# Preparing for the HIPAA Compliance Audit

Mari Turvey, Director, IT Advisory, KPMG

Doron Rotman,
National Privacy Service Leader, KPMG

Governance Risk and Compliance – G13

# Agenda

- HIPAA Title II
- HIPAA Privacy
- HIPAA Security
- HITECH Act Requirements
- Breach Notification
- OCR Audit Program
- First 20 Auditees

# Agenda

## HIPAA Title II

- HIPAA Privacy
- HIPAA Security
- HITECH Act Requirements
- Breach Notification
- OCR Audit Program
- First 20 Auditees

# HIPAA Overview

Health Insurance Portability and Accountability Act (HIPAA) of 1996

HIPAA's Administrative Simplification section addresses three areas:

**Transaction Code Sets and Identifiers**

- Formatting and processing of healthcare claims related transactions

**Privacy**

- Protection of patient rights and information from undue exposure

**Security**

- Safeguarding of the technology systems that process health information

# HITECH Act Impact

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

Though outside of HIPAA title II, this is additional & direct legislation to improve the original HIPAA title II requirements and to define and tighten some open gaps

- **Establishes Breach requirement for Privacy Rule Violation**
  - Effective date was September 23, 2009
  - Establishes Scope and Timeline
  - Clarifies definition of Breach
  - Likelihood of harm must be determines/assessed
- **Establishes New Penalty Levels**
  - Uncorrected willful neglect $1.5 million to Unknowing $25K
- **Establishes compliance requirements for all PHI and PHR, whether included in a BA agreement or not.**
- **Enforcement Broadened to include State A.G.'s and Local Law enforcement**

# HIPAA Impact

## Who is impacted by HIPAA?

**Covered Entities (CE) –**

Healthcare providers, payers, and clearinghouses that **receive, transmit, or process electronic protected health information (ePHI)**

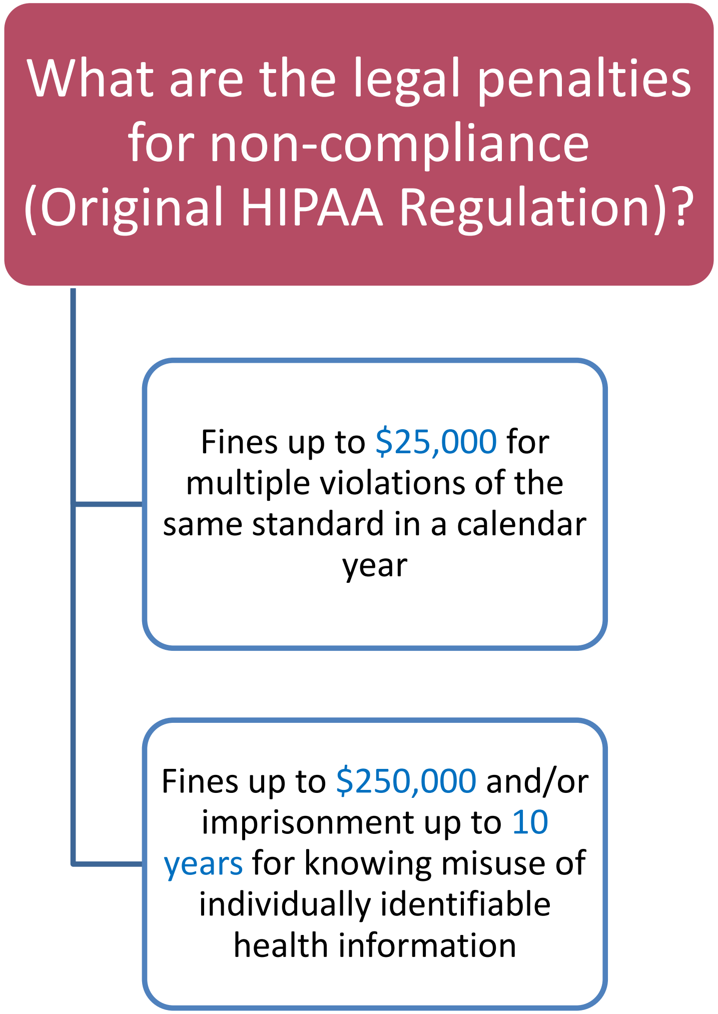
Includes **employer-sponsored health plans, state and local government healthcare payers, and multi-line insurers**

**Business Associates (BA) –**

A person or an organization that performs functions or **services TO, FOR, or ON BEHALF OF, the CE** that involve the Uses & Disclosures of PHI.

The HITECH ACT enforces the same level of requirements on a Business Associate (BA) that it does to a Covered Entity (CE).

# HIPAA Penalties & Oversight



What are the legal penalties for non-compliance (Original HIPAA Regulation)?

Fines up to $25,000 for multiple violations of the same standard in a calendar year

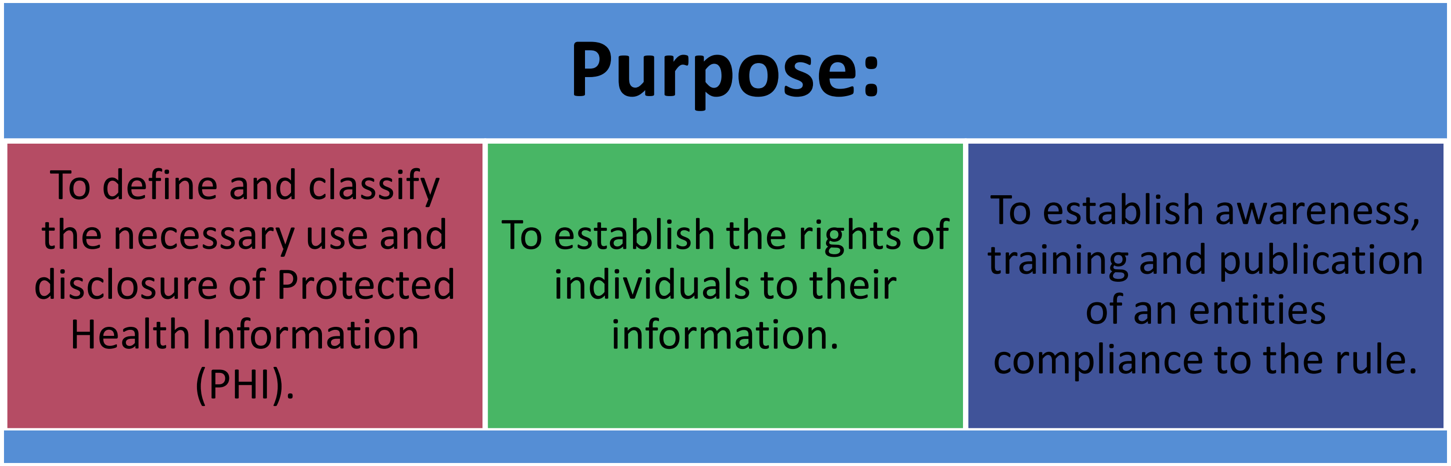
Fines up to $250,000 and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information

- Enforcement responsibility has been delegated to the Office for Civil Rights (OCR) for both Privacy (as of April 13, 2003) and Security (as of July 27, 2009)
- OCR has started a pilot program to assess compliance of Covered Entities with HIPAA.
- 2009, the program has been expanded. Plans by OCR are to conduct up to 150 audits by 12/31/2012 with external service providers and a newly formed examination group staffed internal to OCR.
- States have been additionally involved in privacy exposures and have levied fines in addition to federal guidelines, mostly leveraging State PII laws with HIPAA Title II requirements.

# Agenda

- HIPAA Title II
- HIPAA Privacy
- HIPAA Security
- HITECH Act Requirements
- Breach Notification
- OCR Audit Program
- First 20 Auditees

# HIPAA Privacy Overview



**Purpose:**

To define and classify the necessary use and disclosure of Protected Health Information (PHI).

To establish the rights of individuals to their information.

To establish awareness, training and publication of an entities compliance to the rule.

Establishment of Fines, Penalties for lack of compliance.

- Numerous Modifications were published thru February 21, 2006. Effective dates for modification directly to 45 CFR 160, 164 is 180 days past publication in the Federal Register.
- Effective compliance date – February 26, 2001

# Five Key Areas of Privacy Standards

### Boundaries

- Information used only for intended purpose and only as much information as required for the intended purpose
- Consumer use and disclosure statement

### Safeguards

- Administrative, technical, and physical mechanisms to keep information private, confidential and secure within internal operating systems and external communications

### Consumer Control

- Informed consent to use information
- Right to access and amend information
- Authorization for disclosures
- Record of disclosures

### Accountability

- Federal penalties for violations
- Effective compliance activities to deter, identify, and punish violations

### Public Responsibility

- Process for disclosing information for public health, research & legal purposes

What information is covered by the final rule?

The final rule covers all *Individually Identifiable Health Information (IIHI) regardless of media* ***(electronic, written or oral).***

# PHI - Identifiable Data Elements (18+)

- Name
- Address (street address, city, county, zip code (more than 3 digits) or other geographic codes)
- Names of relatives
- Names of Employers
- Birth Date
- Telephone Number
- Fax Number
- e-mail addresses
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number
- Account Number
- Certificate/License Number
- Any vehicle or device serial number
- Web URL
- Internet Protocol (IP) Address
- Finger or voice prints
- Photographic images
- Any other unique identifying number, characteristic, or code (whether generally available in the public realm or not)

# PHI - Identifiable Data Elements (18+)

- Name
- Address (street address, city, county, zip code (more than 3 digits) or other geographic codes)
- Names of relatives
- Names of Employers
- Birth Date
- Telephone Number
- Fax Number
- e-mail addresses
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number
- Account Number
- Certificate/License Number
- Any vehicle or device serial number
- Web URL
- Internet Protocol (IP) Address
- Finger or voice prints
- Photographic images
- Any other unique identifying number, characteristic, or code (whether generally available in the public realm or not)

# Minimum Necessary

§ 164.502(b)

- A covered entity must make reasonable efforts to limit the PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
- Minimum necessary does NOT apply to:
  - Disclosures to or requests by a health care provider for treatment.
  - Use or disclosures to the individual (refer to the regulations for the exceptions).
  - Disclosures to the Secretary of DHHS.
  - Disclosures required by law.

# Minimum Necessary for the Workforce

§ 164.514 (d) (2)

- A covered entity must identify those persons within its workforce who need access to protected health information to carry out their duties.
- A covered entity must also identify the category or categories of protected health information to which access is needed and any conditions appropriate for such access.

