation of audit program	PWC, LLP	Open Conclude in 2013

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

2011/2012 Implementation

Audit Protocol Design

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

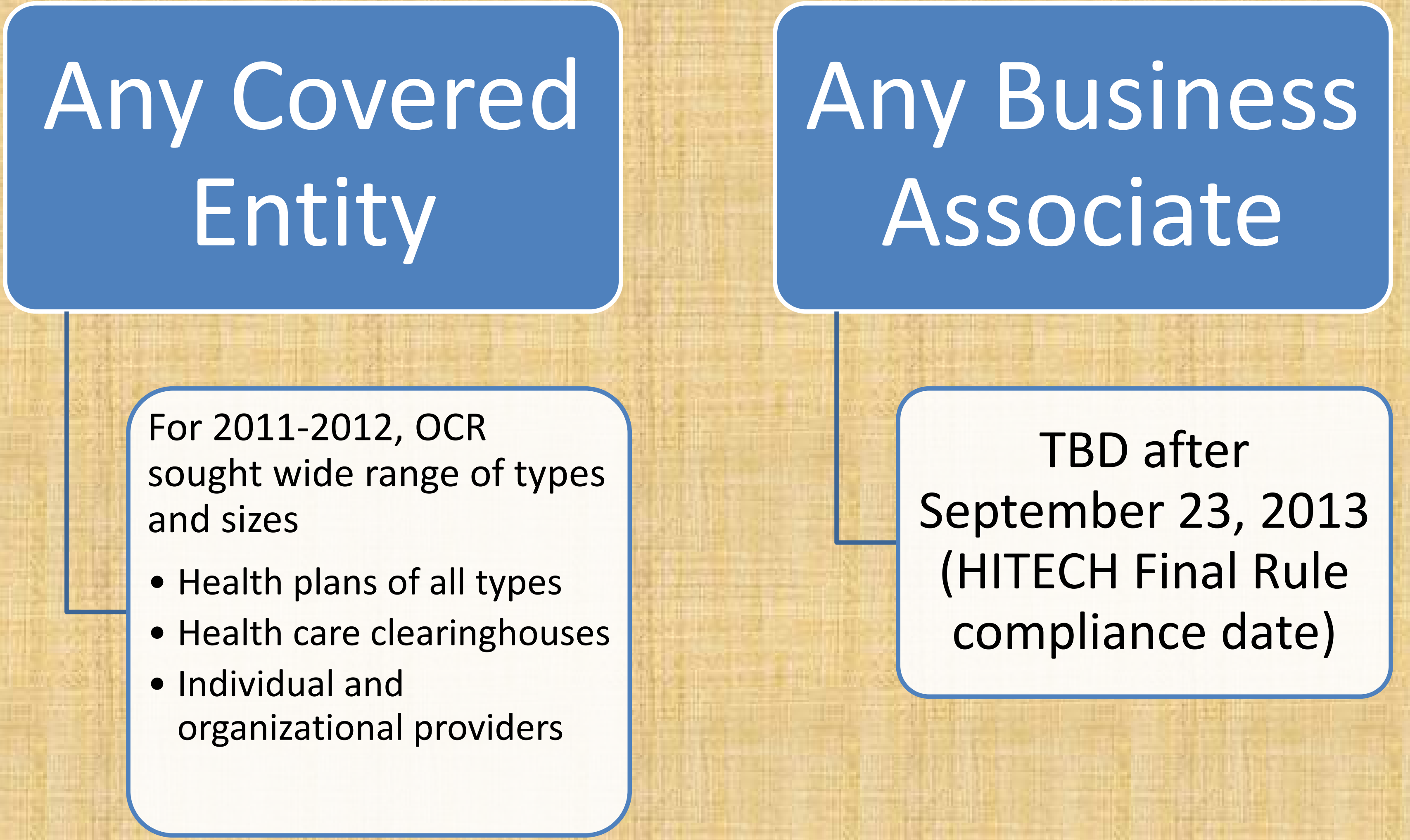
Resulting Audit Program

- 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

What is a Performance Audit?

- An audit service conducted in accordance with GAGAS, Generally Accepted Government Auditing Standards (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 users
- Can entail objective assessments of a variety of attributes:
  - Program effectiveness, economy, and efficiency
  - Internal control
  - Compliance
  - Other questions of interest to management (e.g. value of assets, determination of pension benefits)

Who Can Be Audited?



Any Covered Entity

For 2011-2012, OCR sought wide range of types and sizes

- Health plans of all types
- Health care clearinghouses
- Individual and organizational providers

Any Business Associate

TBD after September 23, 2013 (HITECH Final Rule compliance date)

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

Breakdown of 2012 Auditees

Level 1 Entities

- Large Provider / Health Plan
- Extensive use of HIT - complicated HIT enabled clinical /business work streams
- Revenues and or assets greater than $1 billion

Level 2 Entities

- Large regional hospital system (3-10 hospitals/region) / Regional Insurance Company
- Paper and HIT enabled work flows
- Revenues and or assets $300 million to $1 billion

Level 3 Entities

Community hospitals, outpatient surgery, regional pharmacy / All Self-Insured entities that don't adjudicate their claims

- Some but not extensive use of HIT – mostly paper based workflows
- Revenues $50 Million to $300 million

Level 4 Entities

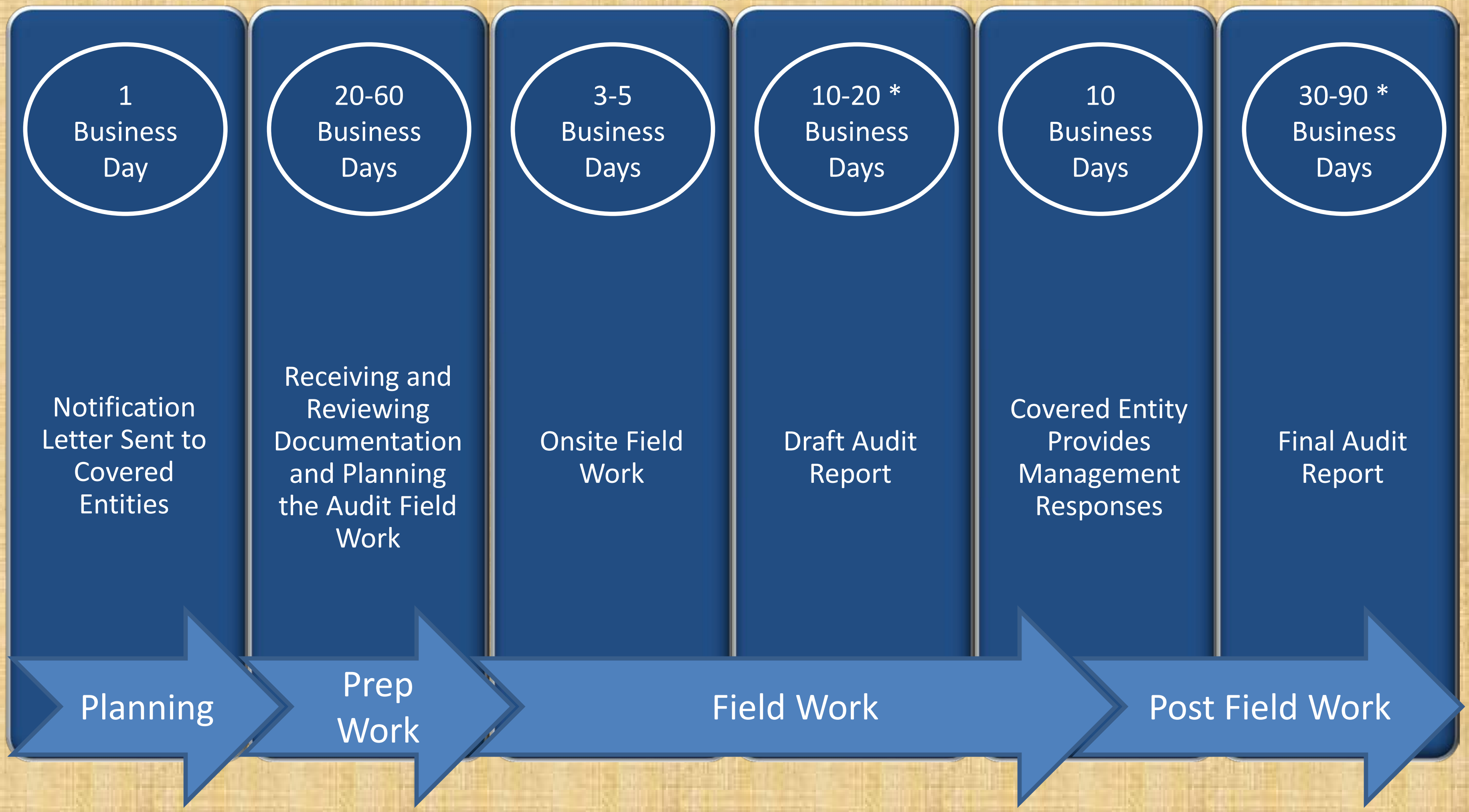
- Small Providers (10 to 50 Provider Practices, Community or rural pharmacy)
- Little to no use of HIT – almost exclusively paper based workflows
- Revenues less than $50 million

Auditees by Type & Size

	Level 1	Level 2	Level 3	Level 4	Total
Health Plans	13	12	11	11	**47**
Health Care Providers	11	16	10	24	**61**
Health Care Clearinghouses	2	3	1	1	**7**
Total	**26**	**31**	**22**	**36**	**115**

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

Audit Timeline



1 Business Day	20-60 Business Days	3-5 Business Days	10-20 * Business Days	10 Business Days	30-90 * Business Days
Notification Letter Sent to Covered Entities	Receiving and Reviewing Documentation and Planning the Audit Field Work	Onsite Field Work	Draft Audit Report	Covered Entity Provides Management Responses	Final Audit Report

