United States Department of Health & Human Services

Office of the Secretary

Office for Civil Rights (OCR)

2012 HIPAA Privacy and Security Audits

Linda Sanches
OCR Senior Advisor, Health Information Privacy
Lead, HIPAA Compliance Audits

Agenda

- Background
- Structure
- Audit Subject Selection
- Process & Timeline
- Initial 20 Auditees

HITECH Act Impact

HITECH Act (of American Recovery and Reinvestment Act) of 2009

- Establishes breach notification requirements
- Establishes New Penalty Levels
- Establishes compliance requirements for business associates
- Extended Enforcement authority to State Attorneys General
- Mandates performance of privacy and security audits

Background

- The American Recovery and Reinvestment Act of 2009, in Section 13411 of the HITECH Act, 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
- To implement this mandate, OCR is piloting a program to perform up to 115 audits of covered entities to assess HIPAA privacy, security and breach notification performance
- Audits are conducted in two phases – initial audits to test the newly developed protocol and final pilot audits through December 2012

Program Objective

- Audits present a new opportunity to:
  - 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

Program Goal

To improve covered entity and business associate compliance with the HIPAA standards.

- Widely publicizing audit program & audit results will spur covered entities, business associates to assess and calibrate their privacy and security protections.

- OCR will 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.

Audit Plan

Description	Vendor	Status/ Timeframe
Audit program development study	Booz Allen Hamilton	Closed 2010
Covered entity & business associate identification and catalog	Booz Allen Hamilton	Closed 2012
Develop audit protocol and conduct audit	KPMG, Inc.	Open 2011-2012
Evaluation of audit program	TBD	To Be Awarded - Conclude in 2013

Protocol Design & Program Performance Contract

- Goal: investigate and assess whether a CE is in compliance with Rules
- Develop in accordance with GAO auditing standards
- Protocol—comprehensive, modules to permit targeting of issues and entity types—designed for future use by OCR or others
- Provide assessment of policies, practices, operations and infrastructure

Who Will be Audited?

- Every covered entity is eligible for an audit
- For 2011-2012, OCR seeks to audit as wide a range of types and sizes of covered entities as possible which includes:
  - Health plans of all types
  - Health care clearinghouses
  - Individual and organizational providers
- Business Associates in later audit wave

Auditee Selection Criteria

- OCR identified a pool of covered entities
- Specific criteria includes but is not limited to:
  - Public versus Private
  - Entity's size, e.g., level of revenues/assets, number of patients or employees, use of HIT
  - Affiliation with other health care organizations
  - Geographic location
  - Type of entity and relationship to patient care

Timeline for the Audit Program

KPMG contract into effect June 2011; now standing up the program activities. Pilot audit program a three step process.

1. Working with KPMG to develop the draft audit protocols.

   Completed November 2011

2. An initial round of audits tested the protocols. Results of field testing provided feedback for final protocol design.

   Field work completed March 1st

   Final protocol design completed April 2012

3. Rolling out the full range of audits and evaluation process.

   All audits will be completed by December, 2012.

How will the Audit Program Work?

- Entities selected for an audit will receive a notification letter from OCR and asked to provide documentation to the auditor
- Every audit will include a site visit and result in an audit report
- KPMG will recommend suggested modifications to the protocol
- KPMG will summarize findings & results, highlight consistent issues
- Final report
  - how the audit was conducted;
  - what the findings were and;
  - what actions the covered entity is taking in response to those findings.

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.

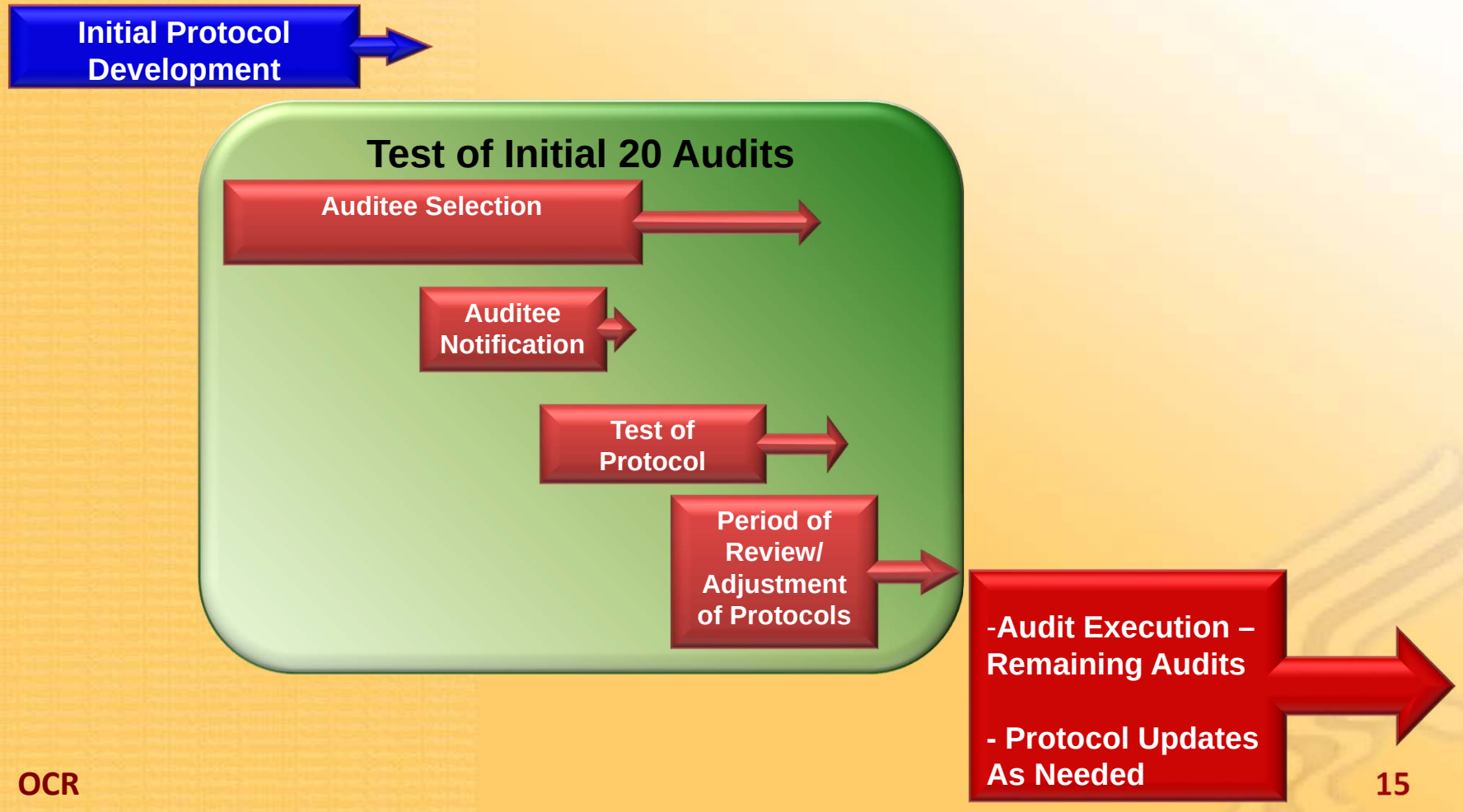
What is a Performance Audit?

