U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE FOR CIVIL RIGHTS

2012 Audits of Covered Entity Compliance with HIPAA Privacy, Security and Breach Notification Rules

Initial Analysis

February 2013

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

Program Background

- 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.
- 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

Breakdown of 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***

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

Auditees by Type & Size

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

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.

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

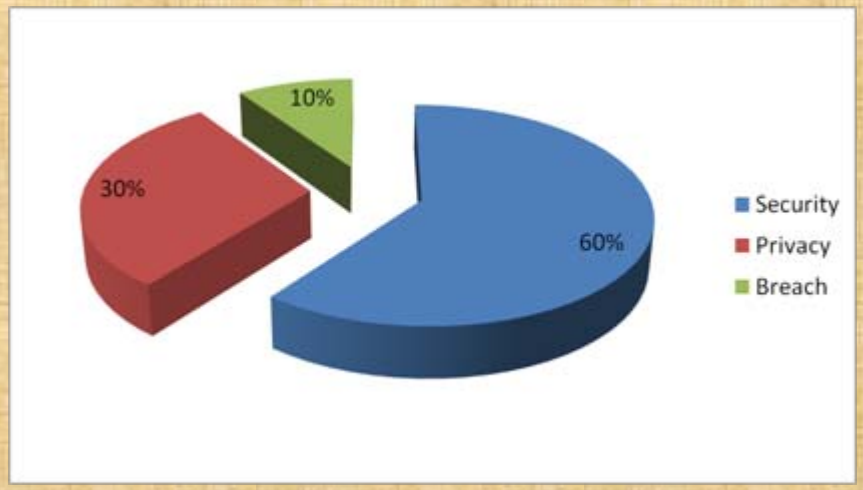
Overall Findings & Observations

- 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 and observations (65%)than would be reflected purely by their proportion of the total set (53%).
- Smaller, *Level 4* entities struggle with all three areas

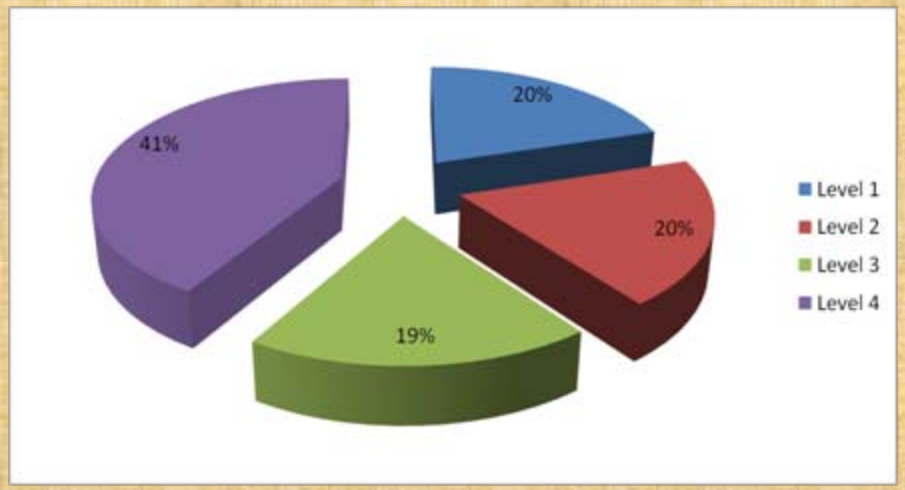
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Audit Findings and Observations