* Duration varies based on several factors such as, the volume and complexity of findings noted

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

Audit Protocol—11 Modules

Breach Notification

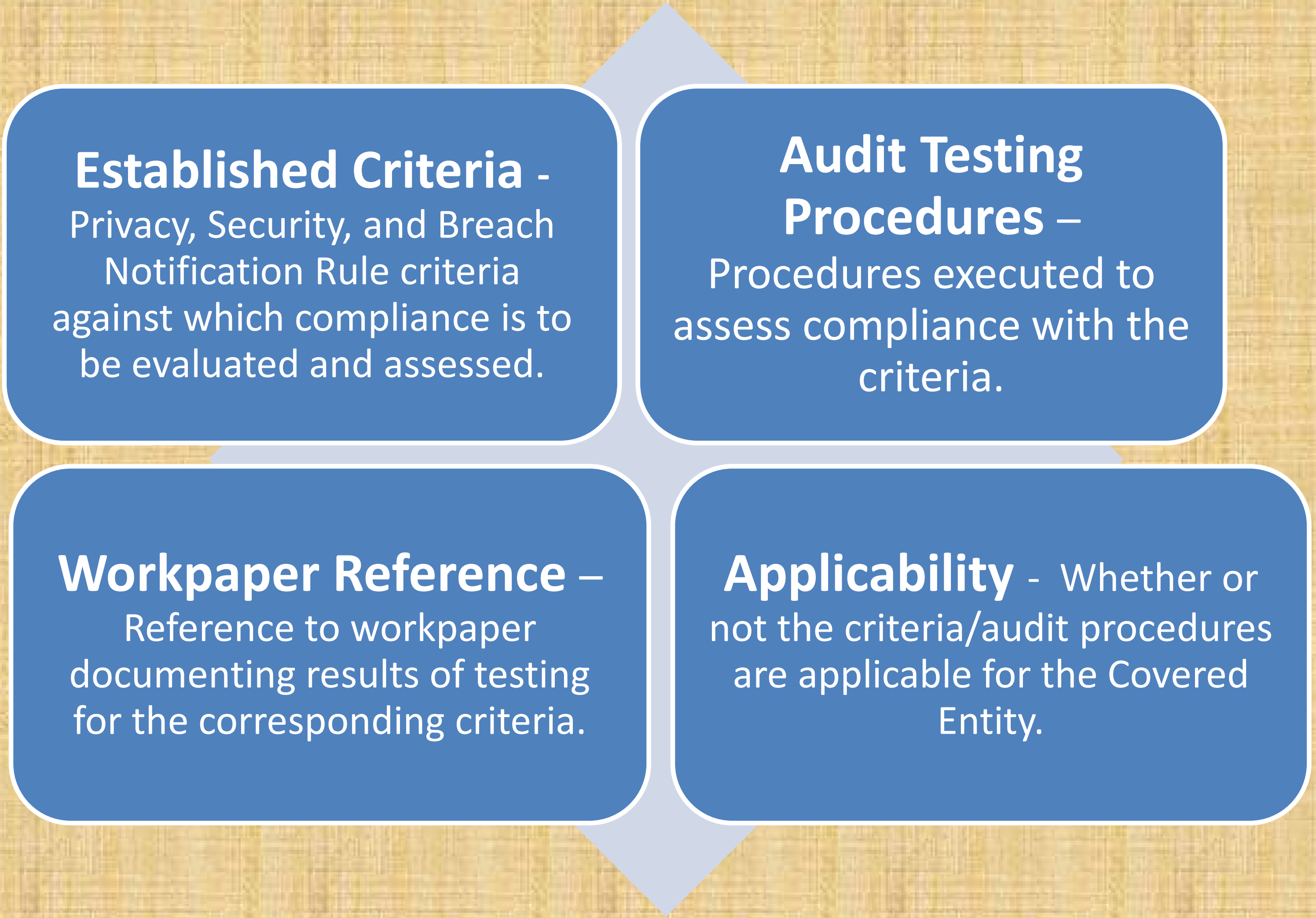
Security

- 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

Audit Protocol Components



Established Criteria - Privacy, Security, and Breach Notification Rule criteria against which compliance is to be evaluated and assessed.

Audit Testing Procedures – Procedures executed to assess compliance with the criteria.

Workpaper Reference – Reference to workpaper documenting results of testing for the corresponding criteria.

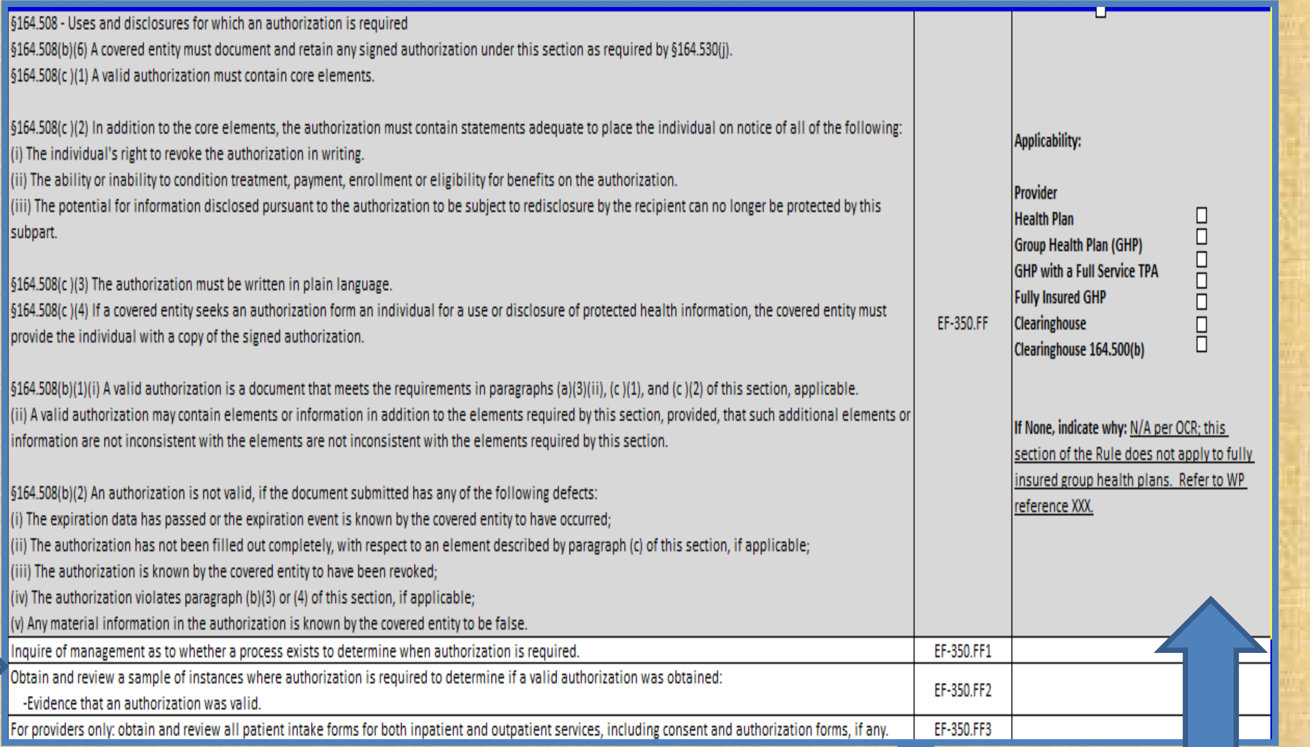
Applicability - Whether or not the criteria/audit procedures are applicable for the Covered Entity.

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

Protocol Example - Authorizations

The following slides walk through the protocol for § 164.508 – Uses & Disclosures. Process is repeated for each applicable section of the rule, listed in Appendices A & B.

1) Criteria



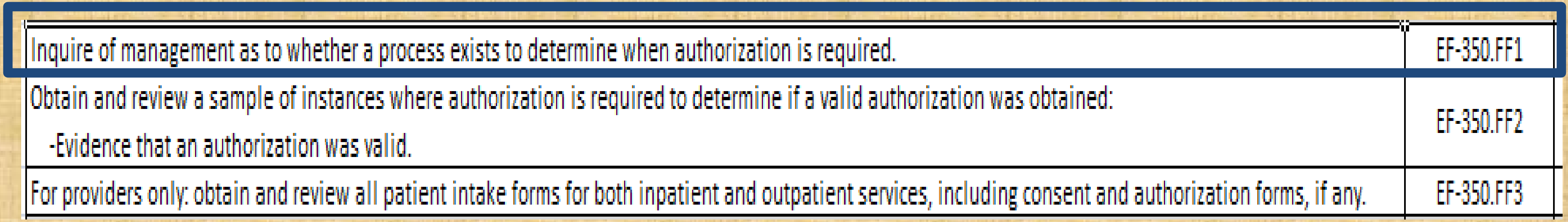
§164.508 - Uses and disclosures for which an authorization is required §164.508(b)(6) A covered entity must document and retain any signed authorization under this section as required by §164.530(j). §164.508(c)(1) A valid authorization must contain core elements. §164.508(c)(2) In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following: (i) The individual's right to revoke the authorization in writing. (ii) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization. (iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient can no longer be protected by this subpart. §164.508(c)(3) The authorization must be written in plain language. §164.508(c)(4) If a covered entity seeks an authorization form an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization. §164.508(b)(1)(i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (c)(1), and (c)(2) of this section, applicable. (ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided, that such additional elements or information are not inconsistent with the elements are not inconsistent with the elements required by this section. §164.508(b)(2) An authorization is not valid, if the document submitted has any of the following defects: (i) The expiration data has passed or the expiration event is known by the covered entity to have occurred; (ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable; (iii) The authorization is known by the covered entity to have been revoked; (iv) The authorization violates paragraph (b)(3) or (4) of this section, if applicable; (v) Any material information in the authorization is known by the covered entity to be false.	EF-350.FF	**Applicability:** **Provider** **Health Plan** □ **Group Health Plan (GHP)** □ **GHP with a Full Service TPA** □ **Fully Insured GHP** □ **Clearinghouse** □ **Clearinghouse 164.500(b)** □ **If None, indicate why:** N/A per OCR; this section of the Rule does not apply to fully insured group health plans. Refer to WP reference XXX.
Inquire of management as to whether a process exists to determine when authorization is required.	EF-350.FF1	
Obtain and review a sample of instances where authorization is required to determine if a valid authorization was obtained: -Evidence that an authorization was valid.	EF-350.FF2	
For providers only: obtain and review all patient intake forms for both inpatient and outpatient services, including consent and authorization forms, if any.	EF-350.FF3	

2) Audit Testing Procedures

3) W/P Ref.