- Measure performance against established criteria
- Privacy, Security and Breach, “the Rules” were made auditable and measureable by developing performance criteria to execute these audits
- Used by regulators to understand how industry is complying with a set of regulations
- Conducted under GAGAS, Generally Accepted Government Auditing Standards, aka, Yellow Book Standards
- Allow for rendering an opinion of whether entity has key controls and processes to allow entity to maintain or achieve compliance with the Rules
- Not intended to be punitive, but rather measure compliance with regulations

Overview of HIPAA Audit Project

2011 - 2012

July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May – Dec.



Breakdown of First 20 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 between $300 million and $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 between $50 Million and $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***

First 20 Auditees by Entity Type

	Level 1	Level 2	Level 3	Level 4	Total
Health Plans	2	3	1	2	8
Healthcare Providers	2	2	2	4	10
Healthcare Clearinghouses	1	1	0	0	2
Total	**5**	**6**	**3**	**6**	**20**

First 20 Plans and Providers

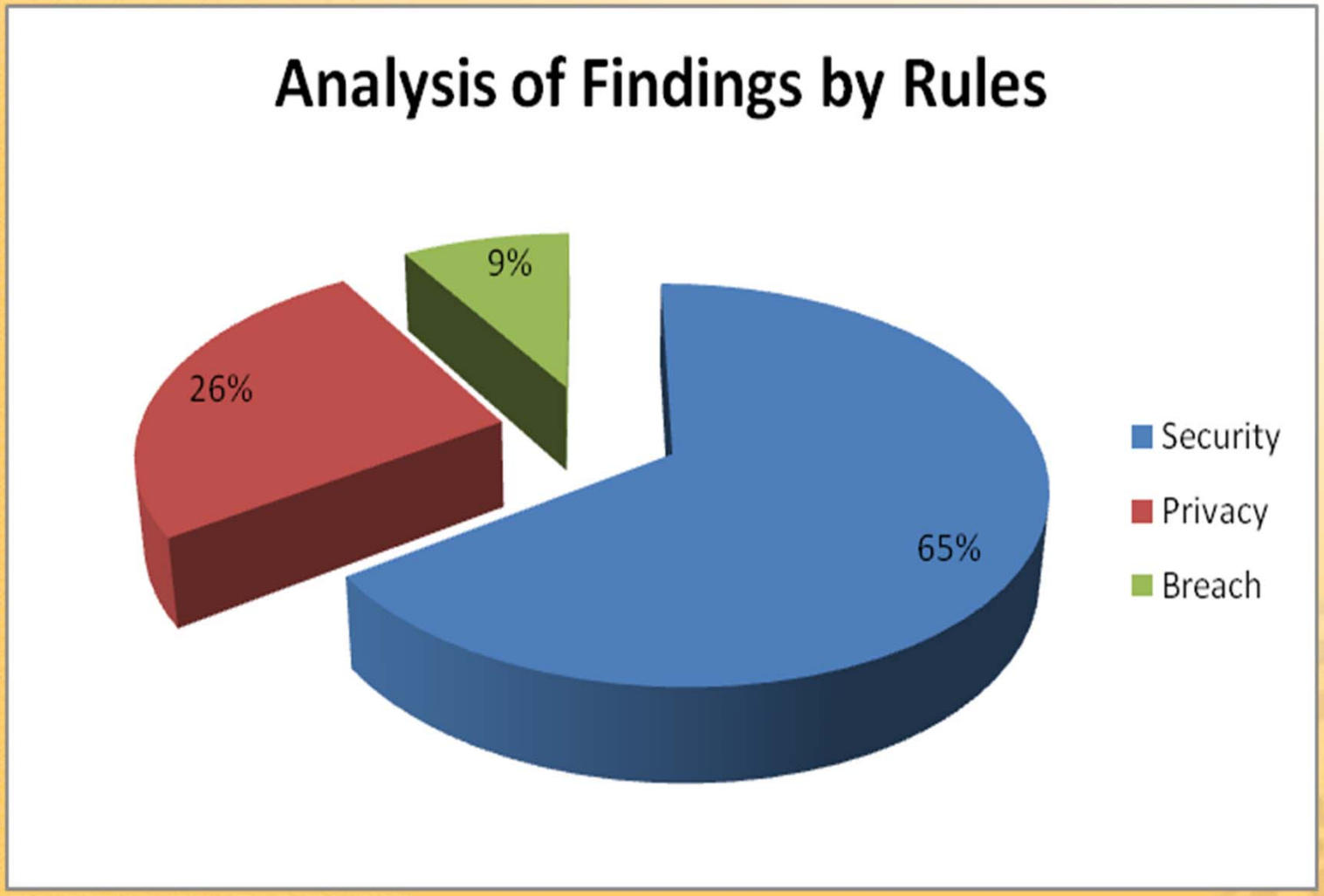
Health Plans

Medicaid	1
SCHIP	1
Group Health	3
Health Insurance Issuer	3

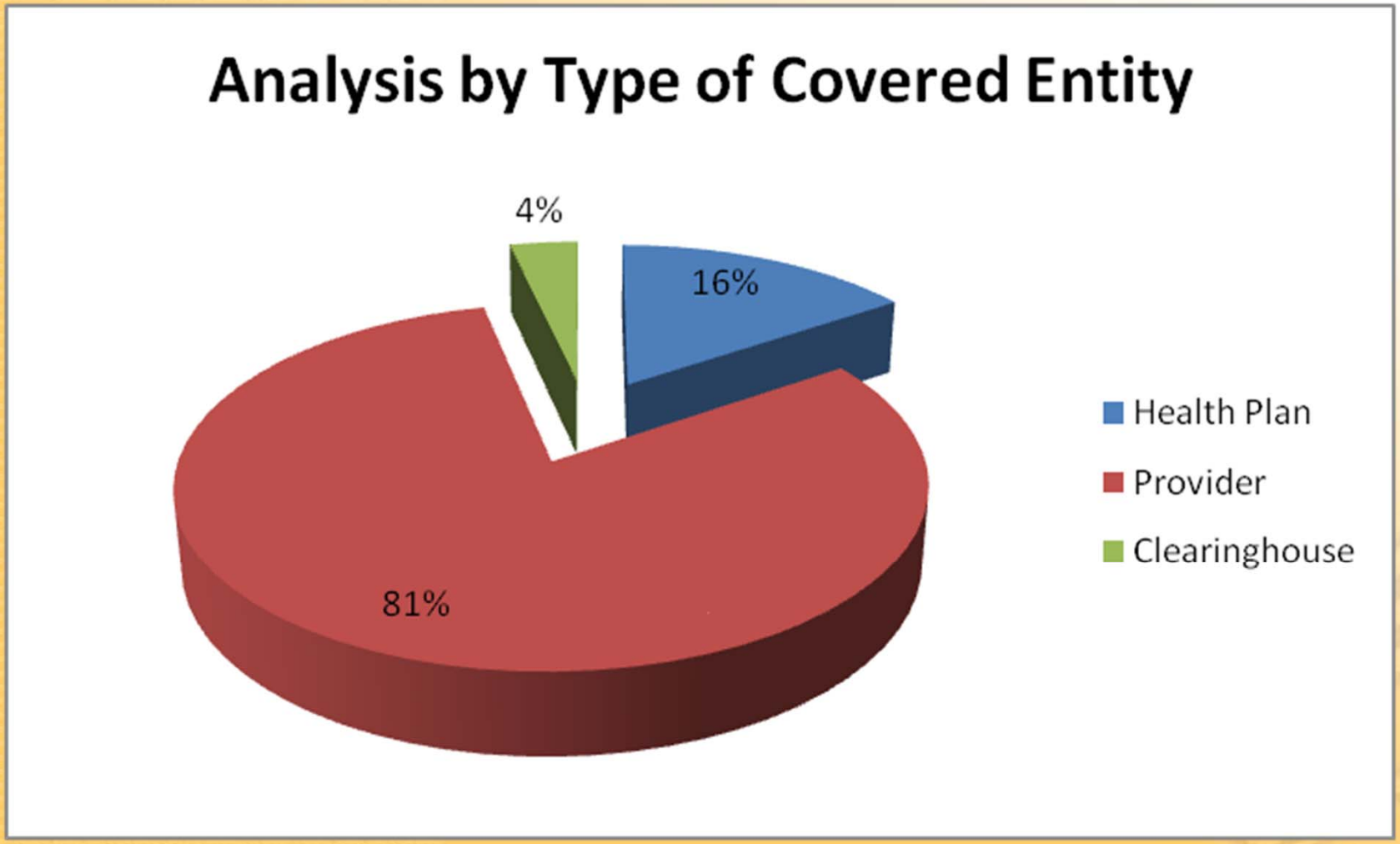
Health Care Providers

Allopathic & Osteopathic Physicians	3
Hospitals	3
Laboratories	1
Dental	1
Nursing & Custodial Care Facilities	1
Pharmacy	1