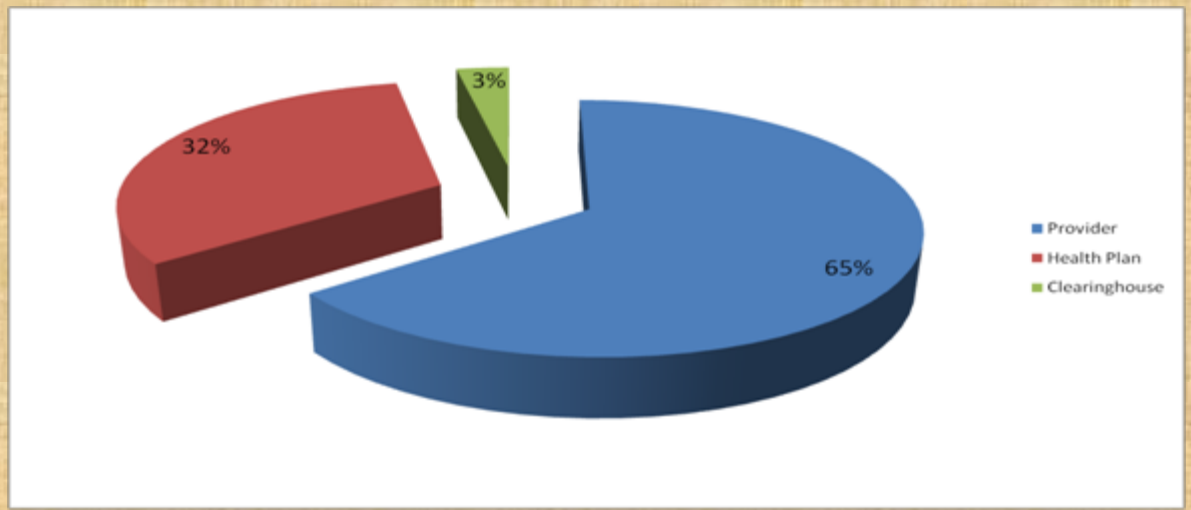
Audit Findings and Observations by Rule



Audit Findings and Observations by Level



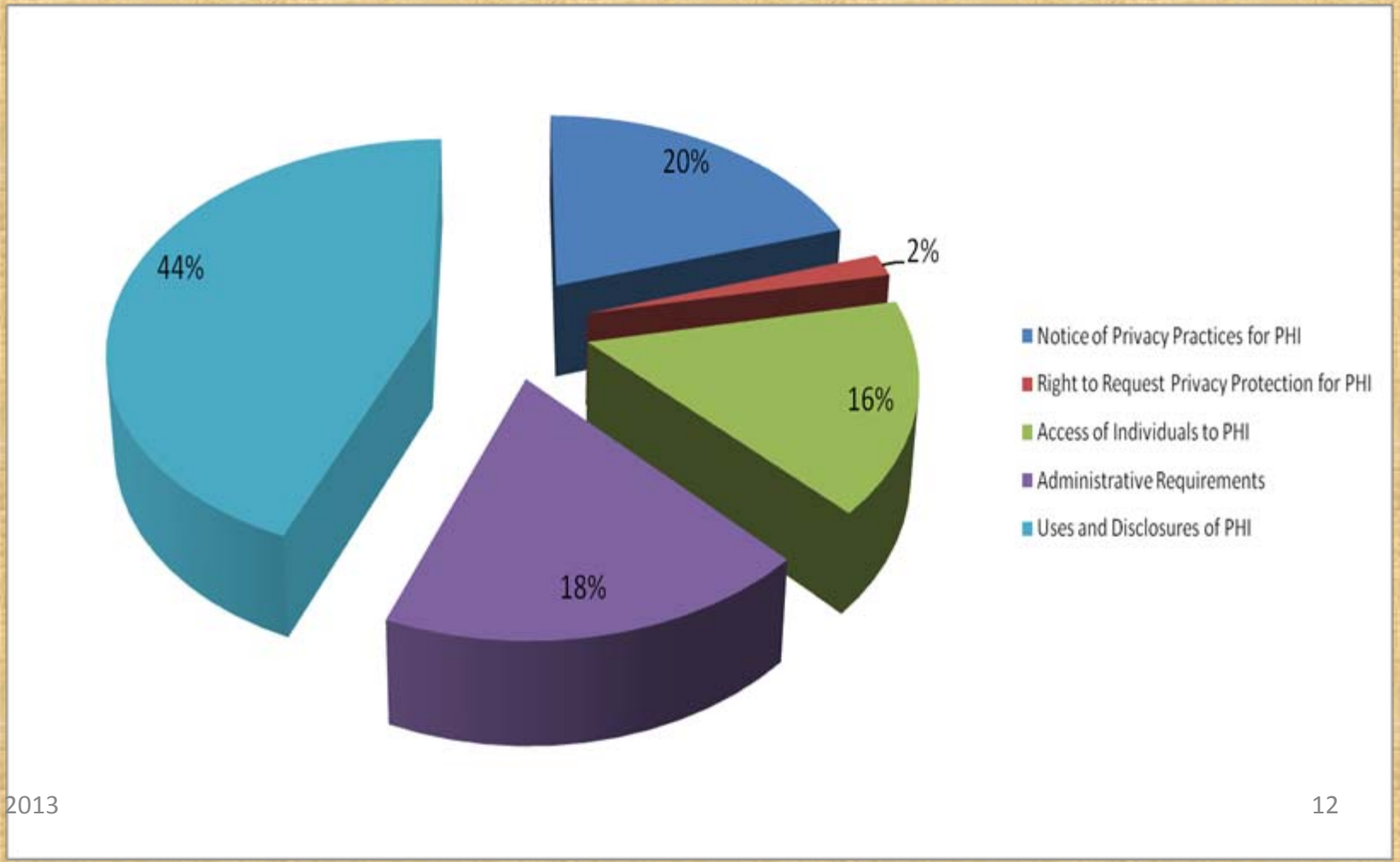
Audit Findings and Observations by Type of Covered Entity