4) Applicability

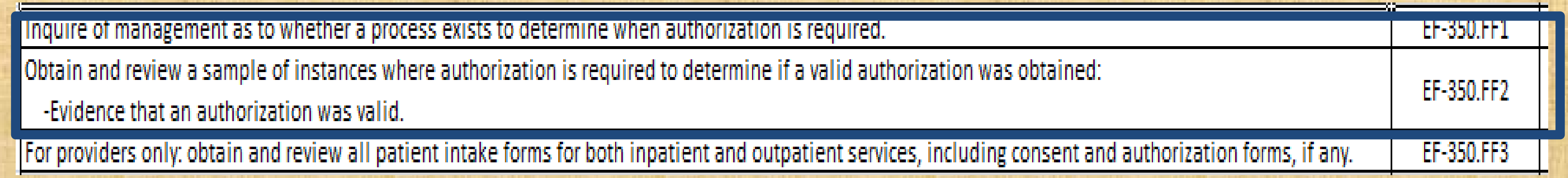
Audit Testing Procedure - Inquiry



Inquire of management as to whether a process exists to determine when authorization is required.	EF-350.FF1
Obtain and review a sample of instances where authorization is required to determine if a valid authorization was obtained: -Evidence that an authorization was valid.	EF-350.FF2
For providers only: obtain and review all patient intake forms for both inpatient and outpatient services, including consent and authorization forms, if any.	EF-350.FF3

- The audit team would execute this audit step through an interview with, for example, the Privacy Officer:
  - Inquire of management as to whether a process exists to determine when authorization is required.

Audit Testing Procedure - Review



Inquire of management as to whether a process exists to determine when authorization is required.	EF-350.FF1
Obtain and review a sample of instances where authorization is required to determine if a valid authorization was obtained: -Evidence that an authorization was valid.	EF-350.FF2
For providers only: obtain and review all patient intake forms for both inpatient and outpatient services, including consent and authorization forms, if any.	EF-350.FF3

- The audit team would execute this audit step through review of documentation:
  - Obtain and review a sample of instances where authorization is required to determine if a valid authorization is obtained:
    - Evidence that an authorization was valid.

Potholes along the way

Entity verification

- Old addresses, no contacts
- CE’s that aren’t
- Nonresponsive

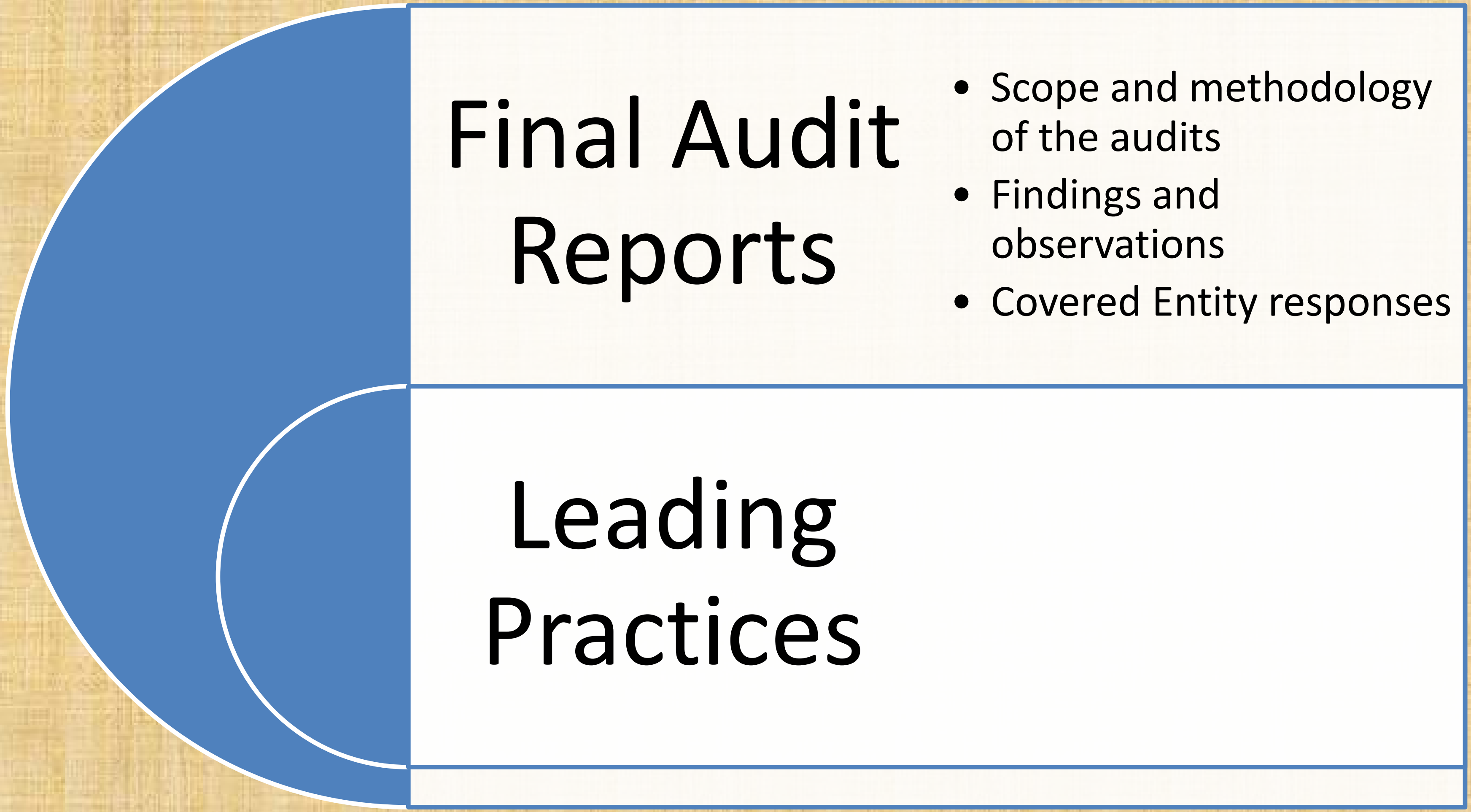
Documents for review

- Newly minted and not trained on (i.e., not implemented)

Interaction and representation to KPMG

- Intentional misrepresentation
- Disavowing staff statements
- GAGAS standards for trusted sources

Program Deliverables



Final Audit Reports

- Scope and methodology of the audits
- Findings and observations
- Covered Entity responses