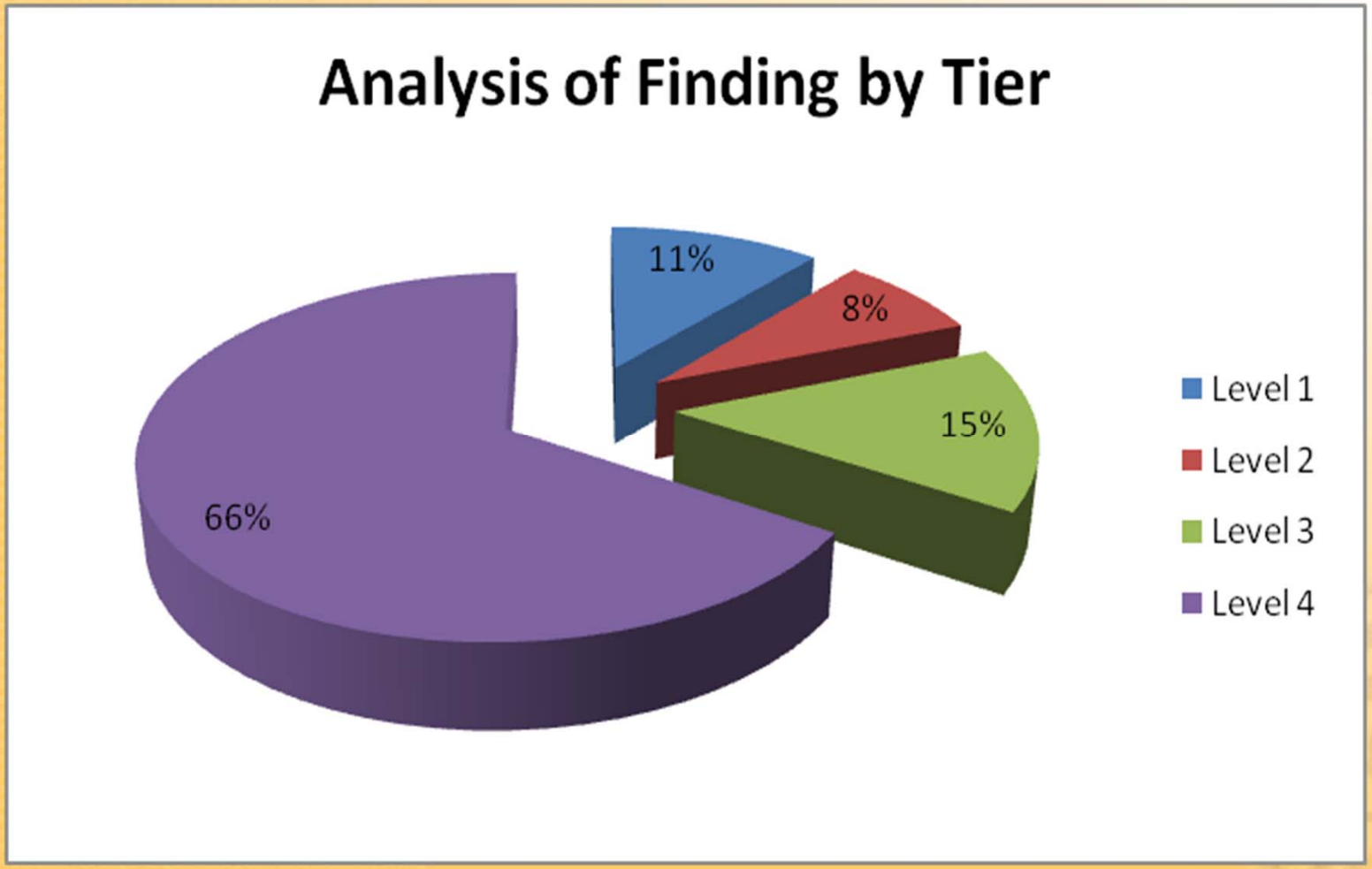
Initial 20 Findings Analysis Overview



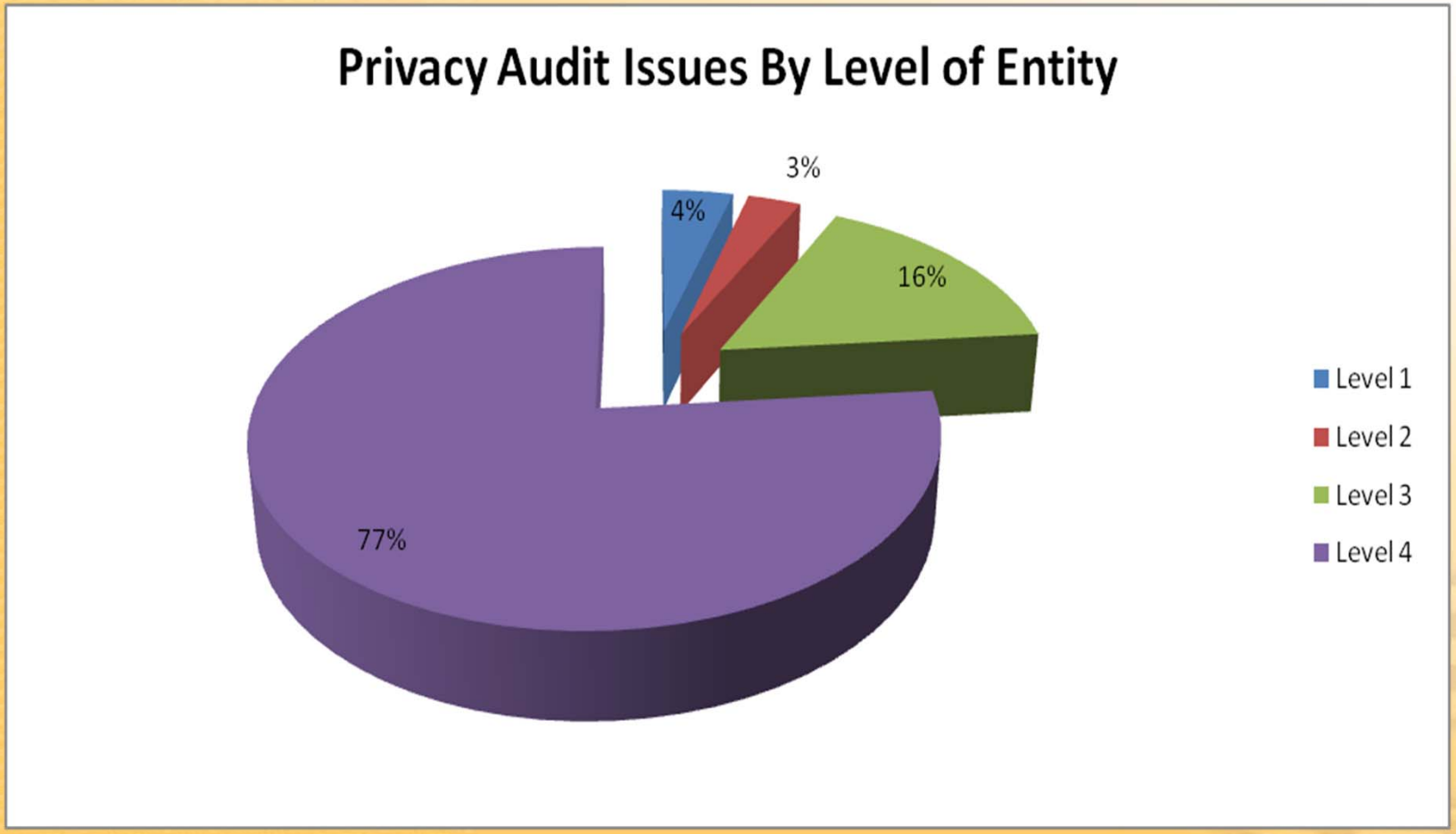