§ 164.514(d)(4)

- Requires covered entities to request only the minimum necessary protected health information to accomplish the purpose for which the request is made.

# Business Associates

§ 164.502 (e) (1)

- PHI may be disclosed to a business associate, and the business associate may create or receive PHI on the covered entity's behalf, provided that satisfactory assurance is obtained that the business associate will "appropriately safeguard the information." HITECH Update, a BA has direct responsibility to maintain Privacy and Security and if they use third parties, they must obtain satisfactory assurance.

§ 164.504 (e) (1)

- This satisfactory assurance must be documented through a written contract or other written agreement or arrangement with the business associate and meet specific requirements.

# Business Associates

§ 164.504 (e) (1)

- If a covered entity is or has been aware of material breach or violation of the business associate’s obligation, and the covered entity does not take reasonable steps to cure the breach or end the violation, or does not end the contract or arrangement, the covered entity is non-compliant with the requirements. HITECH update. This responsibility is now directly the responsibility of the BA as well. Though Breach notification falls to the CE.

# Agenda

- HIPAA Title II
- HIPAA Privacy

## HIPAA Security

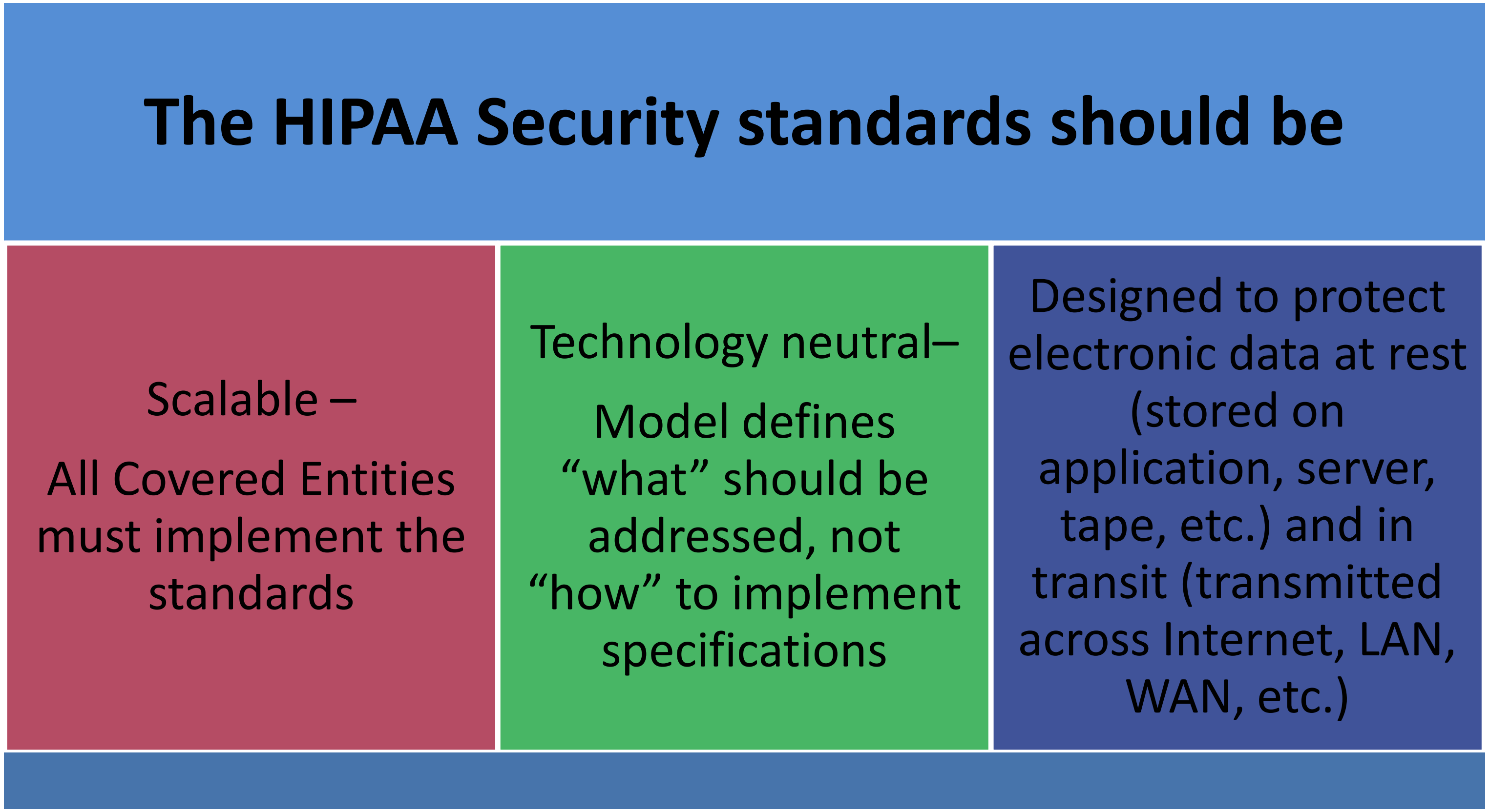
- HITECH Act Requirements
- Breach Notification
- OCR Audit Program
- First 20 Auditees

# HIPAA Security Overview

Purpose: ensure confidentiality, integrity and availability of electronic protected health information (ePHI), i.e., protect technology and processes

- Standards set a minimum “baseline” of controls and safeguards
- CEs should develop information protection and security programs based on:
  - » Performance of a risk assessment
  - » Acceptable level of risk that organizations are willing to tolerate
- BA’s via contract vehicle with CE’s should meet this obligation. HITECH update, a BA is required to meet the Security rule.
- Effective compliance date – April 21, 2005
- Small health plans – April 21, 2006

# HIPAA Security Guiding Principles



**The HIPAA Security standards should be**

Scalable –

All Covered Entities must implement the standards

Technology neutral–

Model defines "what" should be addressed, not "how" to implement specifications

Designed to protect electronic data at rest (stored on application, server, tape, etc.) and in transit (transmitted across Internet, LAN, WAN, etc.)

# HIPAA Security Basics

"Standards" are supported by "Implementation Specifications"

- 20 Required vs. 22 Addressable Specifications
- Addressable specification options:
  - Implement addressable specifications
  - Implement alternative security measures
  - Implement combination of both
  - Not implement specifications or alternatives
- Decision must be based on risk assessment and documented and retained for 6 years
  - Examples include:
    - Workforce Security - Access Authorization
    - Facility Access Controls – Facility Security Plan
    - Transmission Security – Encryption
- Application and data workflows for the control and necessary use determination need to be completed.

# Detailed Requirements

| I. Admin. Safeguards | Required Specifications (12) | Addressable Specifications (11) |
|---|---|---|
| **1. Security Management Process** | 1. Risk Analysis<br>2. Risk Management<br>3. Sanction Policy<br>4. System Activity Review | None |
| **2. Assigned Security Responsibility** | Required but no specs | None |
| **3. Workforce Security** | None | 1. Authorization & Supervision |
| **4. Information Access Management** | Isolate Clearinghouse Function | 1. Access Authorization<br>2. Access Establishment<br>3. Access Modification |
| **5. Security Awareness Training** | None | 1. Security Reminders<br>2. Protection from Malicious SW<br>3. Login Monitoring<br>4. Password Management |
| **6. Incident Procedures** | Response/Reporting | None |
| **7. Contingency Plan** | 1. Plans for Data Backup<br>2. Disaster Recovery<br>3. Emergency Mode Operation | 1. Testing/Revision Procedures<br>2. Application Criticality & Data Criticality Analysis |
| **8. Evaluation** | Required but no specs | None |
| **9. BA Contracts & Agreements** | Written Contract or Other Arrangements | None |

# Detailed Requirements

| II. Physical Safeguards | Required Specifications (4) | Addressable Specifications (6) |
|---|---|---|
| **1. Facility Access Control** | None | 1. Contingency Operations<br>2. Facility Security Plan<br>3. Access Control and Validation<br>4. Maintenance Records |
| **2. Workstation Use** | Required but no specs | None |
| **3. Workstation Security** | Required but no specs | None |
| **4. Device and Media Controls** | 1. Media Disposal<br>2. Media Re-use | 1. Accountability<br>2. Data Backup and Storage |
| **III. Technical Safeguards** | **Required Specifications (4)** | **Addressable Specifications (5)** |
| **1. Access Control** | 1. Unique User ID<br>2. Emergency Access Procedure | 1. Automatic Logoff<br>2. Encryption and Decryption |
| **2. Audit Controls** | Required but no specs | None |
| **3. Integrity** | None | Mechanism to Authenticate Electronic PHI |
| **4. Person or Entity Authentication** | Required but no specs | None |
| **5. Transmission Security** | None | 1. Integrity Controls<br>2. Encryption |

# Agenda

- HIPAA Title II
- HIPAA Privacy
- HIPAA Security

# HITECH Act Requirements

- Breach Notification
- OCR Audit Program
- First 20 Auditees

# ARRA & Healthcare IT

**“Accounting of Disclosures (Effective: 1/1/2011 through 1/1/2014, based upon acquisition of eHR)**

**Covered entities must produce, upon request, an accounting of all disclosures of the individual’s PHI, including routine disclosures over a three year period.**

**Business Associates must produce, upon request, an accounting of disclosures of PHI for treatment, payment and health care operations**

**Prohibition on Sale (Effective: No later than 2/17/2011)**

A Covered Entity or Business Associate is prohibited from receiving direct or indirect receipt of remuneration for any PHI without a HIPAA authorization from the individual

# ARRA & Healthcare IT

**Marketing and Fundraising (Effective: 2/17/2010)**

Marketing and Fundraising activities now require specific authorization for use of PHI and individuals have the right to opt out.

**Enforcement**

**Provides for enforcement of HIPAA by States Attorney Generals and local law enforcement.**

Mandatory investigations for known Privacy Breaches.