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

Privacy Findings & Observations

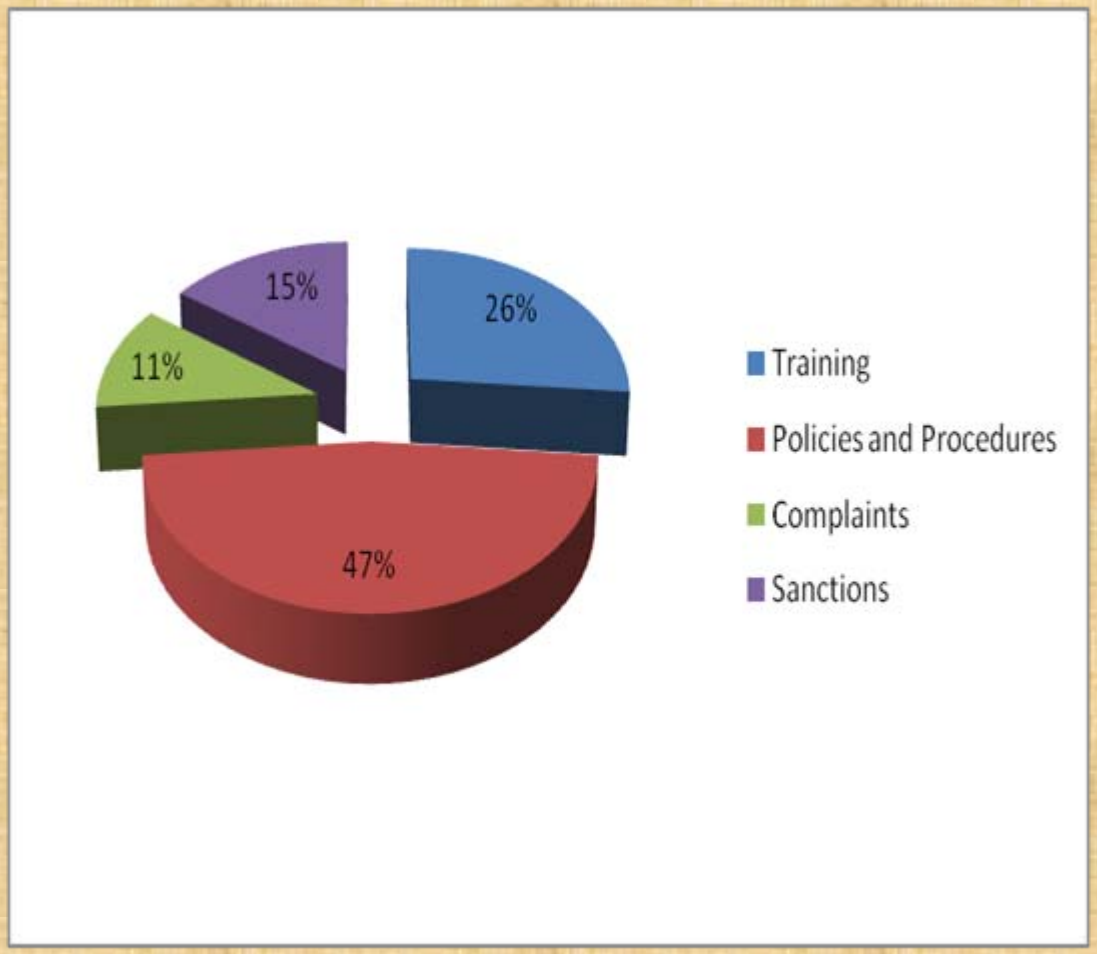
Percentage of Findings and Observations by Area of Focus