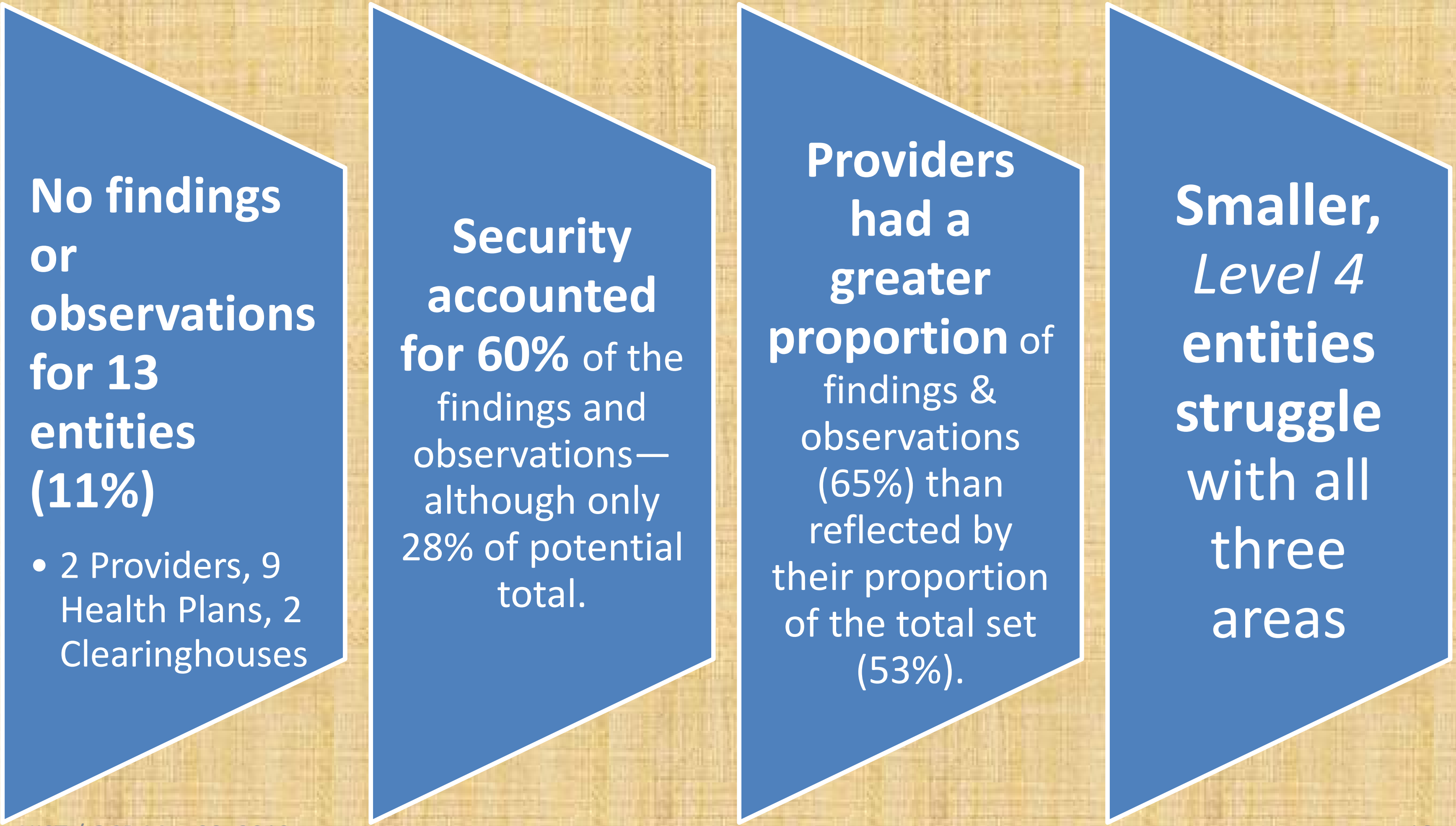
Leading Practices

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

Exceptions Affect Audit Scope

- What did we audit? Varied by type of entity.
- Exceptions to certain requirements applied to several audited entities
  - 6 of the 7 clearinghouses asserted they only act as a business associate to other covered entities; in accordance with §164.500(b) few privacy procedures applied
  - 8 of the 47 heath plans asserted they were fully insured group health plans, so only one privacy procedure applied.
  - 2 of the 61 providers and 4 of the 47 health plans asserted they do not create, receive or retain electronic Protected Health Information (ePHI), so security protocol was not executed.

Overall Findings & Observations



No findings or observations for 13 entities (11%)

- 2 Providers, 9 Health Plans, 2 Clearinghouses

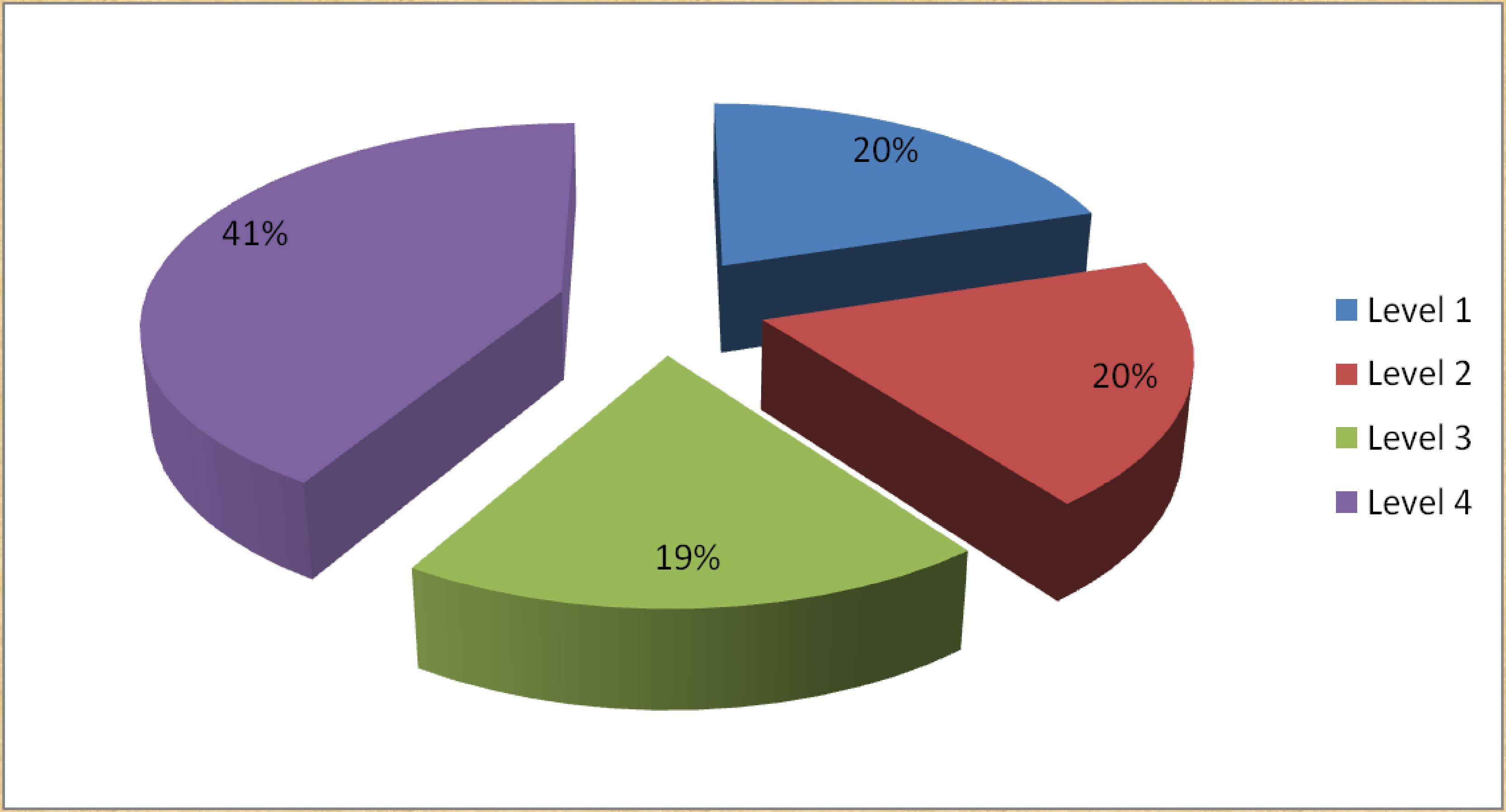
Security accounted for 60% of the findings and observations—although only 28% of potential total.

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

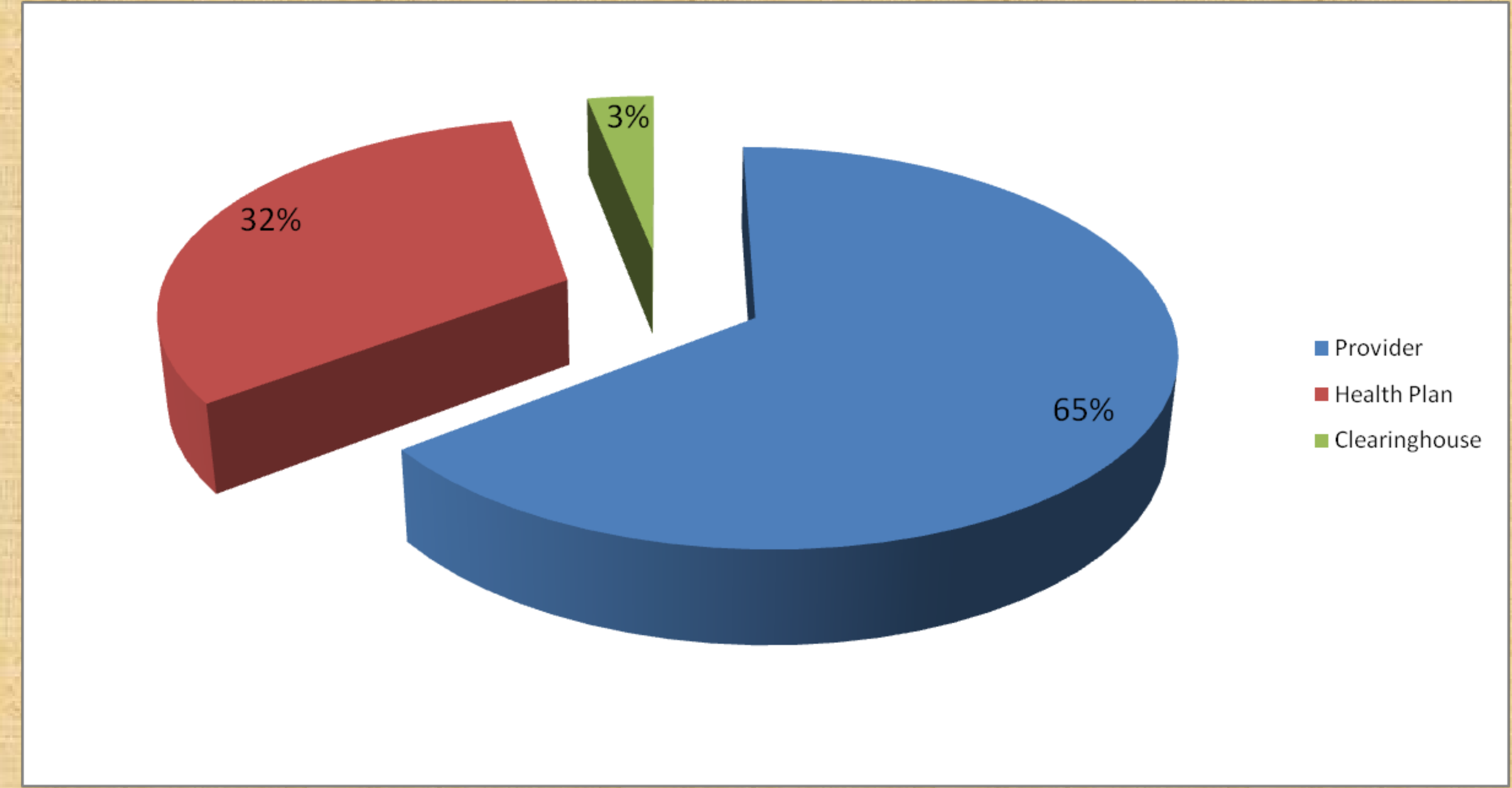
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Audit Findings & Observations By Level