Initial 20 Findings Analysis Overview



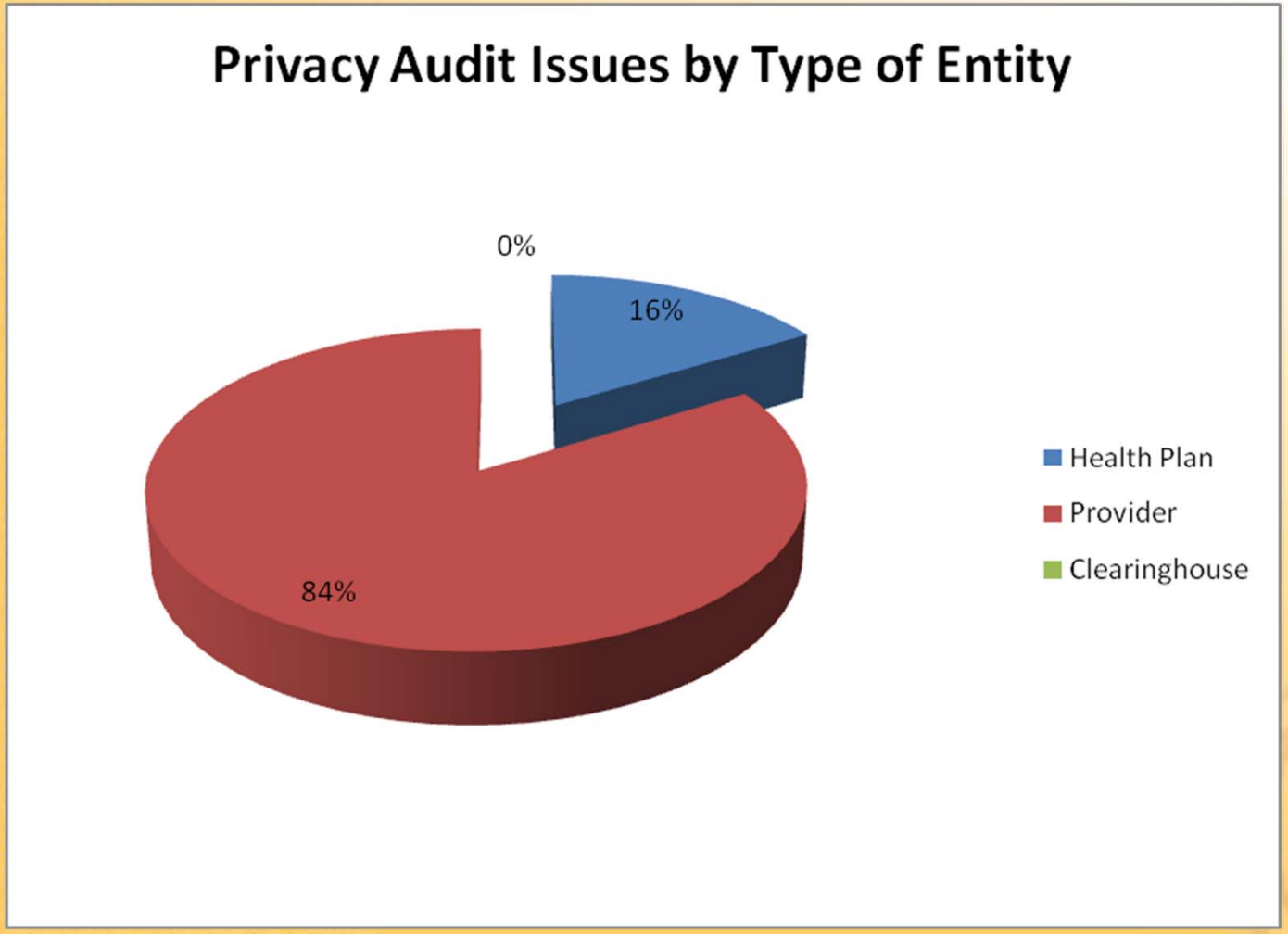
Initial 20 Findings Analysis Overview



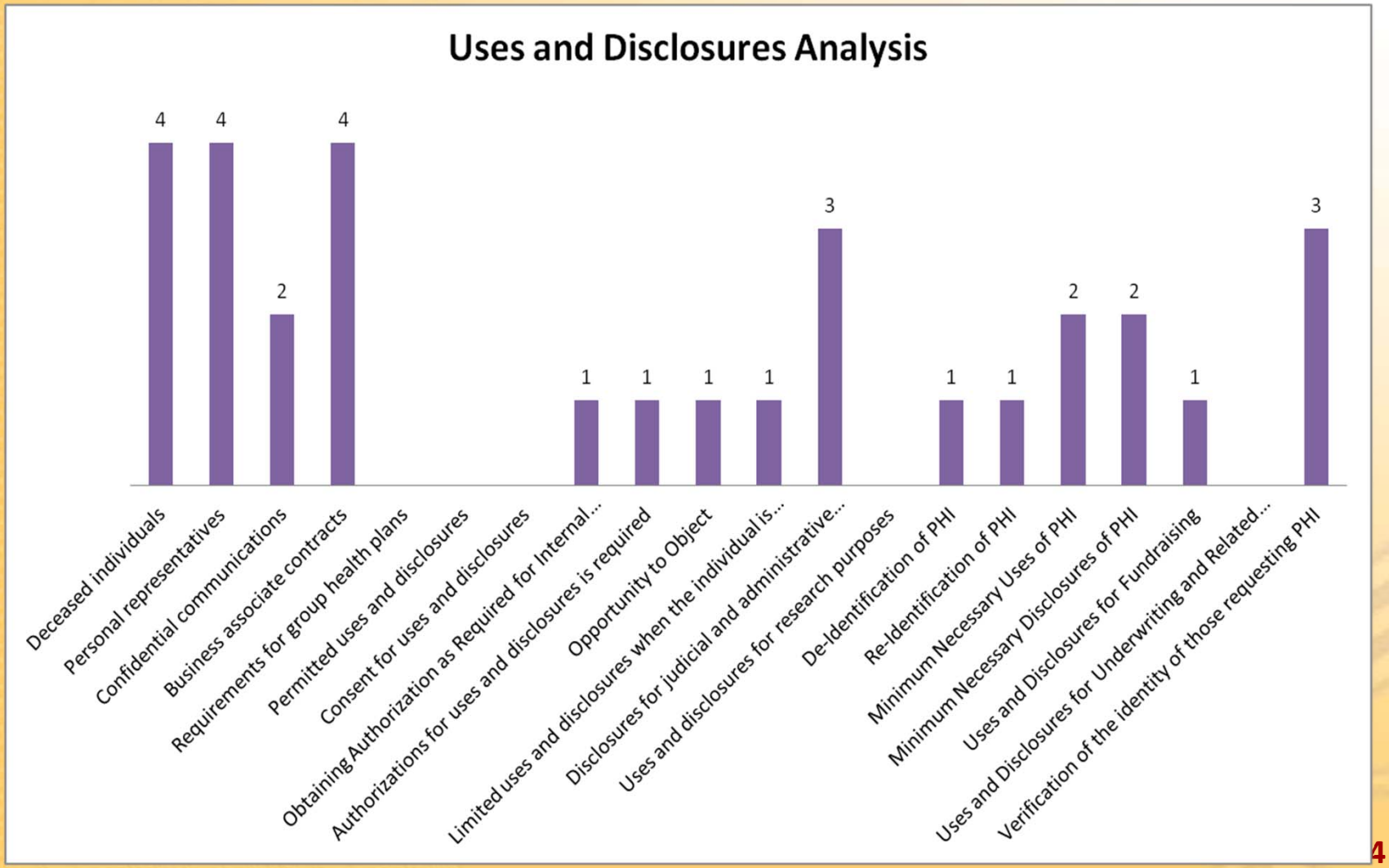