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

Privacy Administrative Elements

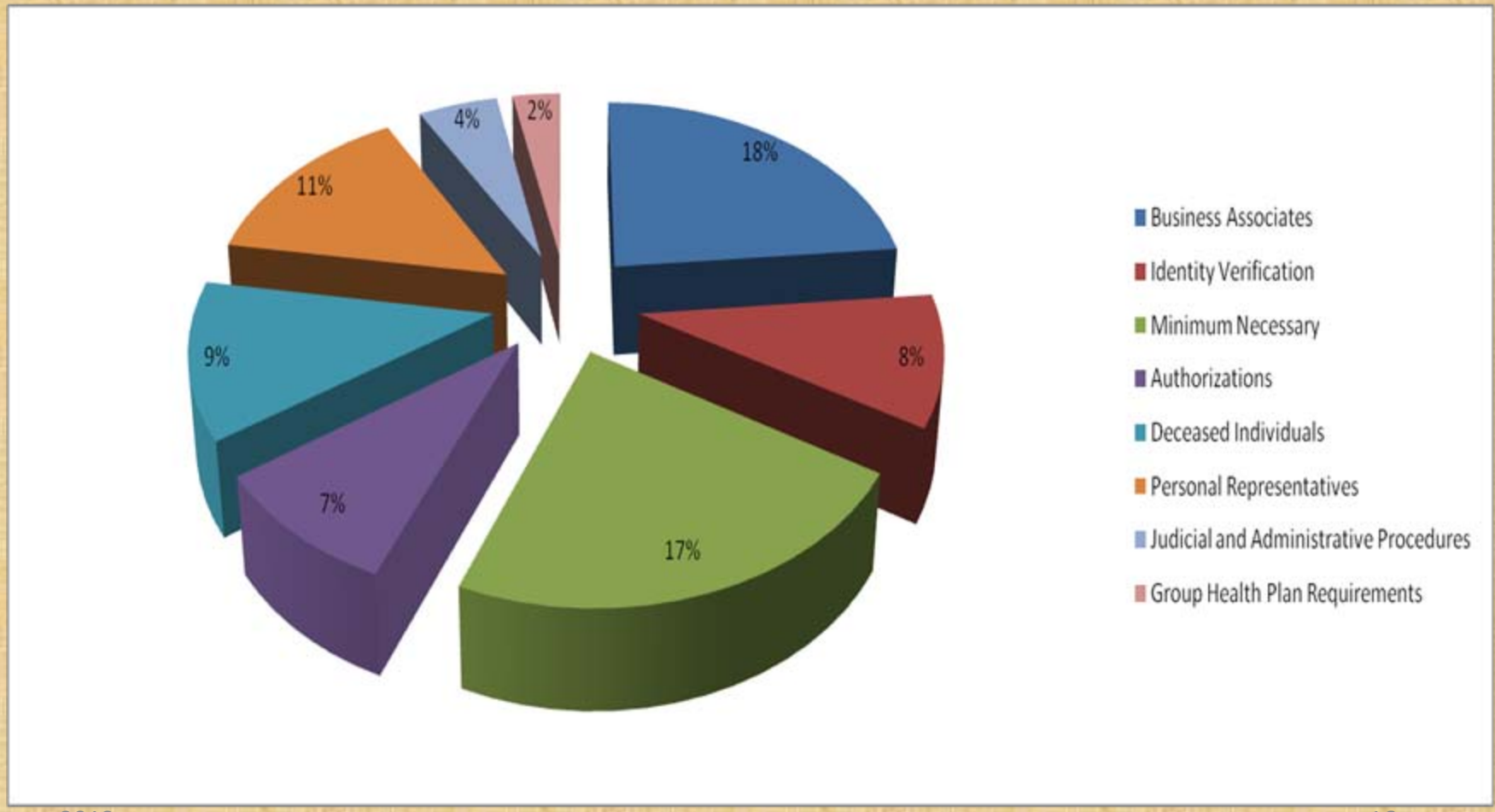
Administrative Requirements
Findings and Observations