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

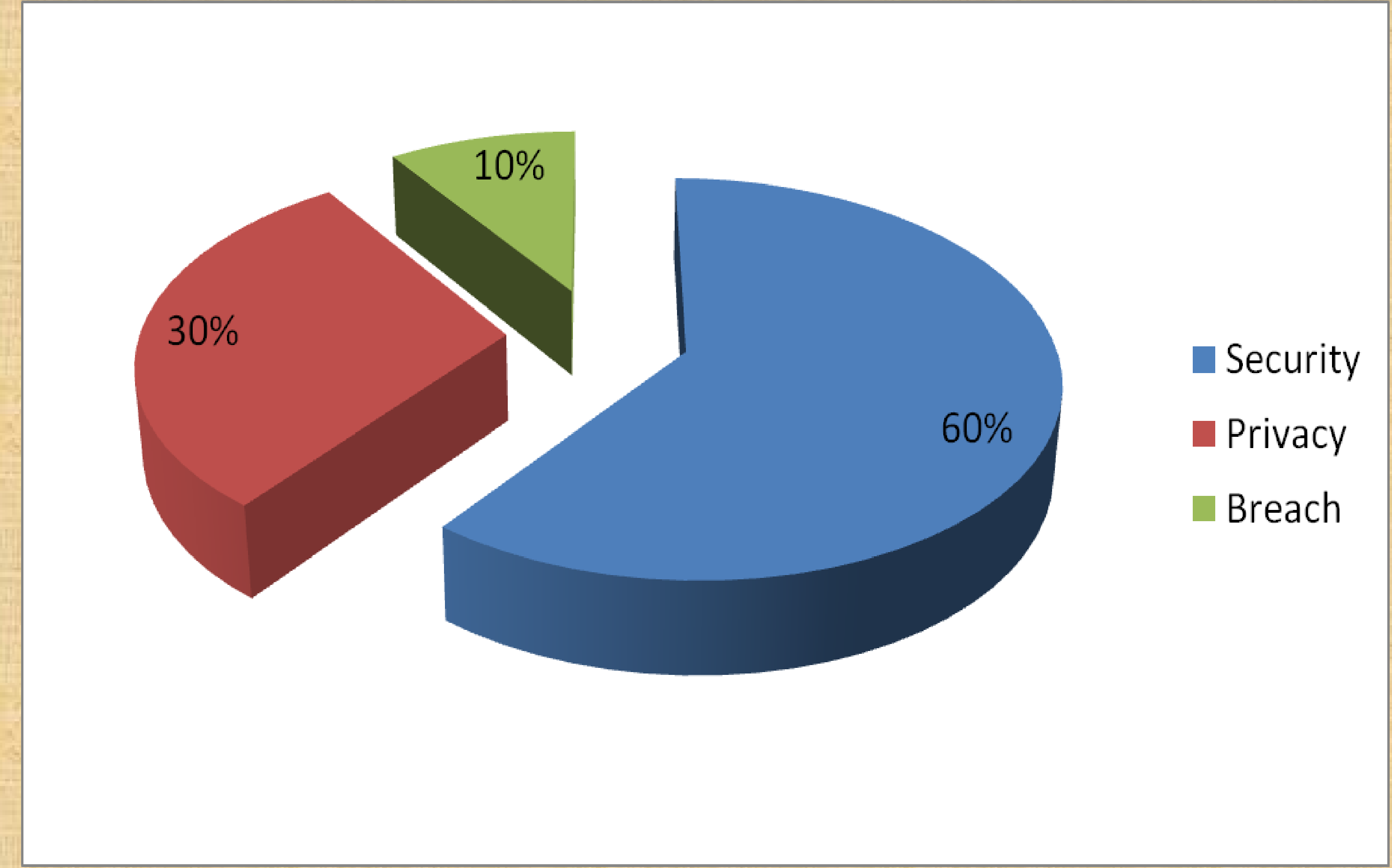
Proportional by Entity Type



AUDIT FINDINGS AND OBSERVATIONS BY TYPE OF COVERED ENTITY

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

Proportional Findings by Rule

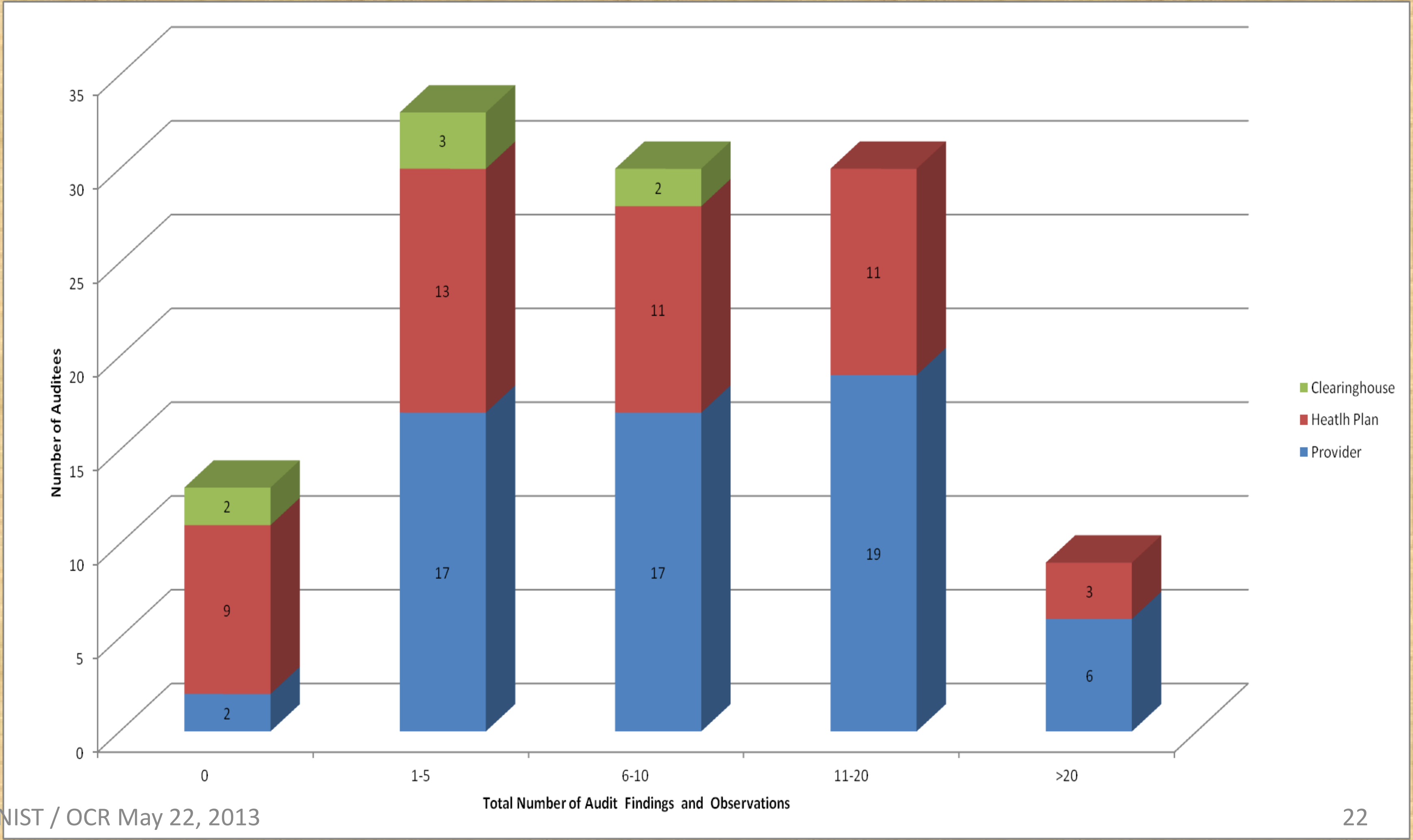


Audit Findings and Observations by Rule

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

Element Exposure by Entity Type

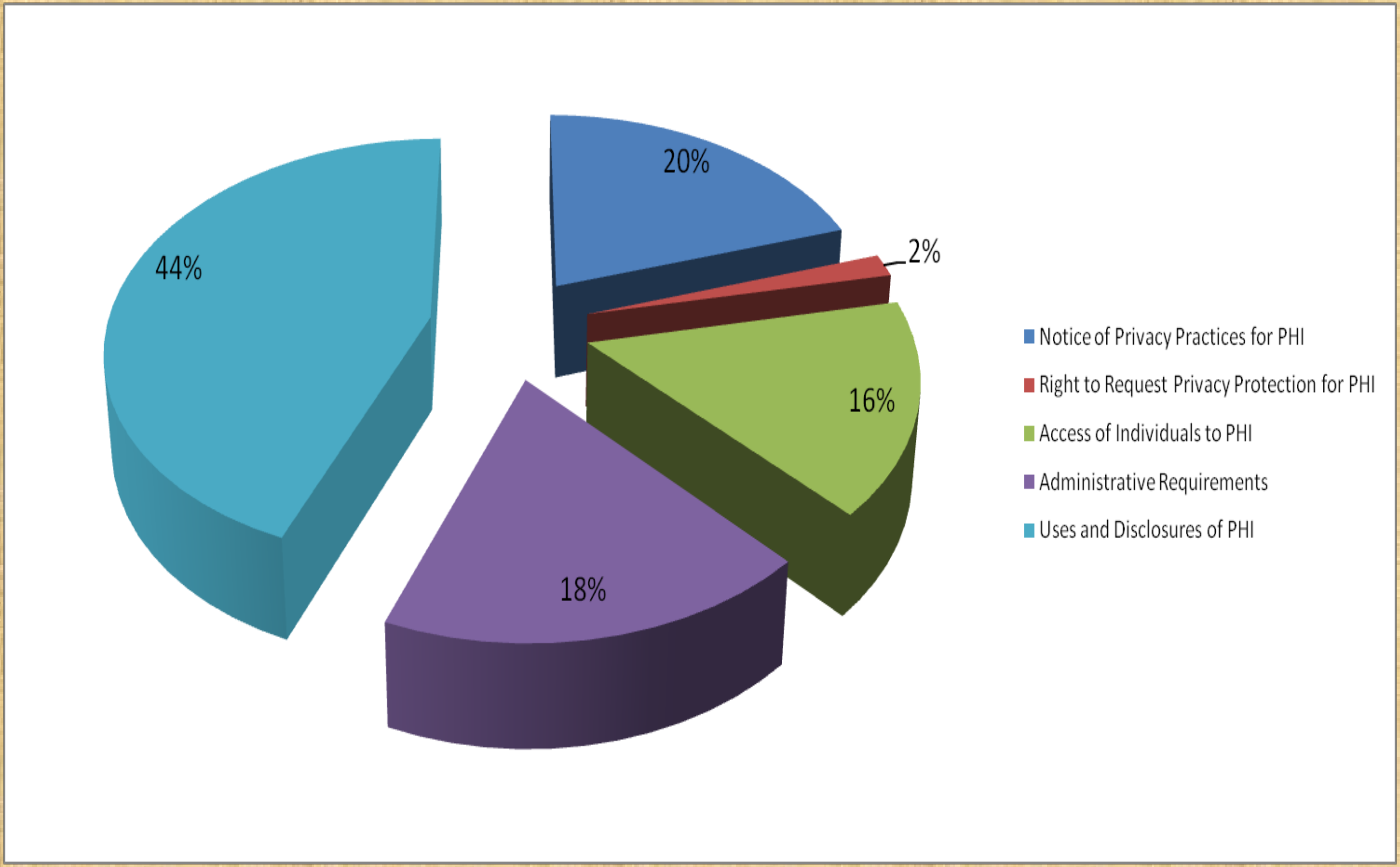
Audit Findings and Observations Distribution