**Increases the civil penalties**

- **Unknowing ($25K)**
- **Reasonable cause ($100k)**
- **Willful Neglect ($250K)**
- **Uncorrected willful neglect ($1.5 M)**

# Agenda

- HIPAA Title II
- HIPAA Privacy
- HIPAA Security
- HITECH Act Requirements

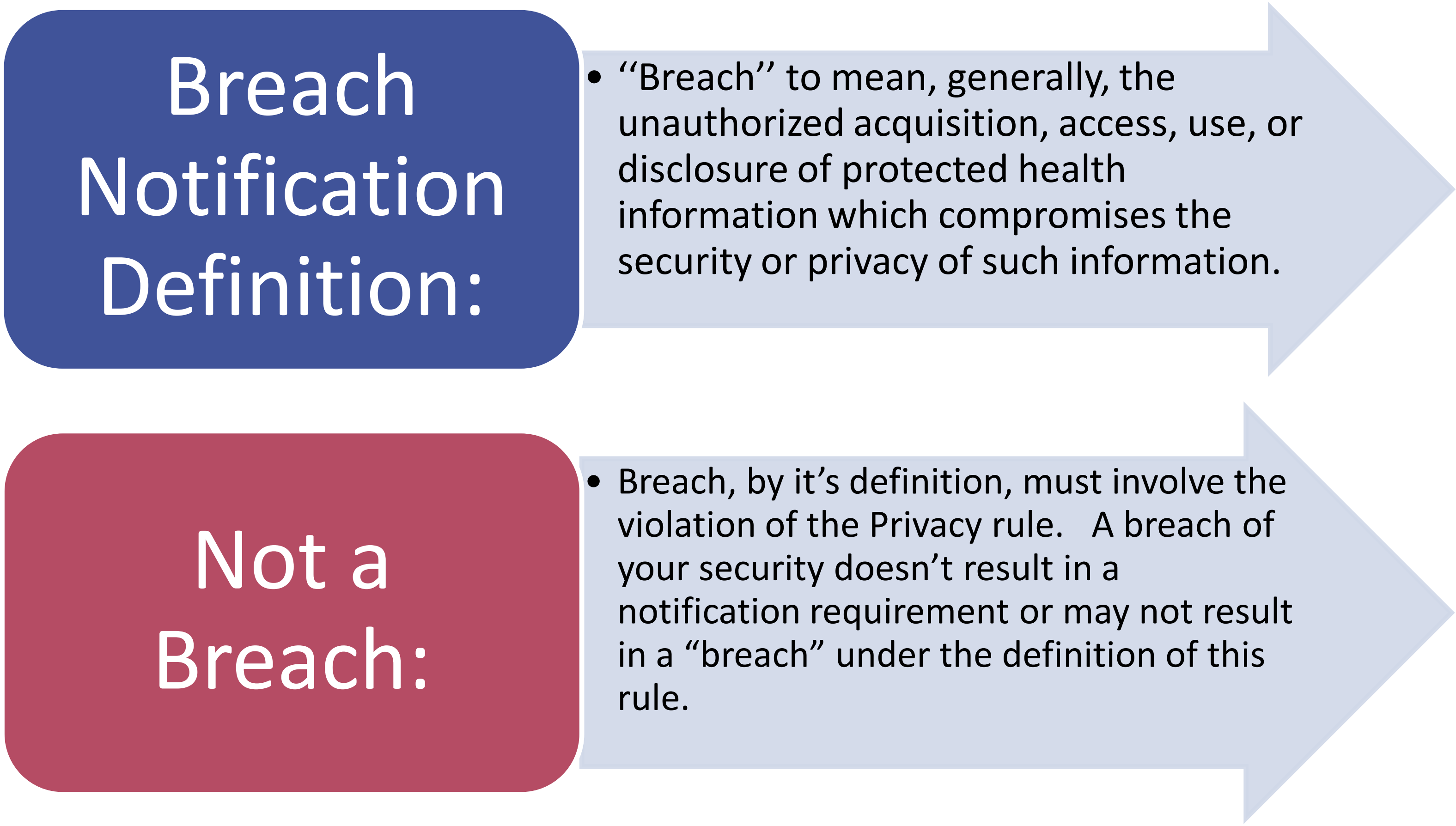
**Breach Notification**

- OCR Audit Program
- First 20 Auditees

# Breach Notification

- The HITECH Act requires HIPAA covered entities to provide notification to affected individuals and to the Secretary of Health and Human Services (HHS) following the discovery of a breach of unsecured protected health information. In addition, in some cases, the Act requires covered entities to provide notification to the media of breaches.
- If a Business Associate, you must provide immediate notification to the Covered Entity.
- Compliance with this rule was effective for enforcement on September 23, 2009
- The standard establishes specific technology requirements, via the references to NIST and FIPS standards on encryption.

# Breach Notification



Breach Notification Definition:

- ‘‘Breach’’ to mean, generally, the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information.

Not a Breach:

- Breach, by it’s definition, must involve the violation of the Privacy rule. A breach of your security doesn’t result in a notification requirement or may not result in a “breach” under the definition of this rule.

# Breach Notification

Under 45 CFR 160 and 164, Breach Notification

A breach must constitute significant risk of financial, reputational or other harm to an individual, to require notification to a group or an individual.

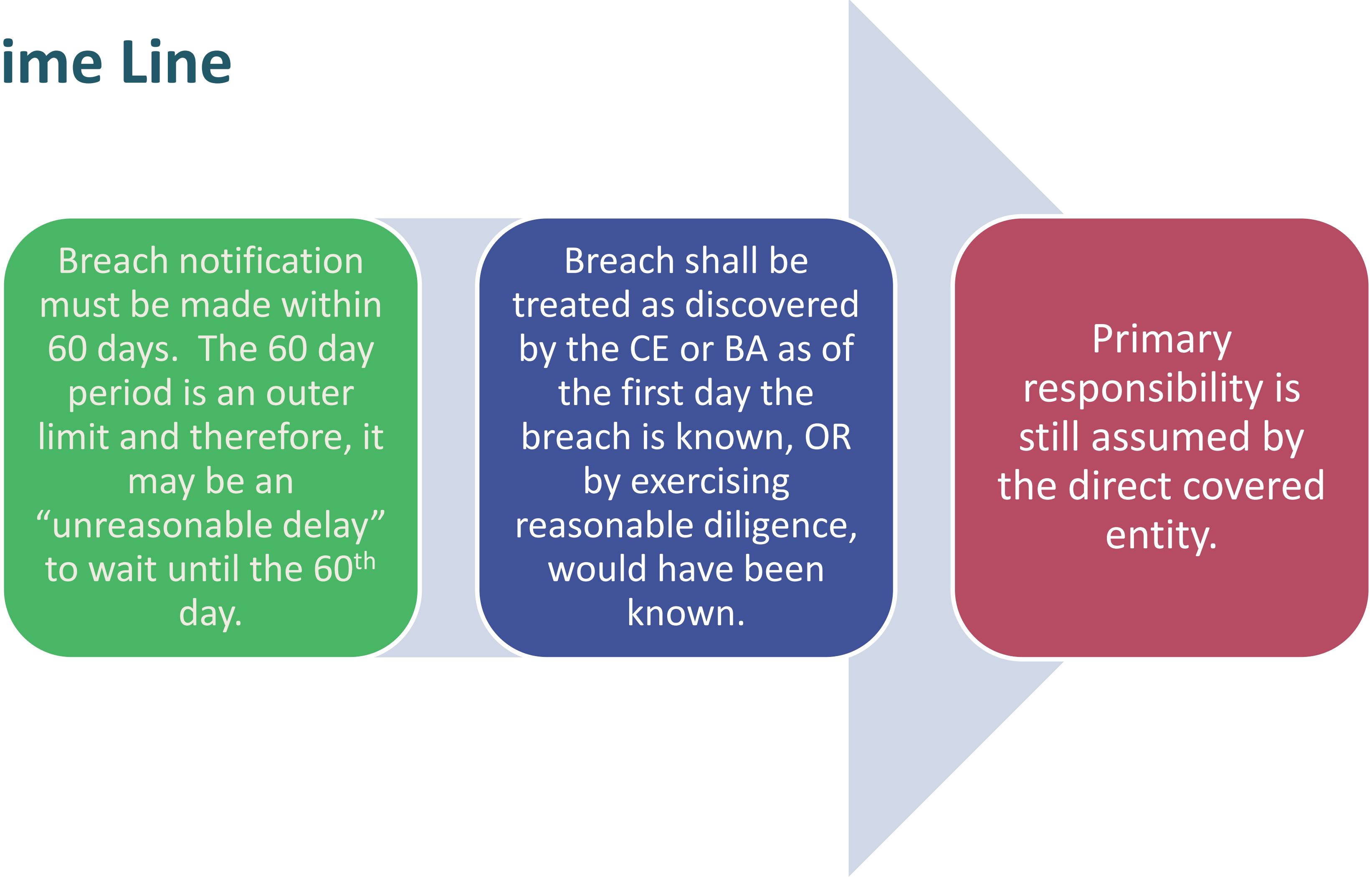
You must document your risk assessment whether you are declaring a breach and notification or not declaring a breach.

Breaches effecting over 500 people must include notification to the Secretary of HHS.

Breaches effecting over 500 people in a State or jurisdiction must include Media Notification.