Initial 20 Findings Analysis
Privacy Issues



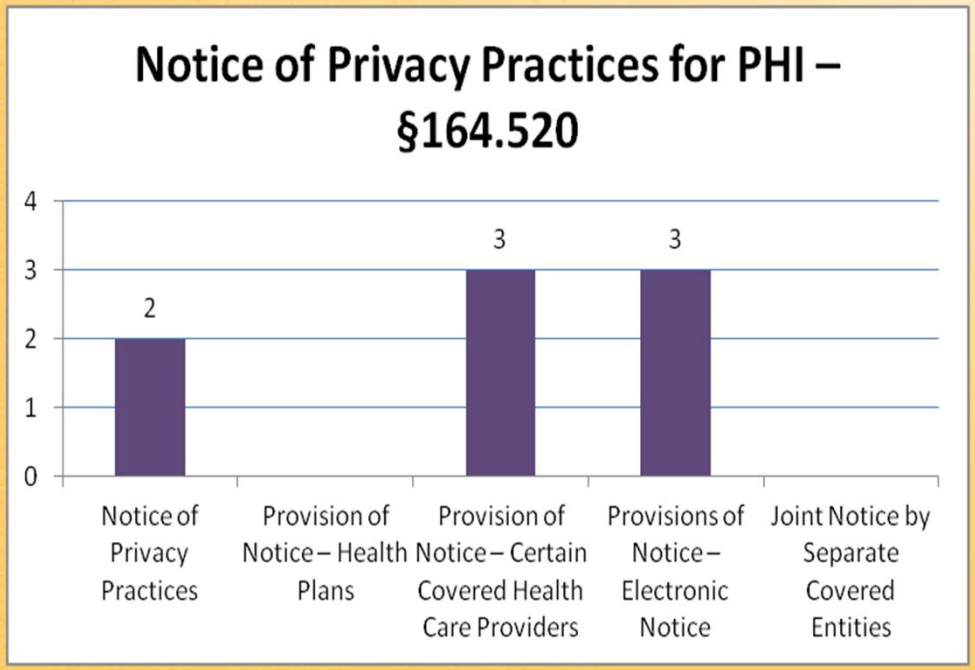
Initial 20 Findings Analysis
Privacy Issues