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

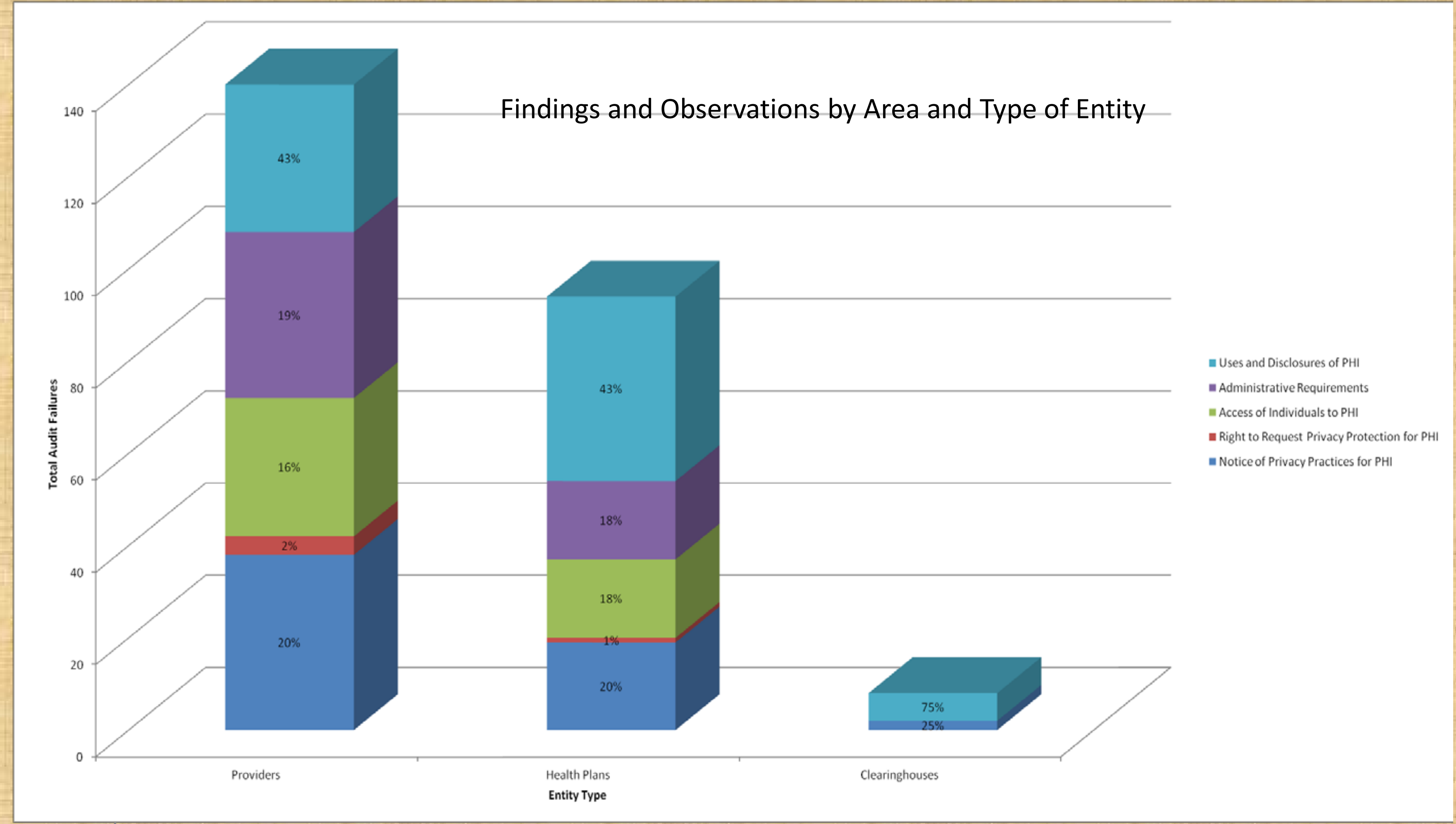
Privacy Findings & Observations

PERCENTAGE OF FINDINGS AND OBSERVATIONS BY AREA OF FOCUS



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

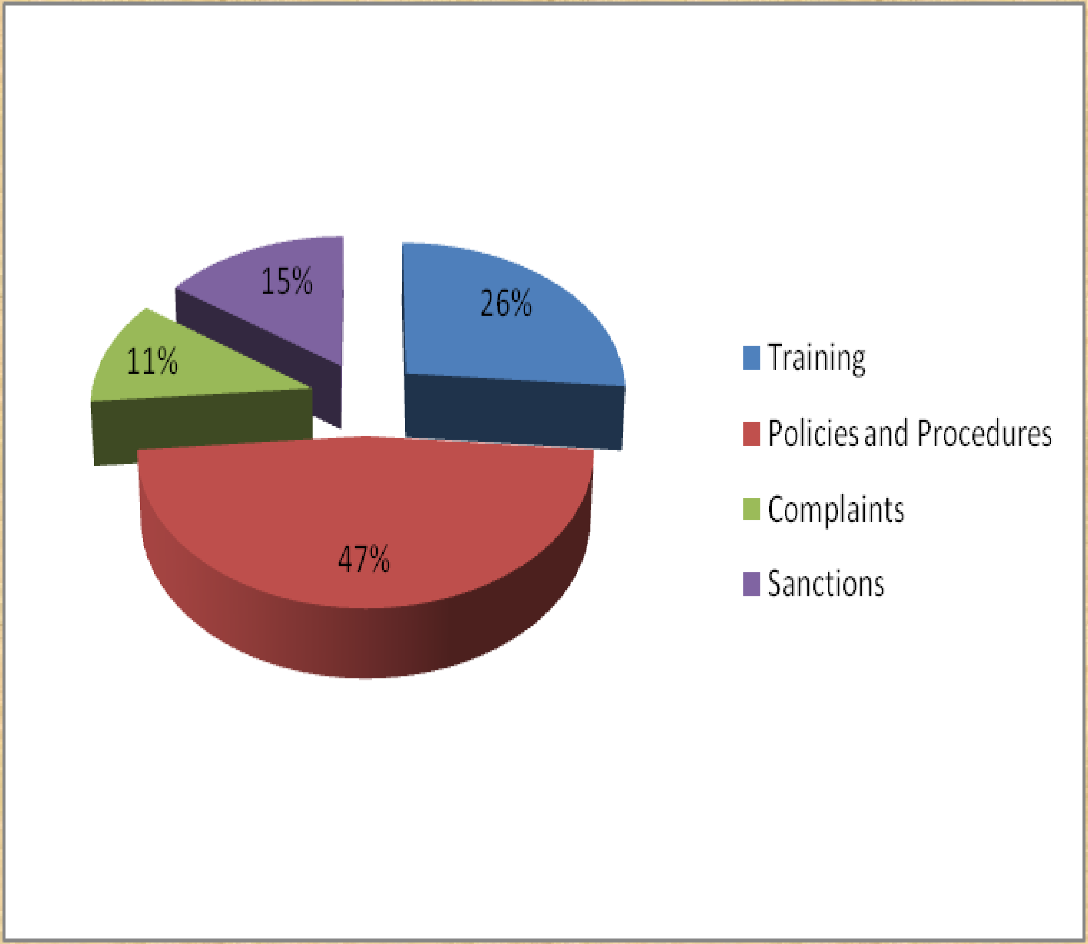
Privacy Results by Entity Type



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

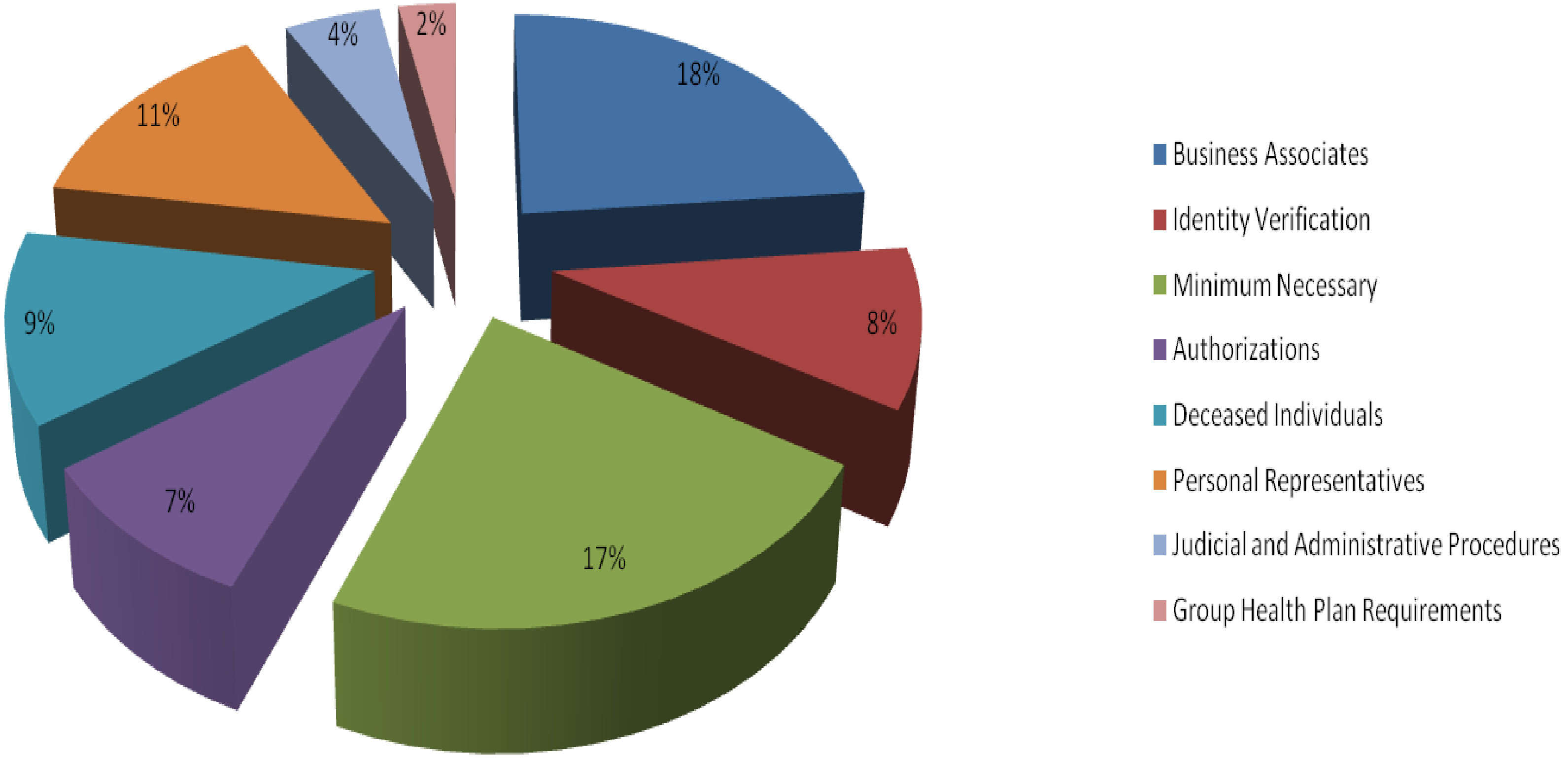
Privacy Administrative Elements

ADMINISTRATIVE REQUIREMENTS FINDINGS AND OBSERVATIONS



Privacy -- Uses and Disclosures

Uses and Disclosures of PHI Findings and Observations



Security Results