# Breach Notification

## Time Line



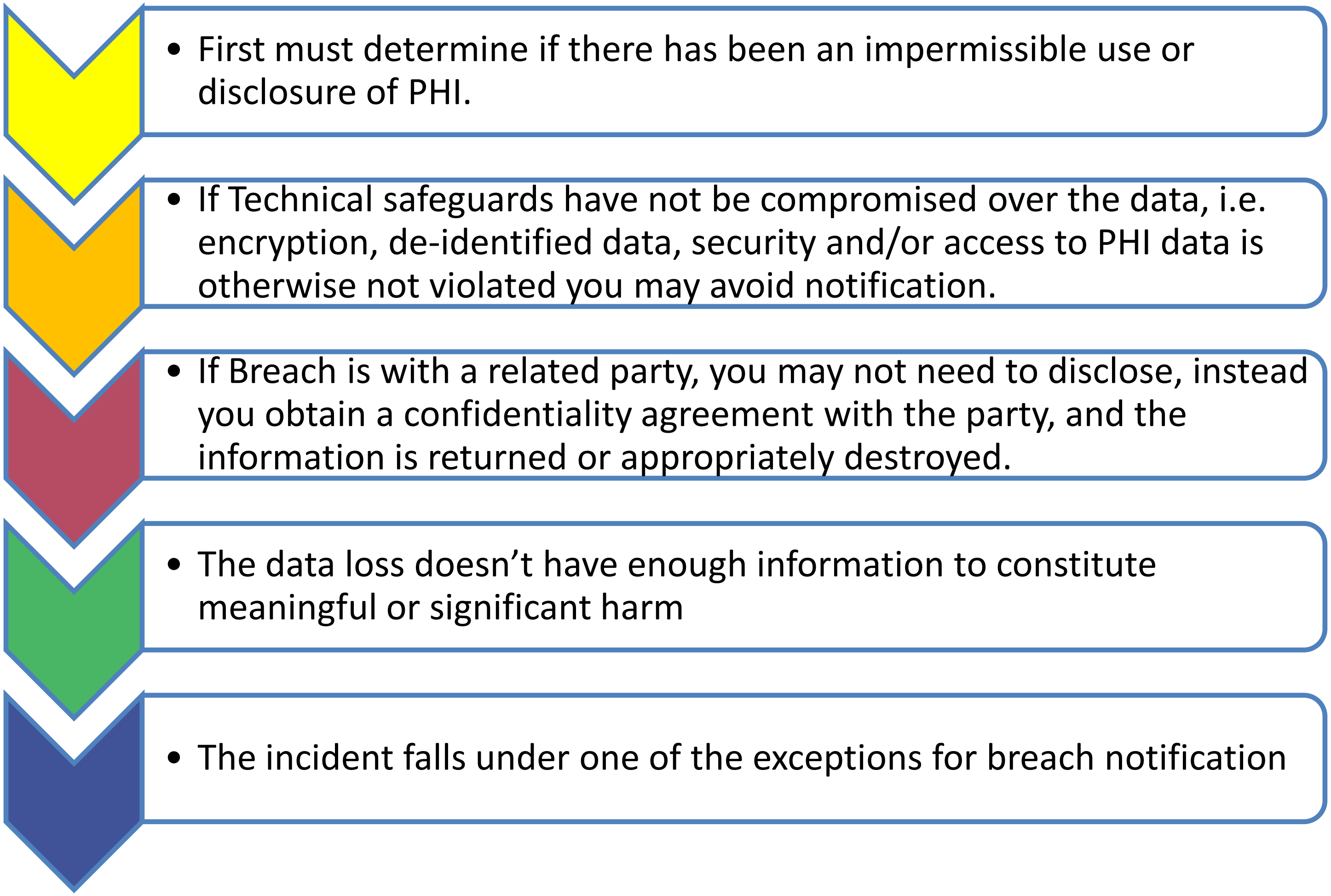
Breach notification must be made within 60 days. The 60 day period is an outer limit and therefore, it may be an "unreasonable delay" to wait until the 60th day.

Breach shall be treated as discovered by the CE or BA as of the first day the breach is known, OR by exercising reasonable diligence, would have been known.

Primary responsibility is still assumed by the direct covered entity.

# Breach Notification

## Risk Assessment



- First must determine if there has been an impermissible use or disclosure of PHI.
- If Technical safeguards have not be compromised over the data, i.e. encryption, de-identified data, security and/or access to PHI data is otherwise not violated you may avoid notification.
- If Breach is with a related party, you may not need to disclose, instead you obtain a confidentiality agreement with the party, and the information is returned or appropriately destroyed.
- The data loss doesn't have enough information to constitute meaningful or significant harm
- The incident falls under one of the exceptions for breach notification

# Agenda

- HIPAA Title II
- HIPAA Privacy
- HIPAA Security
- HITECH Act Requirements
- Breach Notification

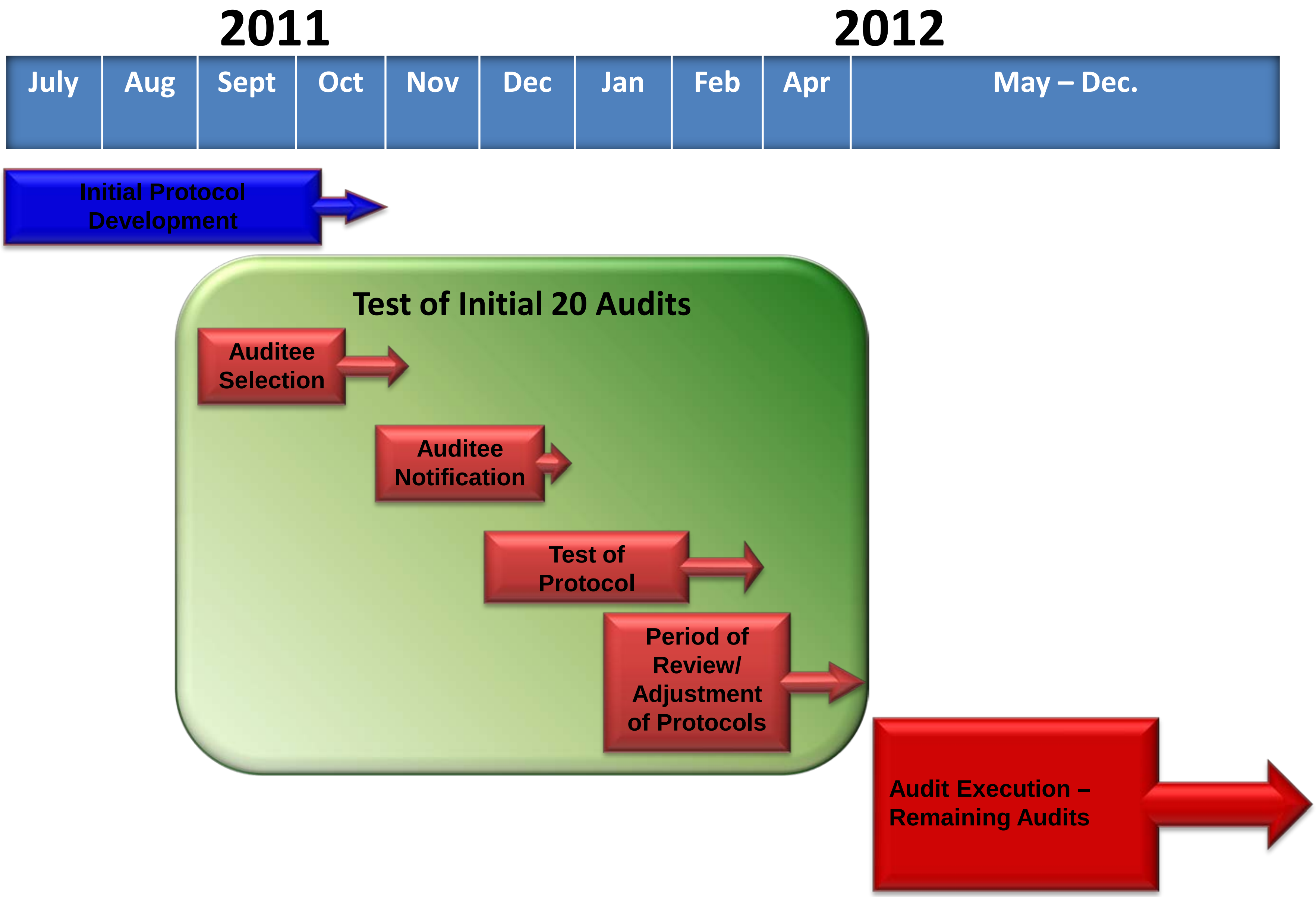
## OCR Audit Program

- First 20 Auditees

# Overview & Objective of the Audits

- Overview
  - ARRA 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.
  - OCR is piloting a program to perform up to 150 audits of covered entities to assess privacy and security compliance.
- Program Objectives
  - OCR will use the audit program to assess HIPAA compliance efforts by a range of covered entities.
  - Audits present a new opportunity to examine mechanisms for compliance, identify best practices and discover risks and vulnerabilities that may not have come to light through OCR’s ongoing complaint investigations and compliance reviews.
  - OCR will broadly share best practices gleaned through the audit process and guidance targeted to observed compliance challenges on its web site and other outreach portals.

# Overall Audit Timeline



2011

2012

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

Initial Protocol Development

Test of Initial 20 Audits

Auditee Selection

Auditee Notification

Test of Protocol

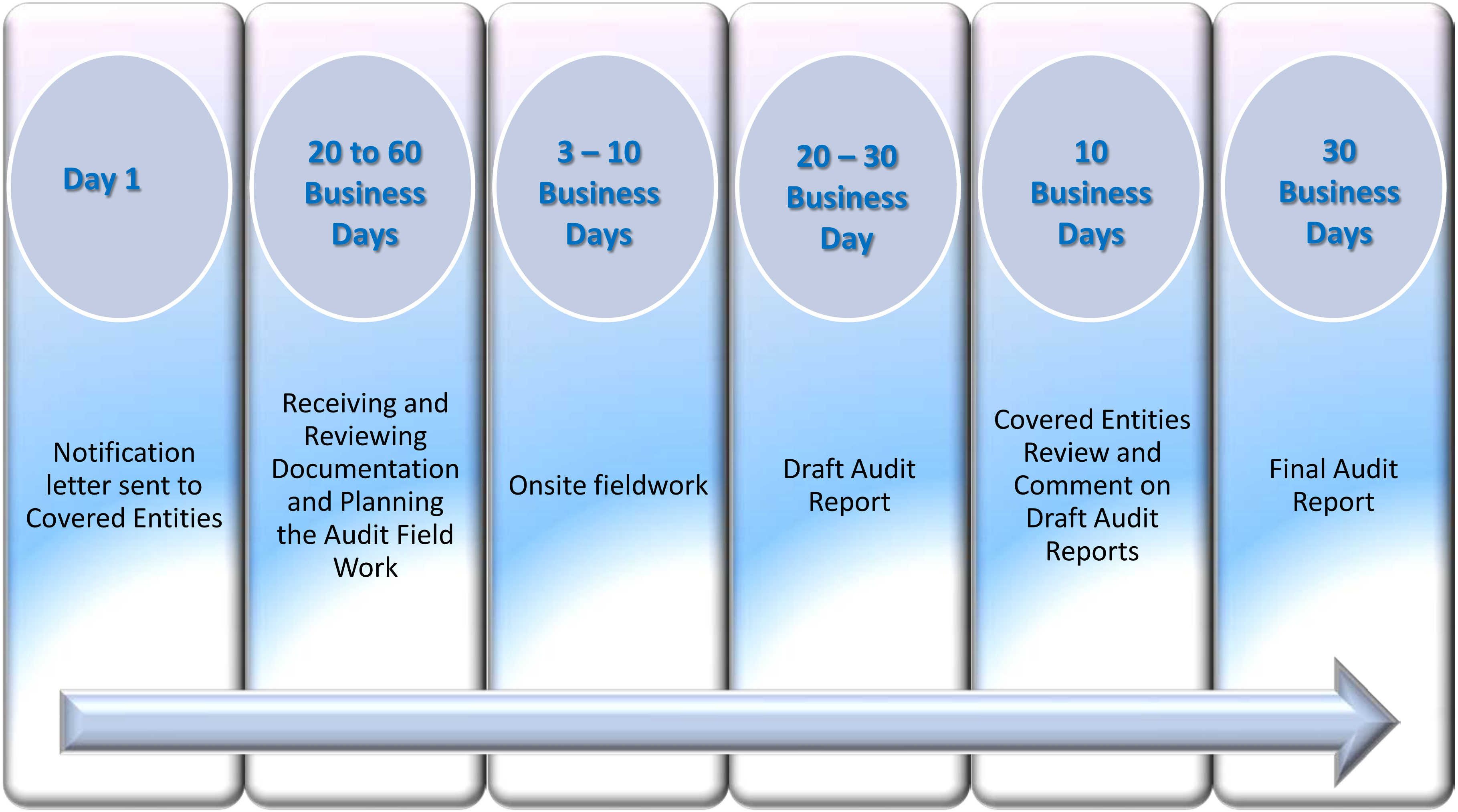
Period of Review/ Adjustment of Protocols

Audit Execution – Remaining Audits

# Who is being audited?

- Every covered entity and business associate is eligible for an audit.
- Selections in the initial round will be designed to provide a broad assessment of a complex and diverse health care industry.
- OCR is responsible for selection of the entities & will audit as wide a range of types and sizes of covered entities
- Business Associates will be included in future audits.