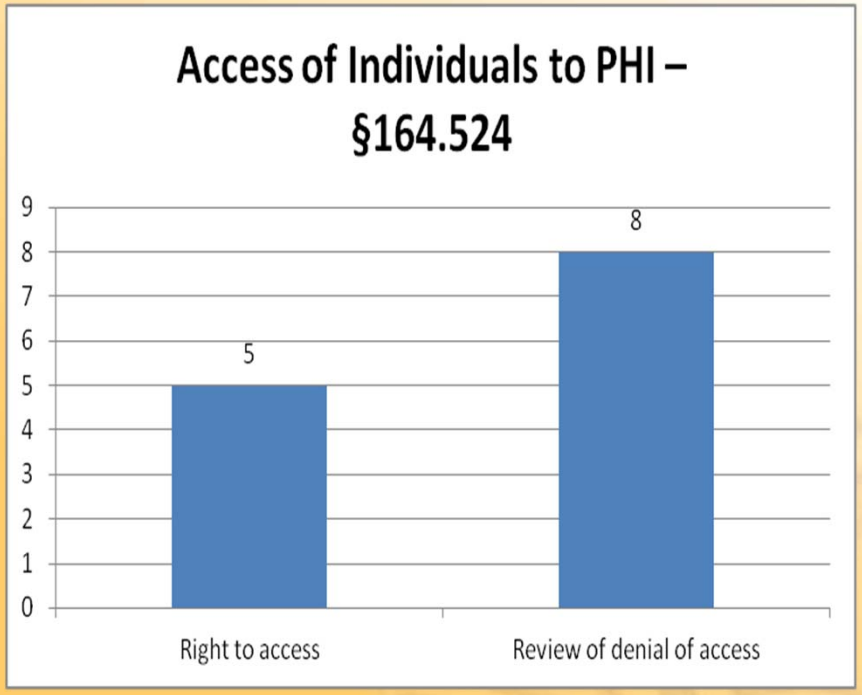


Initial 20 Findings Analysis Privacy: Uses and Disclosures

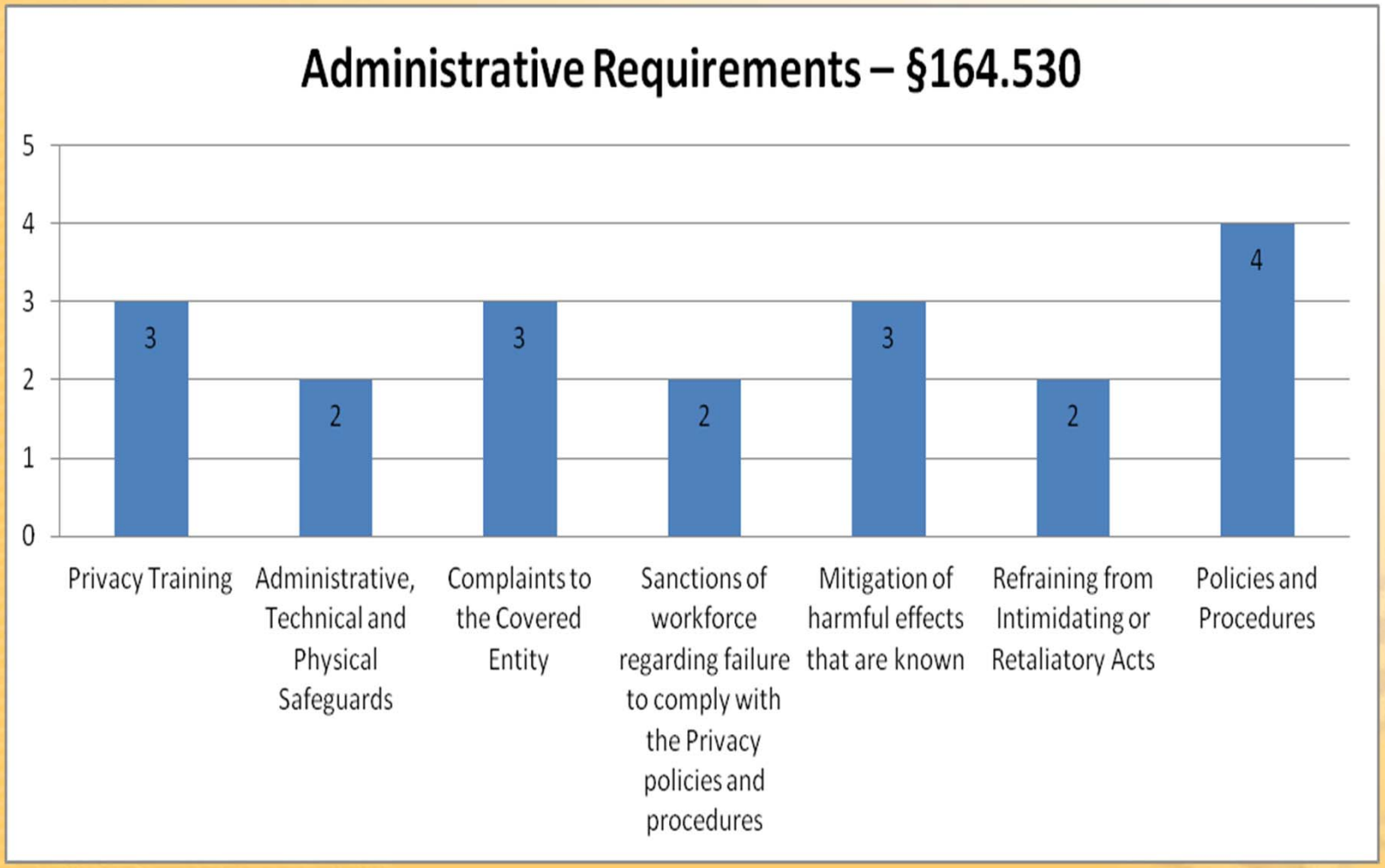


Initial 20 Findings Analysis
Privacy: Notice and Access