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

No complete & accurate risk assessment in two thirds of entities

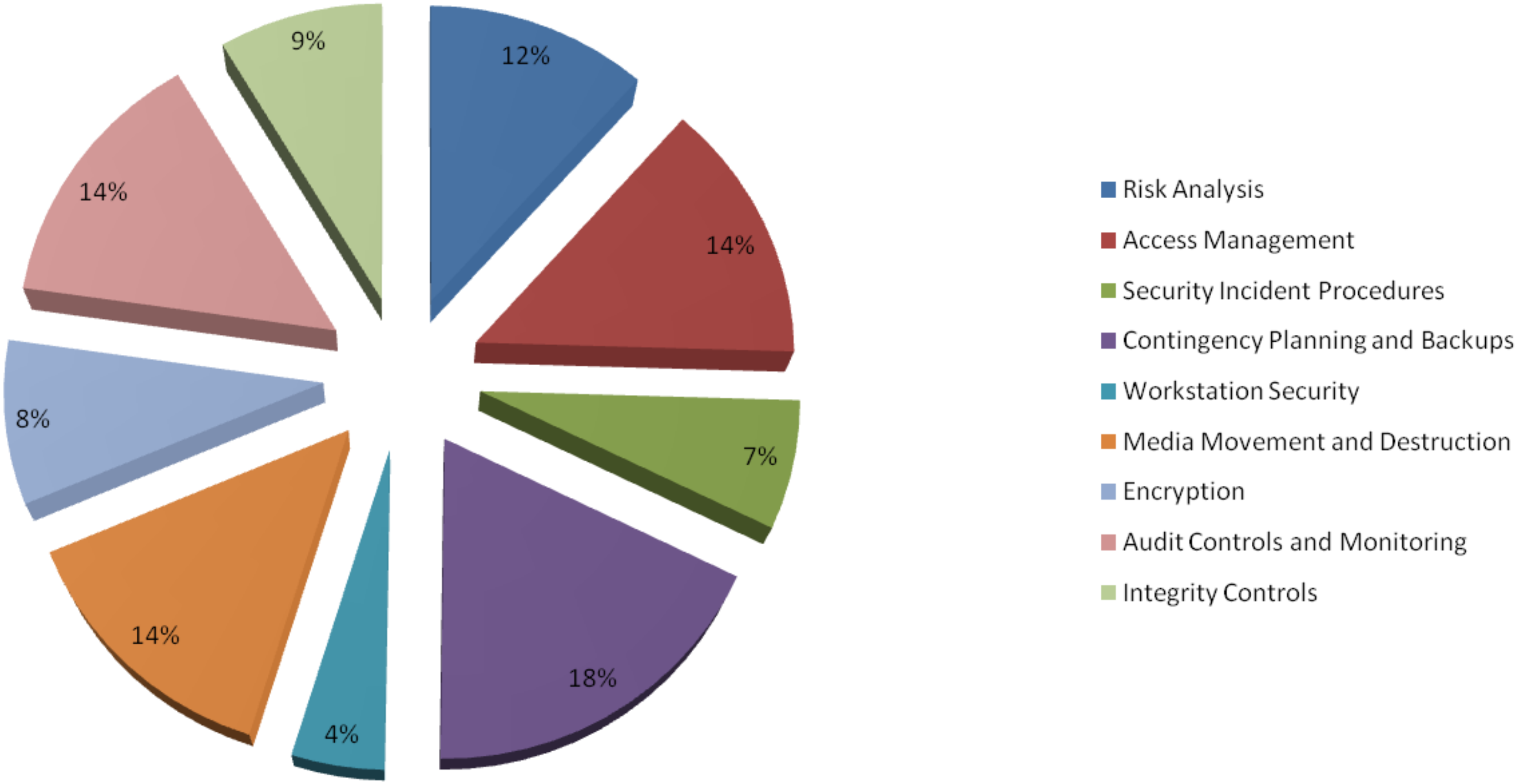
- 47 of 59 providers,
- 20 out of 35 health plans and
- 2 out of 7 clearinghouses

Security addressable implementation specifications: Almost every entity had a finding or observation that could be met by fully implementing the addressable specification.

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

Security Elements

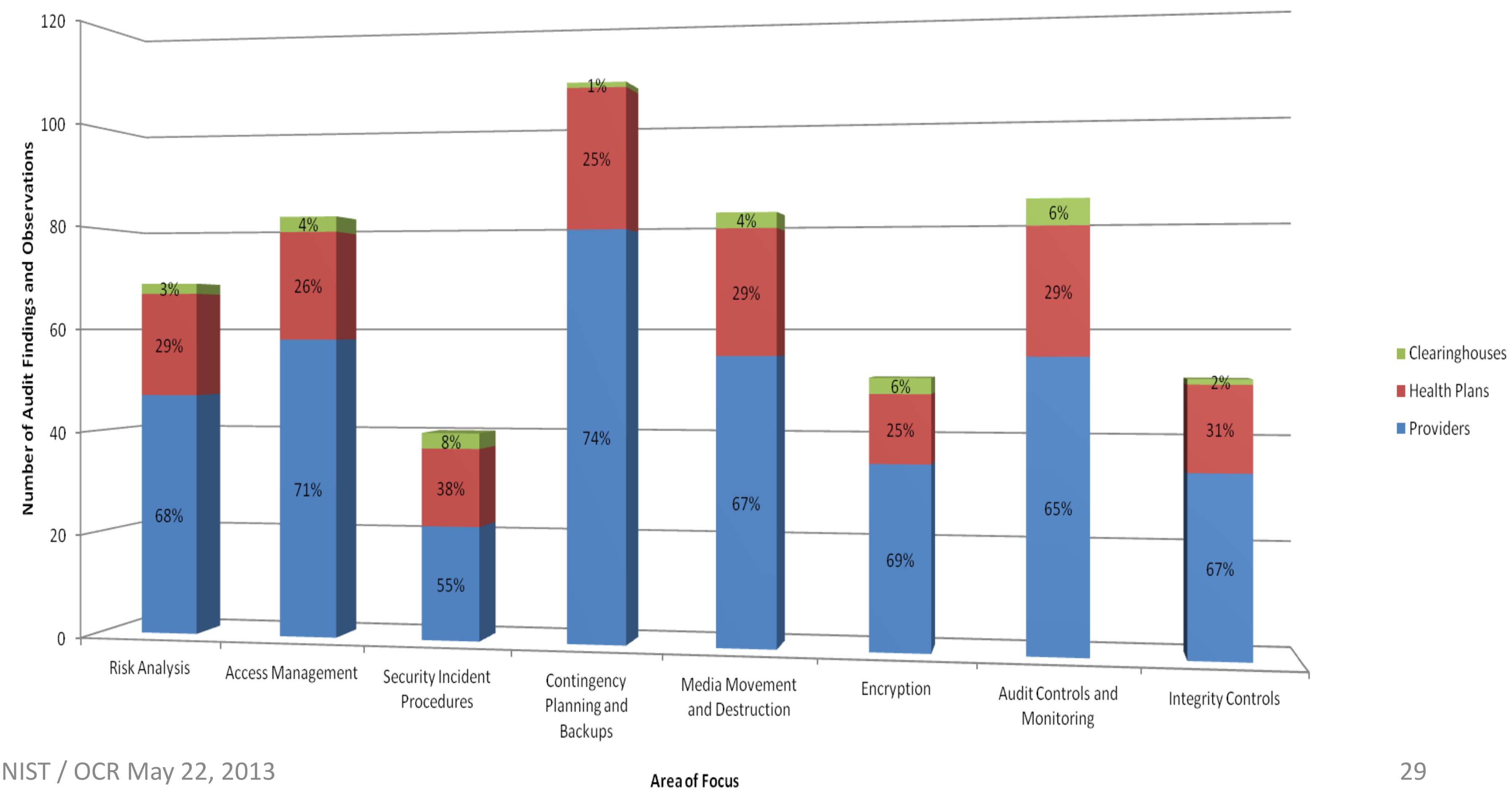
Percentage of Audit Findings and Observations by Area of Focus