# Auditee Timeline



**Day 1**

Notification letter sent to Covered Entities

**20 to 60 Business Days**

Receiving and Reviewing Documentation and Planning the Audit Field Work

**3 – 10 Business Days**

Onsite fieldwork

**20 – 30 Business Day**

Draft Audit Report

**10 Business Days**

Covered Entities Review and Comment on Draft Audit Reports

**30 Business Days**

Final Audit Report

# After the Audits

- Audits are primarily a compliance improvement activity.
- OCR will review the final reports, including the findings and actions taken by the audited entity to address findings.
- The aggregated results of the audits will enable OCR to better understand compliance efforts in the industry
- OCR will use the audit reports to determine what types of technical assistance should be developed, and what types of corrective action are most effective, however
- Should an audit report indicate a serious compliance issue, OCR may initiate a compliance review to address the problem.
- OCR will not post a listing of audited entities or the findings of an individual audit which clearly identifies the audited entity.

# Summary

- How can you prepare?  Some key take aways…
  - Ensure the appropriate infrastructure is in place (policies, procedures, contingency plans, notice of privacy practices and other required documentation)
  - Hold an annual meeting with your teams and conduct training/awareness on Healthcare Privacy and Security
  - Understand where your PHI, ePHI exists and in what formats (reports, paper files, EMR, billing systems, laptops, hard drives)
  - Understand who has what access (employees, physicians, business associates)
  - Do a risk assessment (this is more than a simple check list approach)
  - Have a process in place when bad things happen

# Agenda

- HIPAA Title II
- HIPAA Privacy
- HIPAA Security
- HITECH Act Requirements
- Breach Notification
- OCR Audit Program

# First 20 Auditees

# 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***

***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

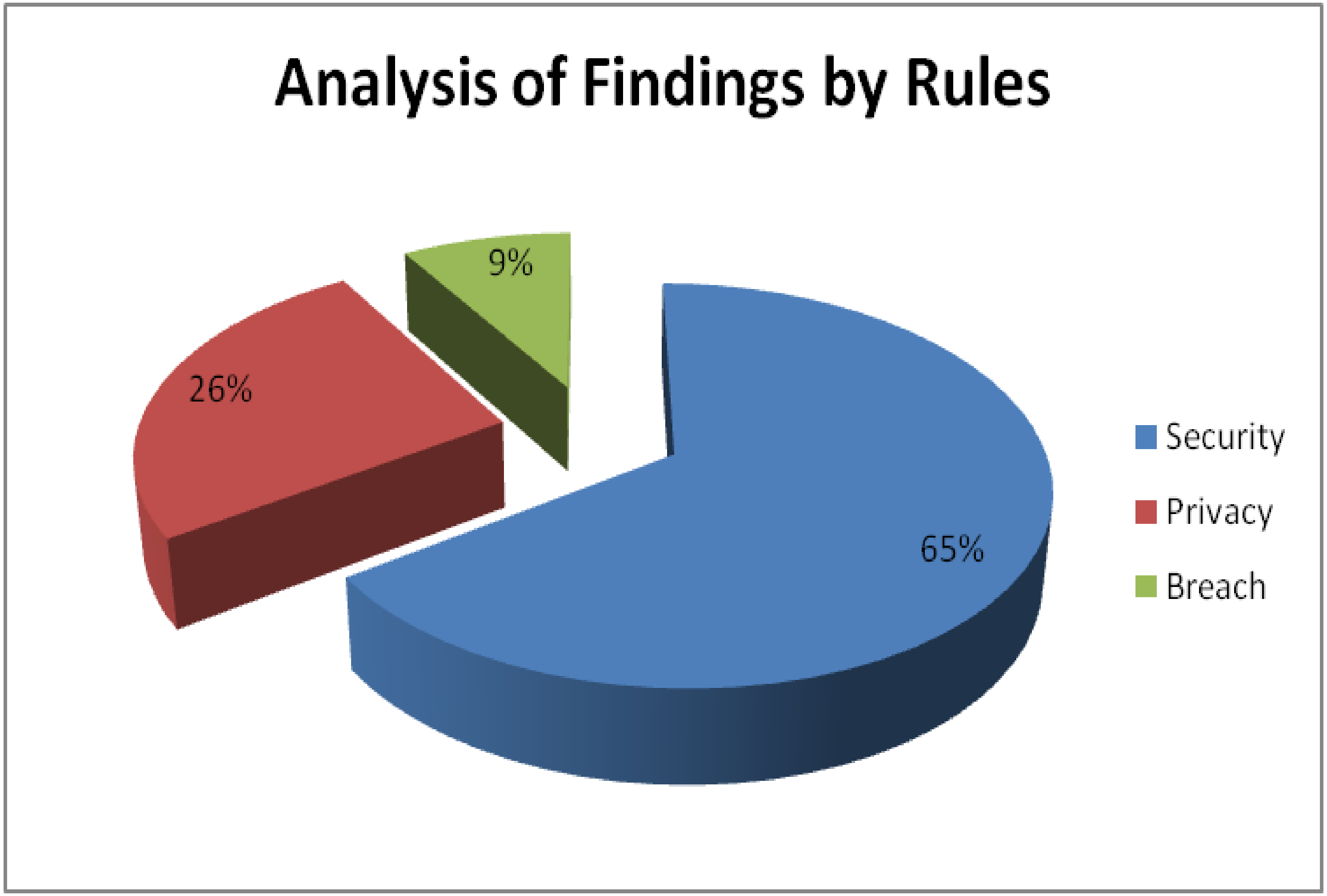
**Health Plans**

| | |
|---|---|
| Medicaid | 1 |
| SCHIP | 1 |
| Group Health | 3 |
| Health Insurance Issuer | 3 |

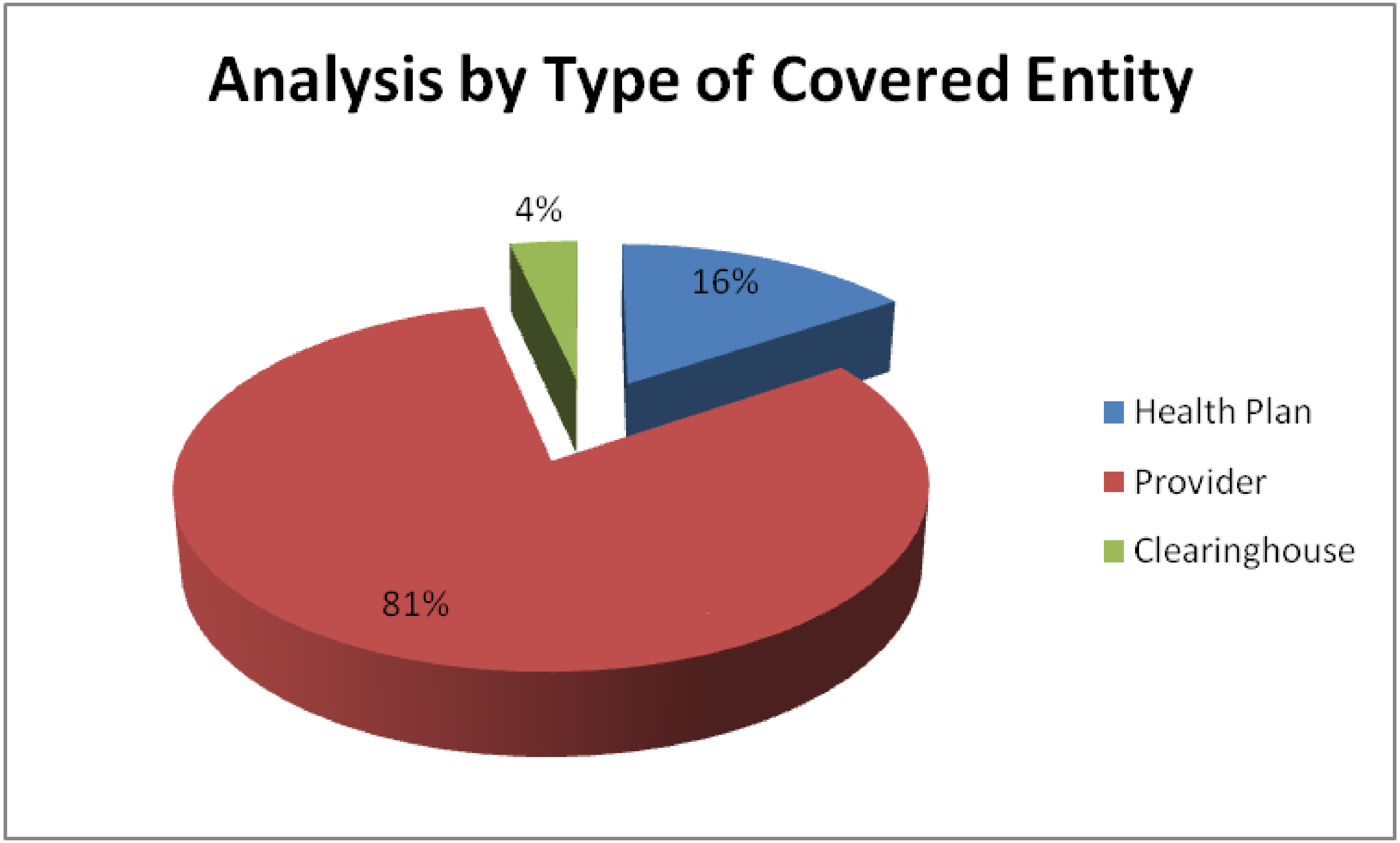
**Health Care Providers**

| | |
|---|---|
| Specialty Physicians | 3 |
| Hospitals | 3 |
| Laboratories | 1 |
| Dental | 1 |
| Nursing & Custodial Care Facilities | 1 |
| Pharmacy | 1 |