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

Privacy -- Uses and Disclosures

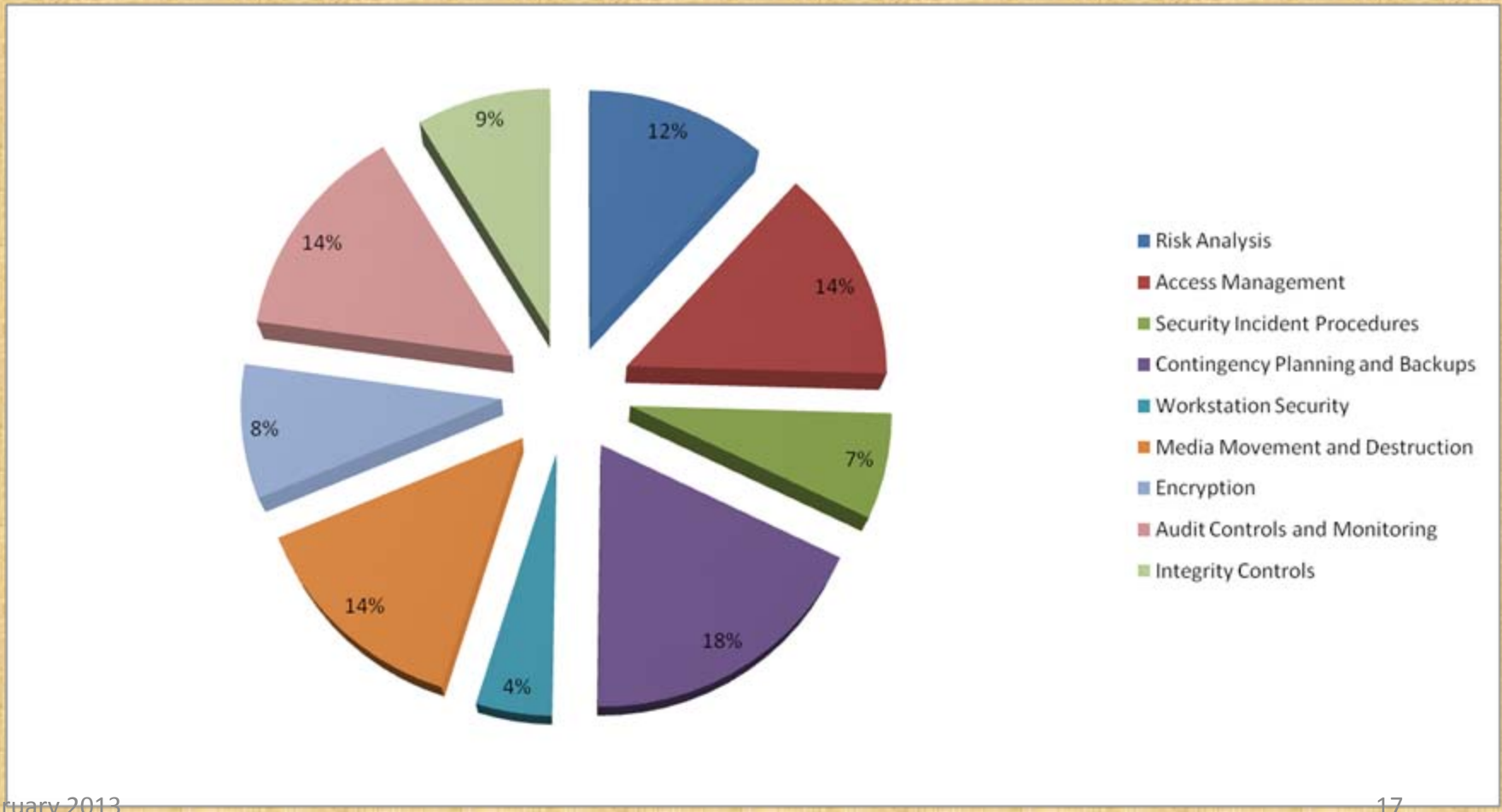
Uses and Disclosures of PHI Findings and Observations



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 Results

- 58 of 59 providers had at least one Security finding or observation
- No complete & accurate risk assessment-two thirds
  - 47 of 59 providers,
  - 20 out of 35 health plans and
  - 2 out of 7 clearinghouses
- Security addressable implementation specifications: Almost every entity without a finding or observation met by fully implementing the addressable specification.

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

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

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
- Internal analysis of leading practices, audit results
- Developing Options for ongoing program design and focus
- Creation of technical assistance based on results
- Determine where entity follow up is appropriate

February 19, 2013

CYNERGISTEK

National Hipaa summit: Response to ocr audits

Presented by:

Mac McMillan

CEO

CynergisTek, Inc.

Observations

- Performance was no where near where it should have been by this juncture
- No startling revelations here…
- Healthcare as a whole has much to do still
- Smaller providers have the biggest challenges
- Lack of definition and standards affects performance
- Lack of resources affects performance
- Lack of priority affects performance

Implications

- If we can't manage basic privacy and security requirements well…what of
- HIPAA provides underpinning for other requirements – Meaningful Use
- Basic privacy and security frameworks necessary to support – HIE, ACO, Physician Alignment, Patient Engagement, etc.
- Basic privacy and security frameworks affects our ability to innovate

Industry Next Steps

We need to:

- Increase educational and awareness efforts,
- Provide clearer standards for what is expected to meet compliance
- Provide guidance that reflects those standards
- Recognize those who do well, hold those who ignore their responsibilities accountable
- Identify better mechanisms for supporting the smaller provider community