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

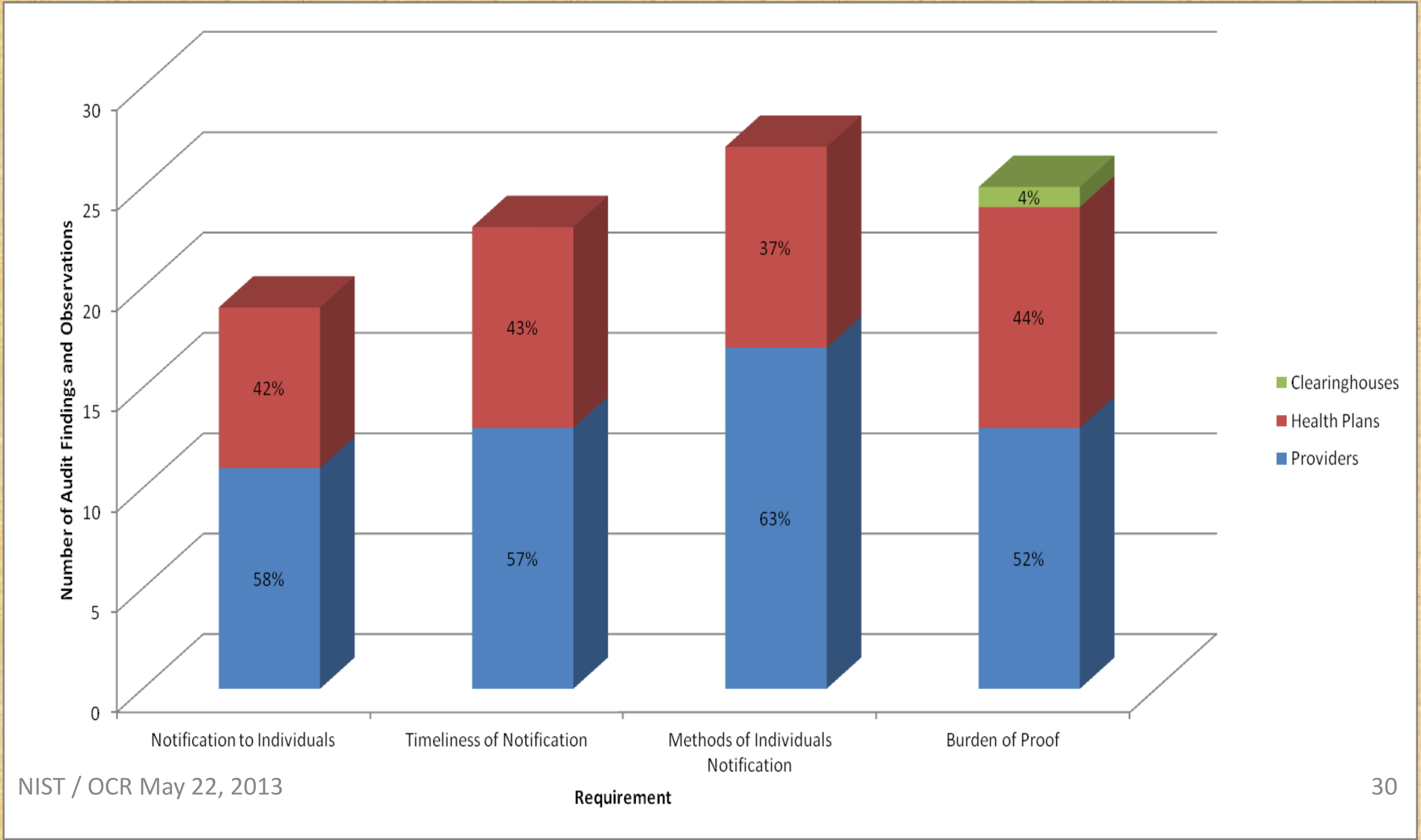
Security by Entity Type

Total Audit Findings and Observations by Area of Focus and Entity Type



Breach Notification by Entity Type

Audit Findings and Observations by Requirement
and Type of Entity



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

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

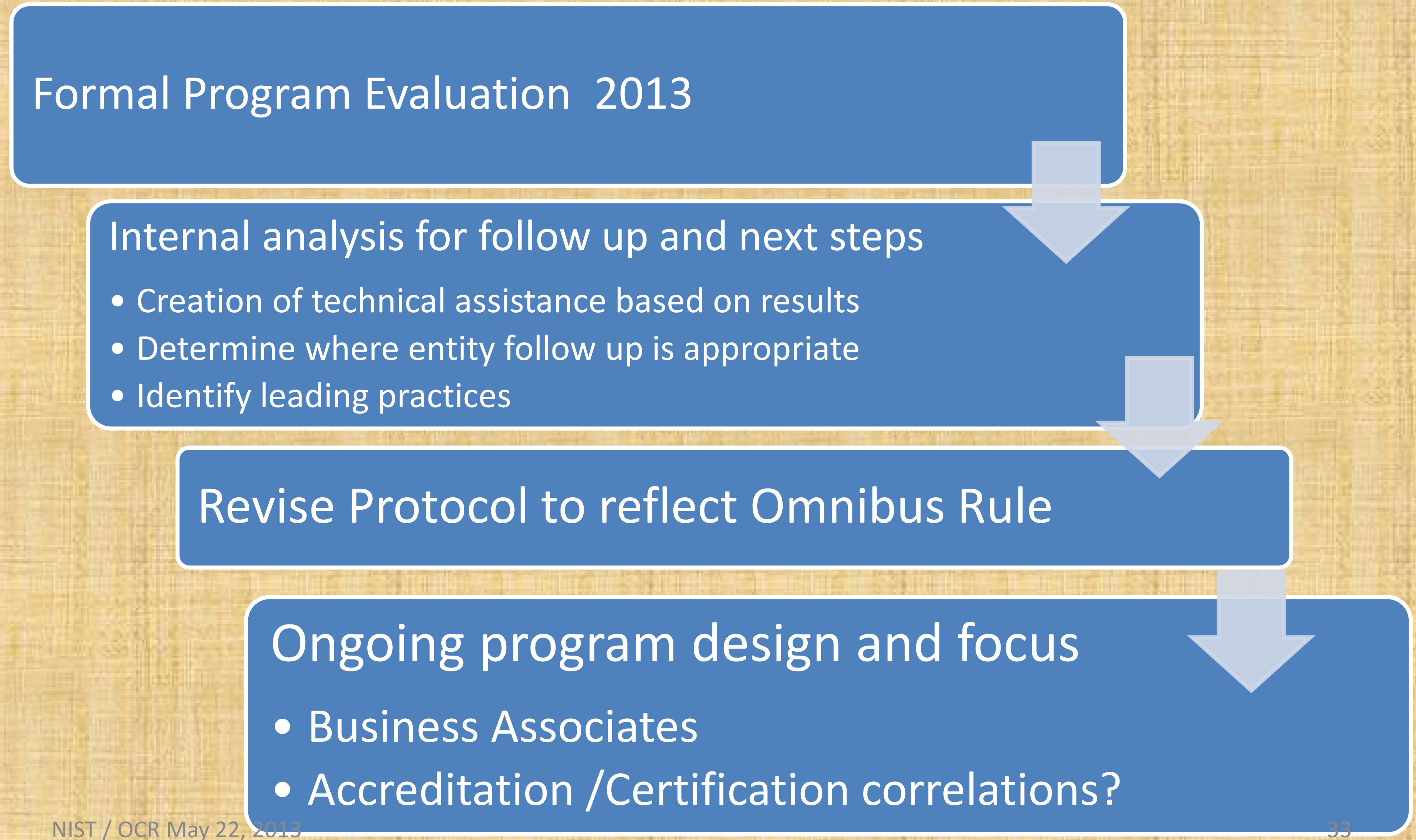
- Notice of Privacy Practices;
- Access of Individuals;
- Minimum Necessary; and,
- Authorizations.

Security

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

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

Next Steps for OCR



Formal Program Evaluation 2013

Internal analysis for follow up and next steps

- Creation of technical assistance based on results
- Determine where entity follow up is appropriate
- Identify leading practices

Revise Protocol to reflect Omnibus Rule

Ongoing program design and focus

- Business Associates
- Accreditation /Certification correlations?

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

New Provider 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.

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

Want More Information?

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

OCR offers a wide range of helpful 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/