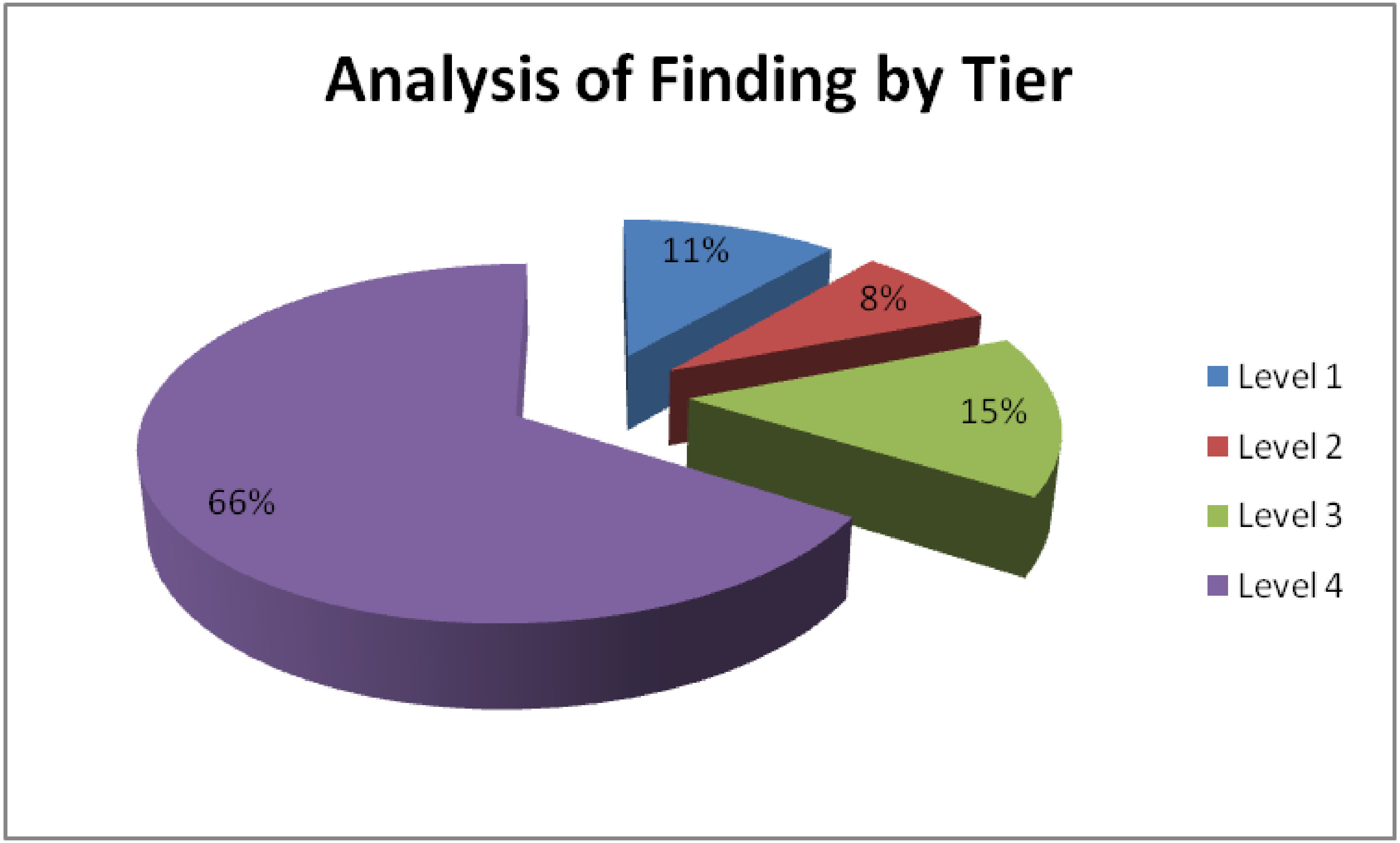
# Initial 20 Findings Analysis Overview



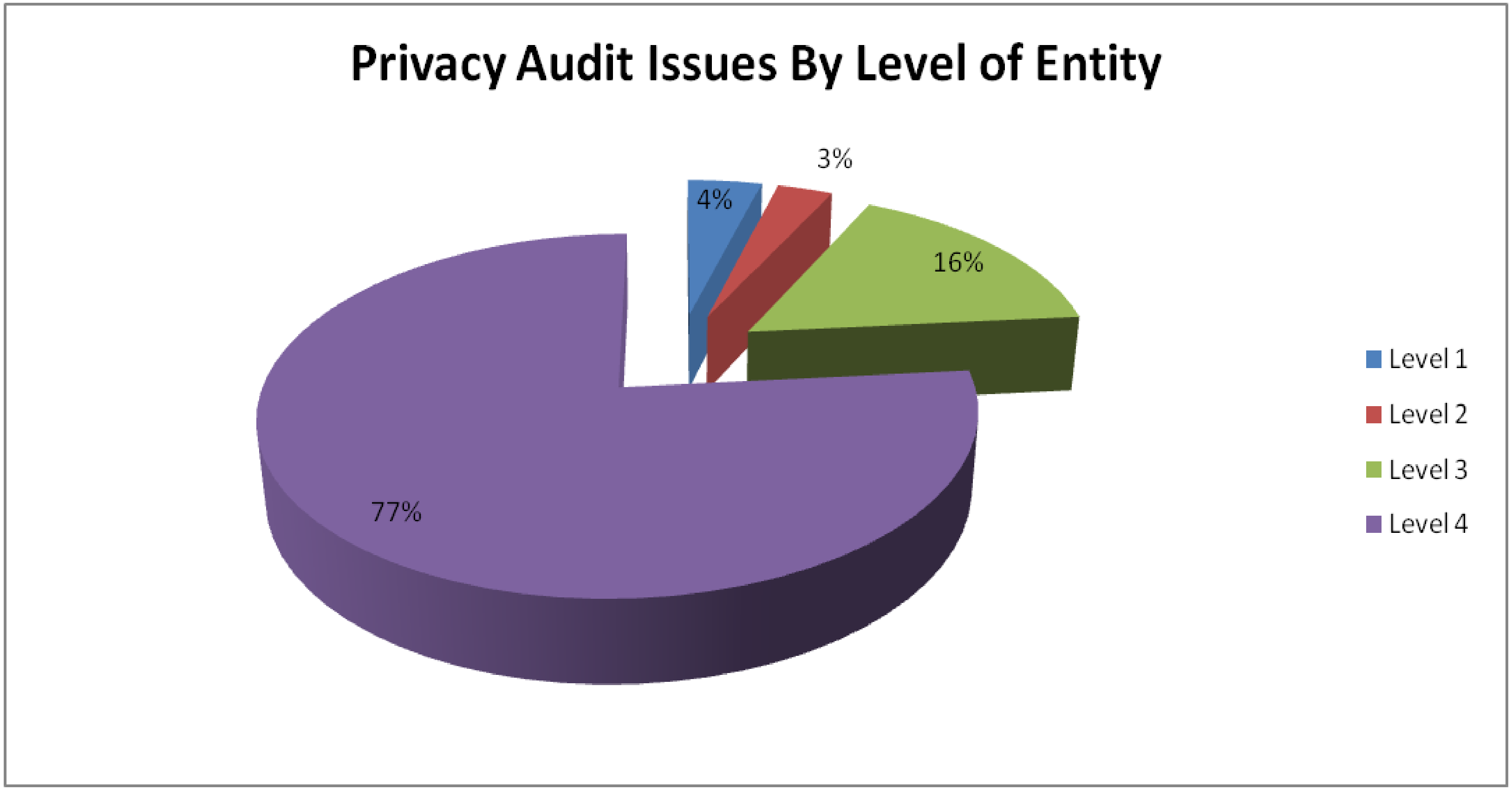
# Initial 20 Findings Analysis Overview



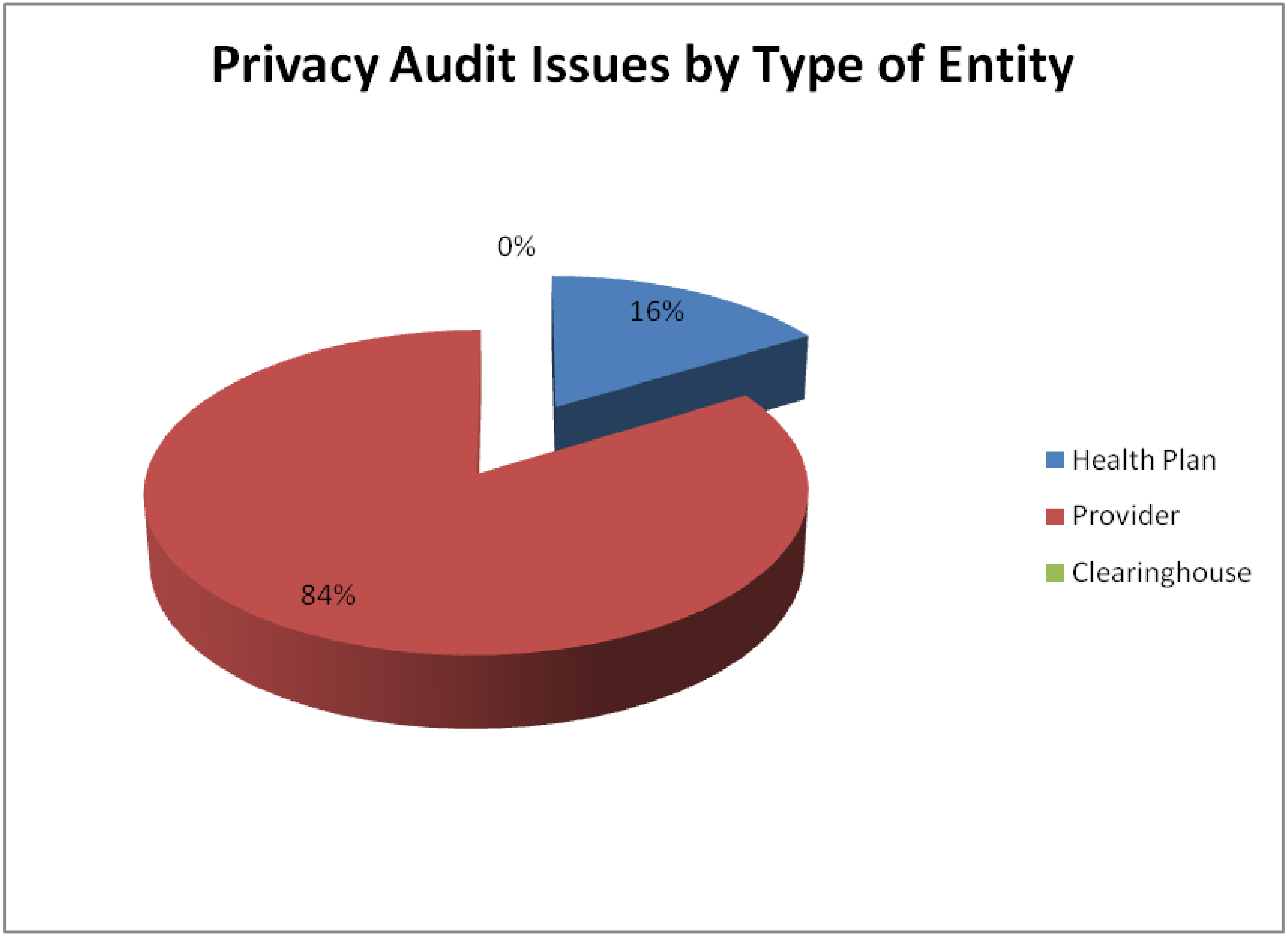