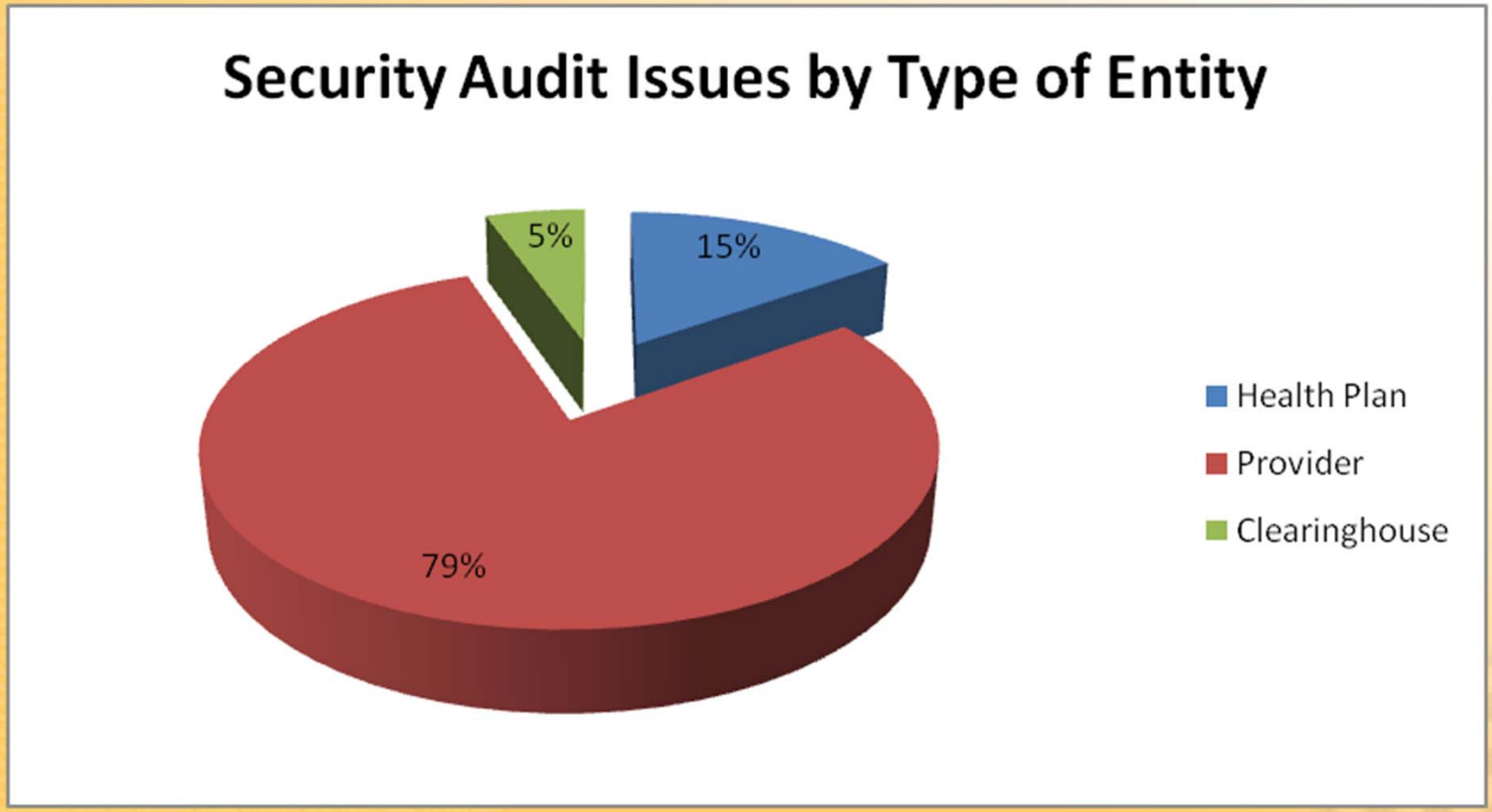




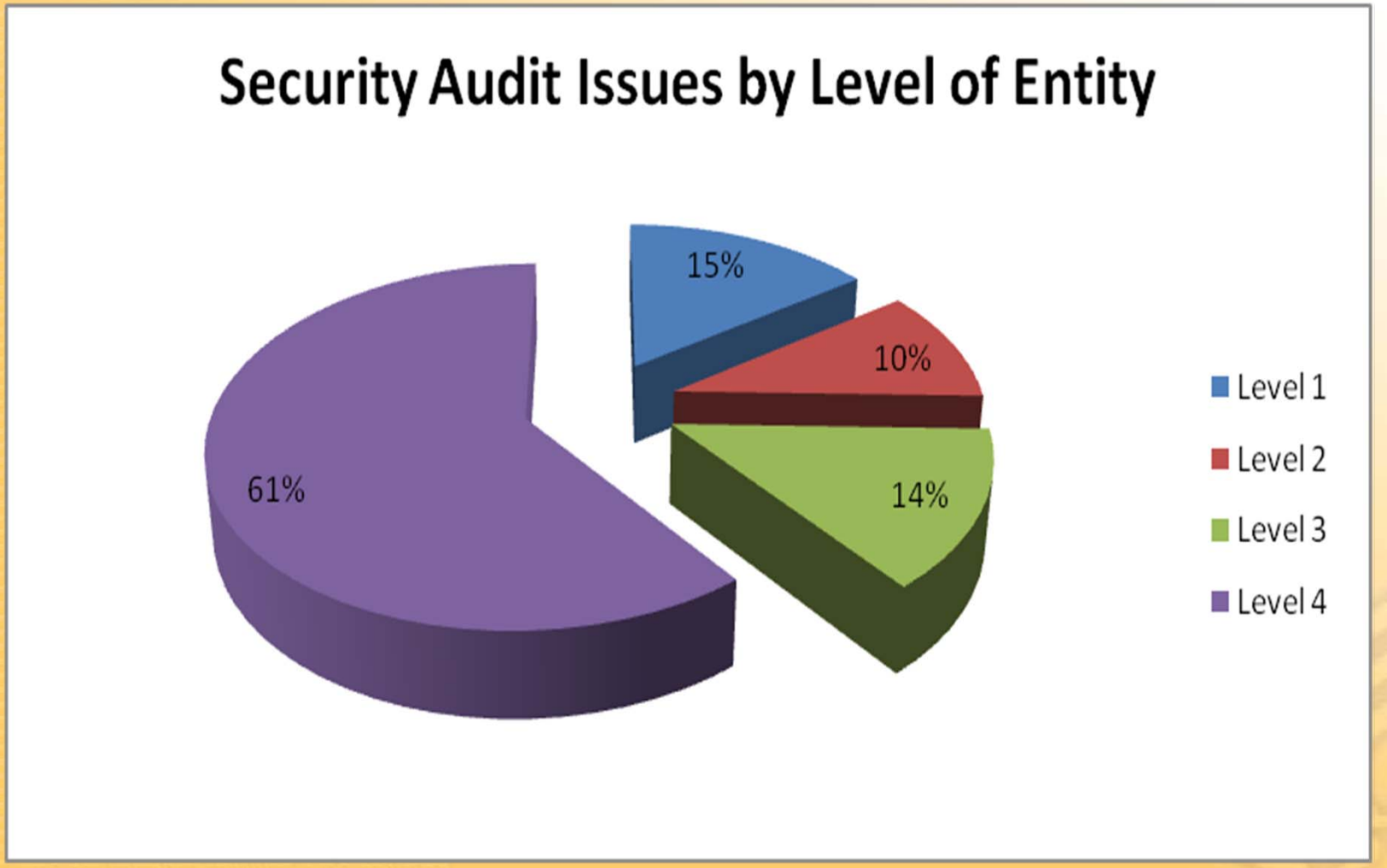
Initial Findings Analysis Privacy: Administrative Requirements



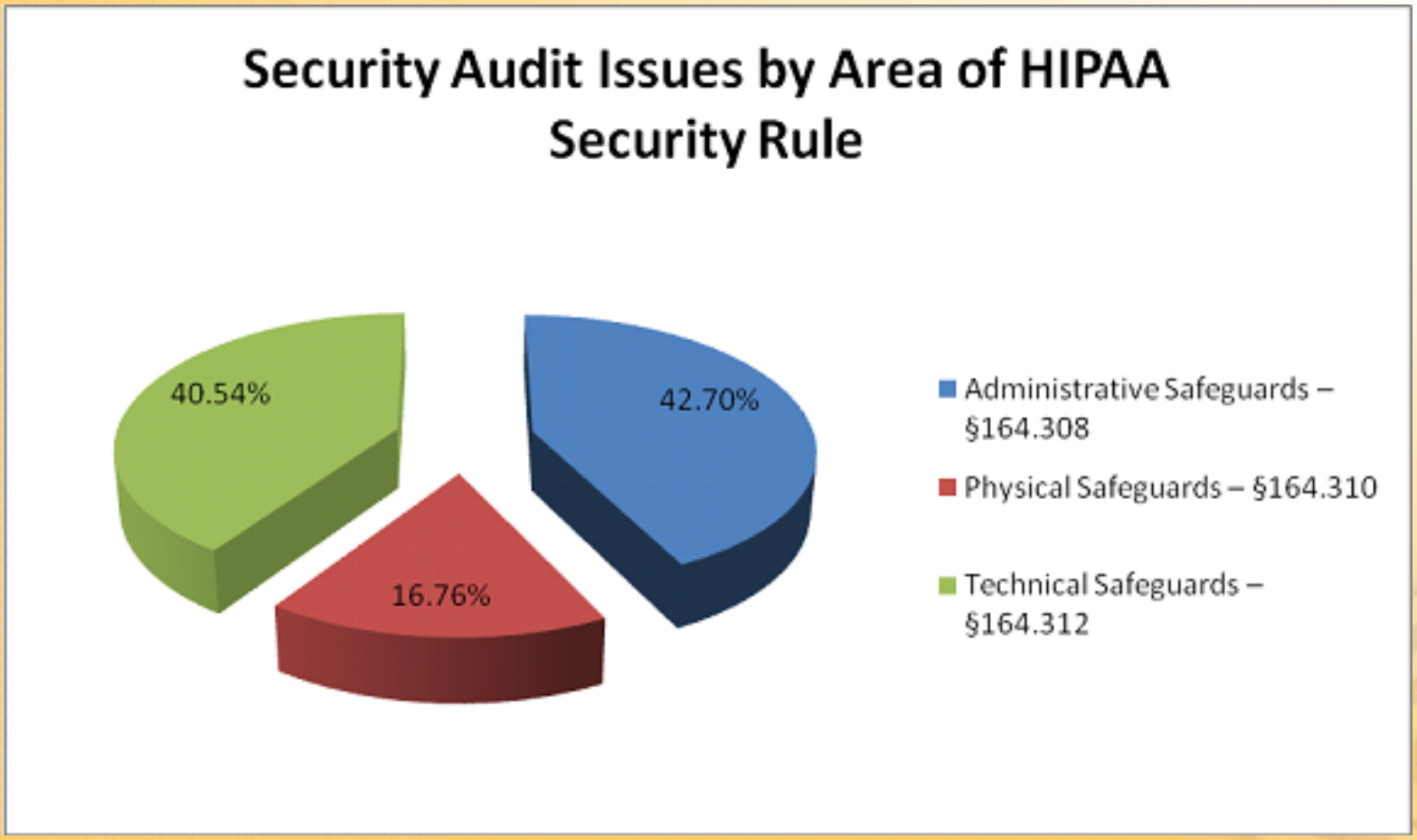
Initial 20 Findings Analysis Security Issues



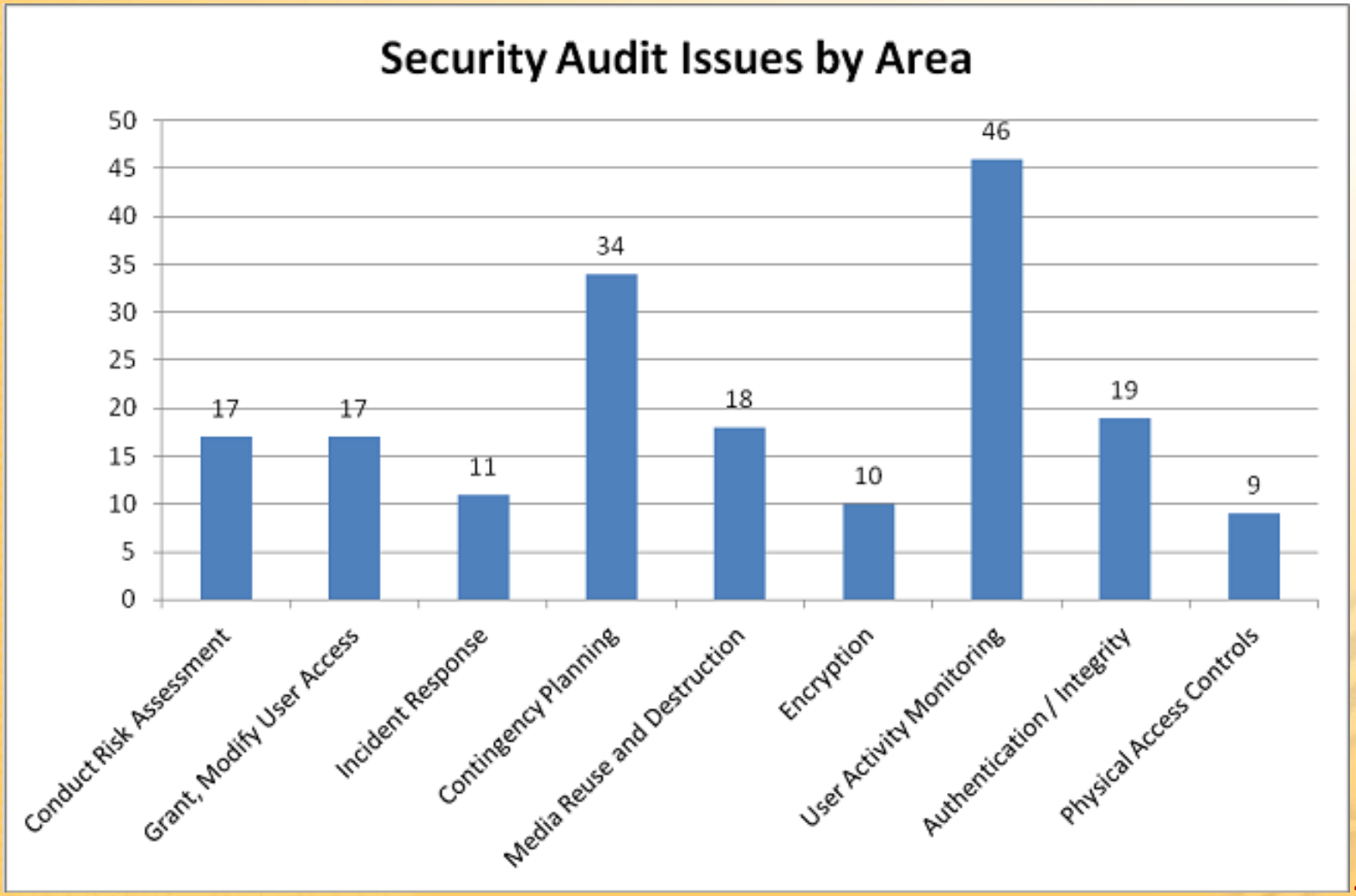
Initial 20 Findings Analysis
Security Issues



Initial 20 Findings Security Issues



Initial 20 Findings
Security Top Issues



Preliminary Observations

- Policies and Procedures
- Priority HIPAA compliance programs
- Small providers
- Larger entities security challenges
- Conduct of Risk Assessments
- Managing third party risks
- Privacy challenges are widely dispersed throughout the protocol - no clear trends by entity type or size

Future of Audit

- All audits in pilot to end December 2012
- Findings will be used to look for trends
- Evaluation contract to conduct analysis of 2011 and 2012 activities
- Pilot experience and reports will feed into decisions re ongoing audit program
  - *Structure, focus, size*

Future of Audit

- TBD: Business Associates – more decisions
- BA Protocol Development
- Who to Audit – how to identify BAs
  - Who is a business associate? How to identify in the population?
  - Location; line of business; timeliness of information; subcontractors?
- What to Audit
  - Limited requirements for BAs

Non-Compliance Risks

- Loss of Contracts
- Criminal and Civil investigation
- Federal penalties, State fines
- Public Harm and Reputational Risk
- Legal Costs
- Cost of Notification

Next Steps to Consider

- Conduct a robust review & assessment
- Determine Lines of Business affected by HIPAA
- Map/Flow PHI movement within your organization, as well as flows to/from third parties
- Find all of your PHI
- See guidance available on OCR web site