# Initial 20 Findings Analysis Overview



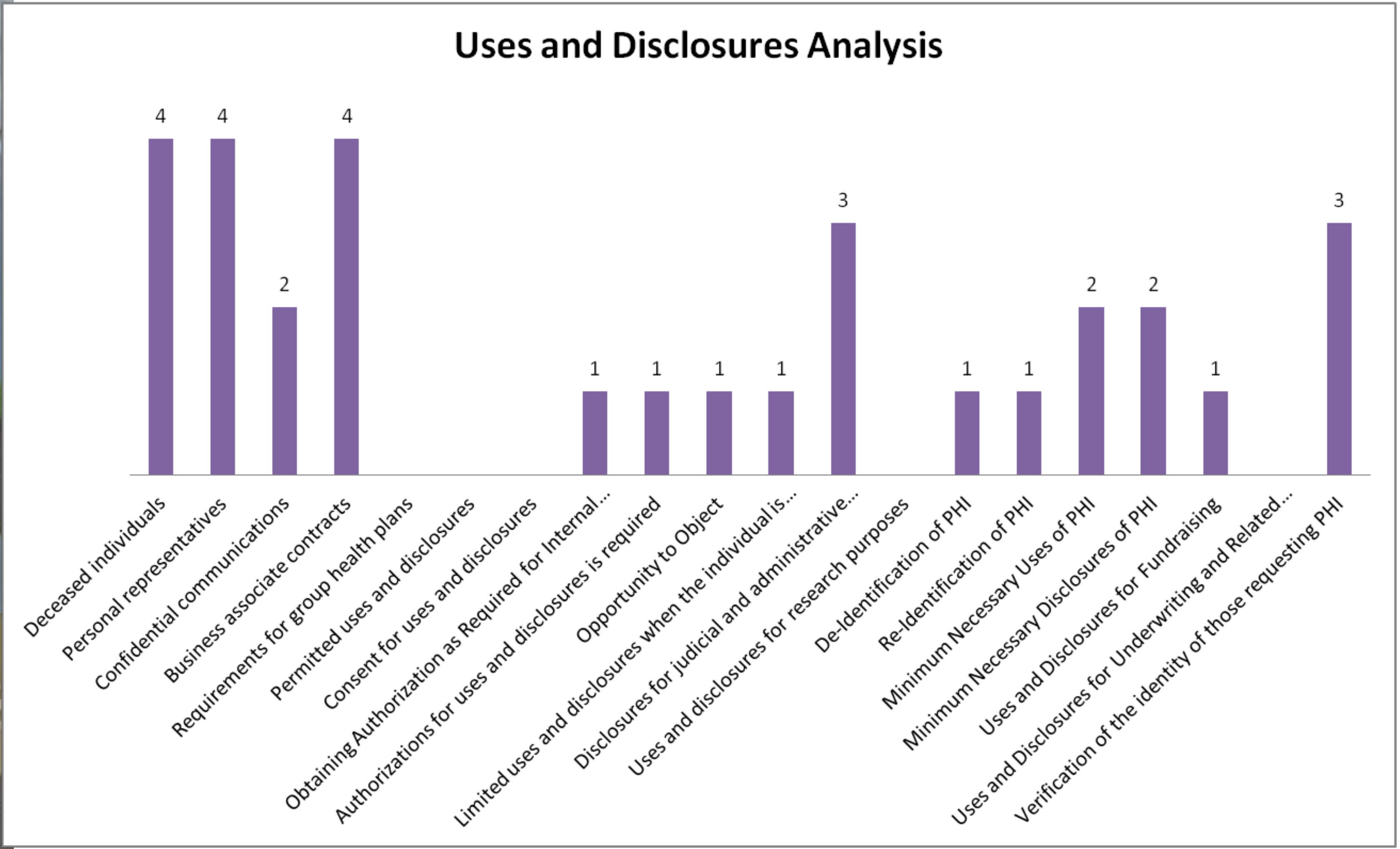
# Initial 20 Findings Analysis Privacy Issues



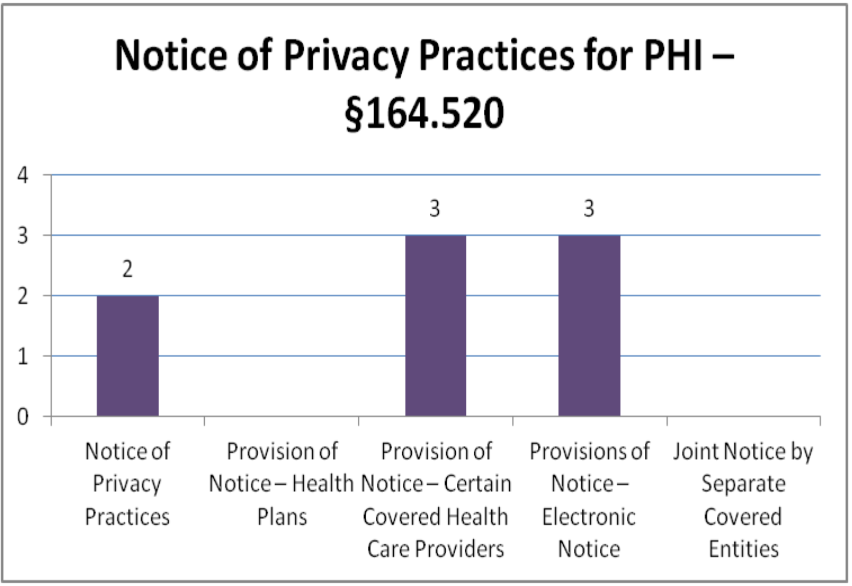
# Initial 20 Findings Analysis Privacy Issues

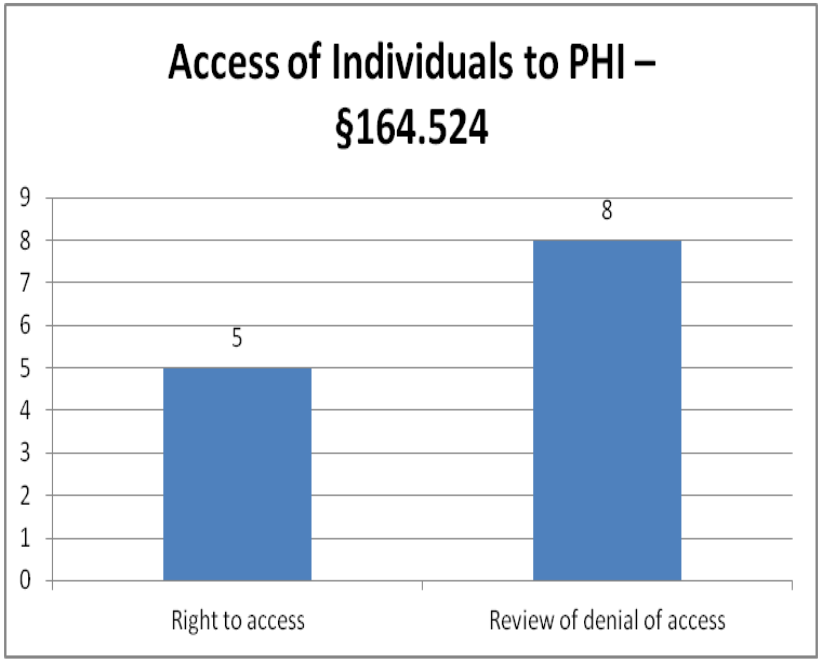


# Initial 20 Findings Analysis Privacy: Uses and Disclosures

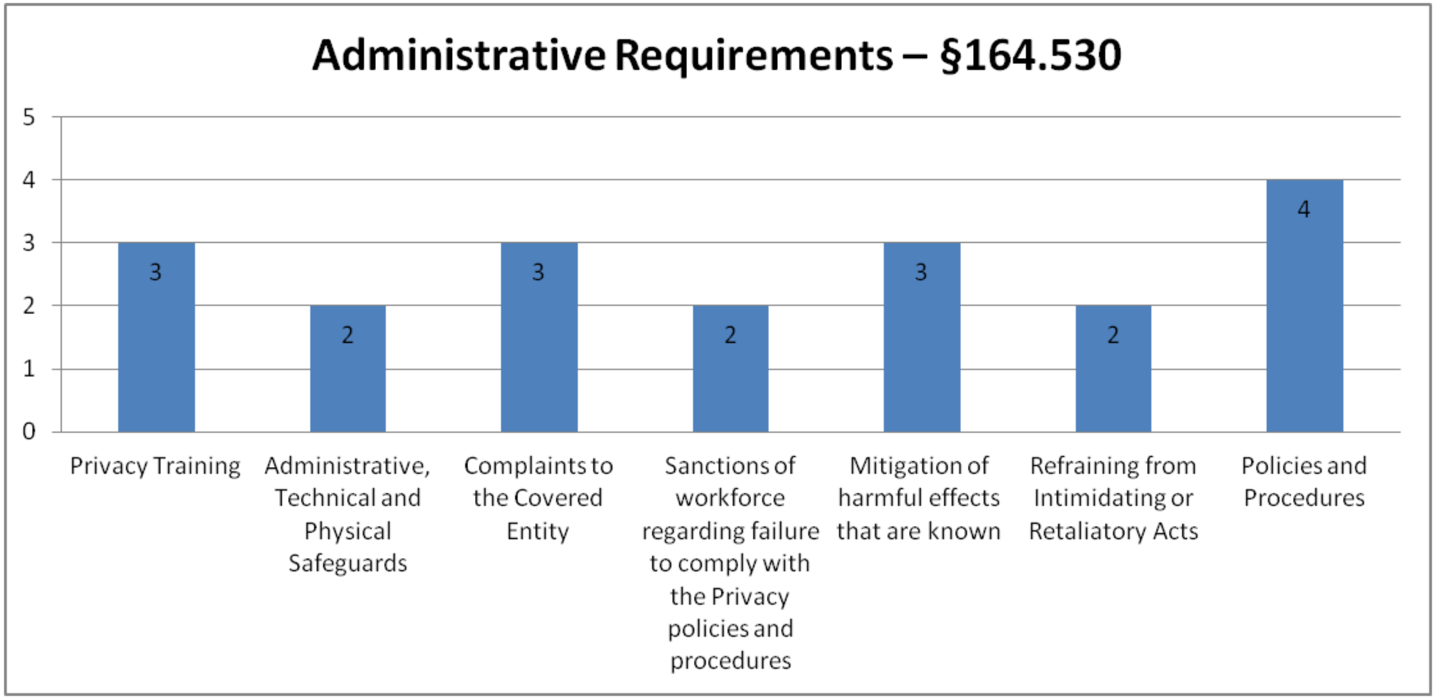


# Initial 20 Findings Analysis Privacy: Notice and Access

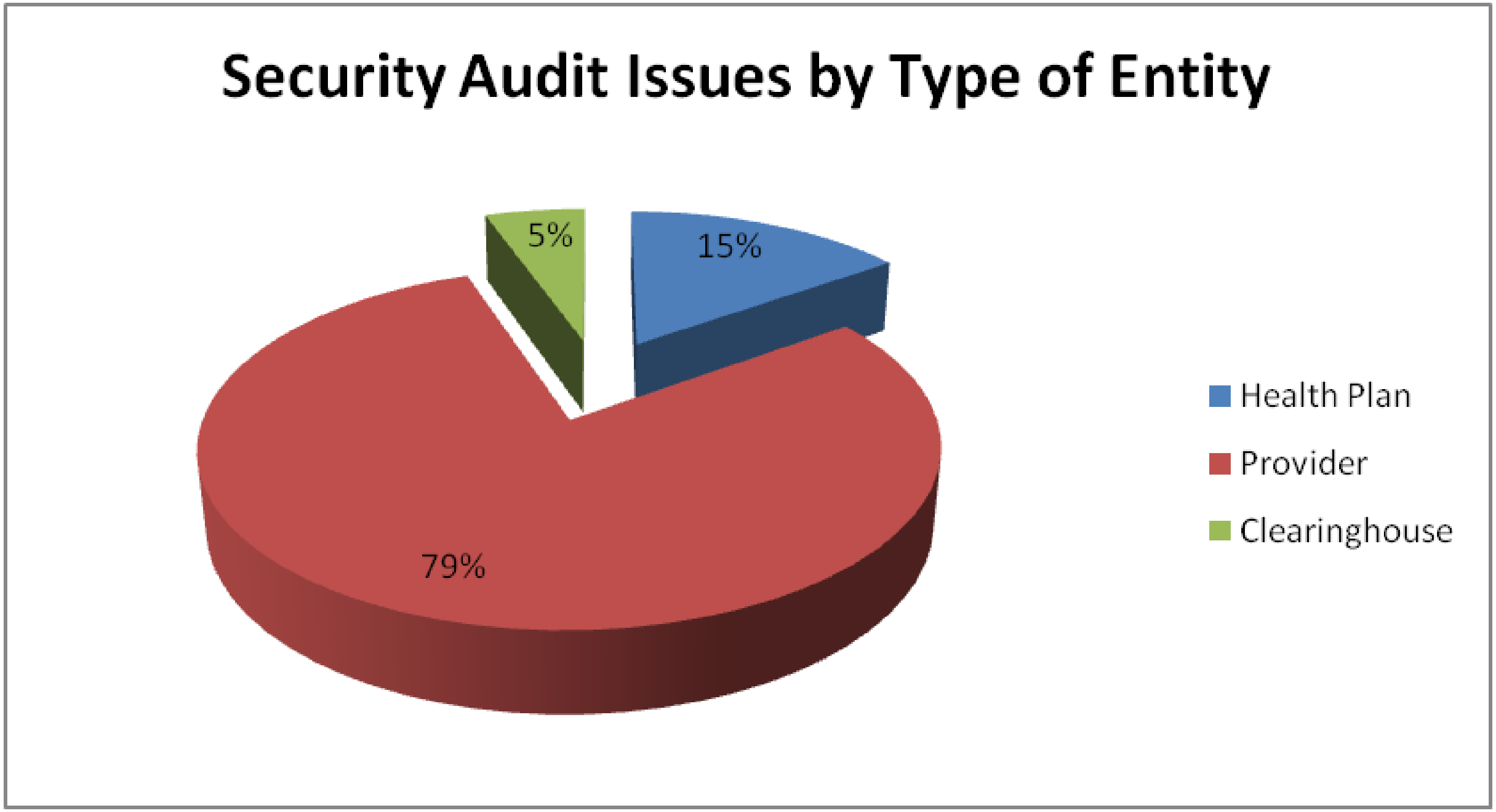

Notice of Privacy Practices for PHI – §164.520
4
3
2
1
0
2
3
3
Notice of Privacy Practices
Provision of Notice – Health Plans
Provision of Notice – Certain Covered Health Care Providers
Provisions of Notice – Electronic Notice
Joint Notice by Separate Covered Entities



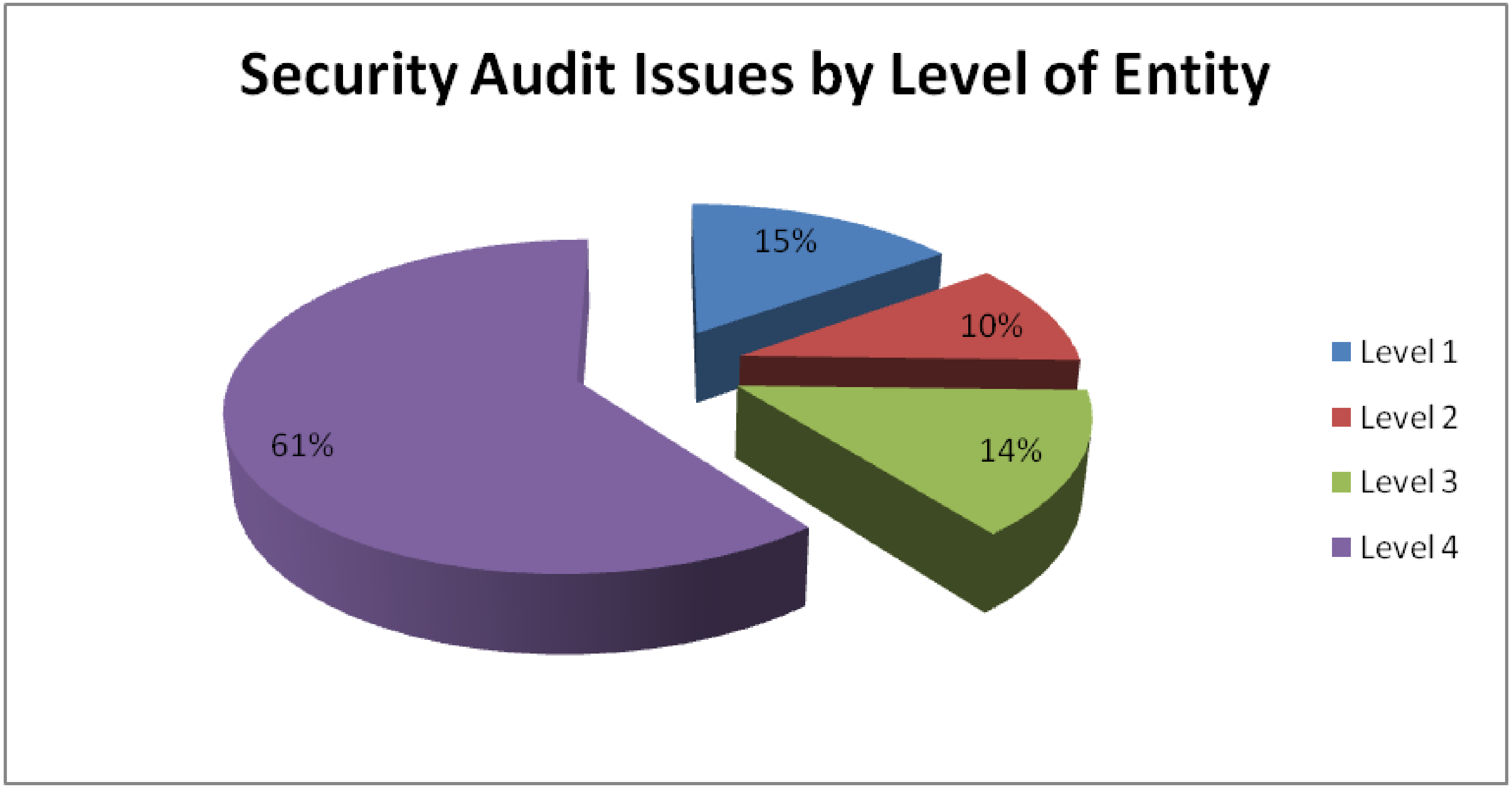
# Initial Findings Analysis Privacy: Administrative Requirements



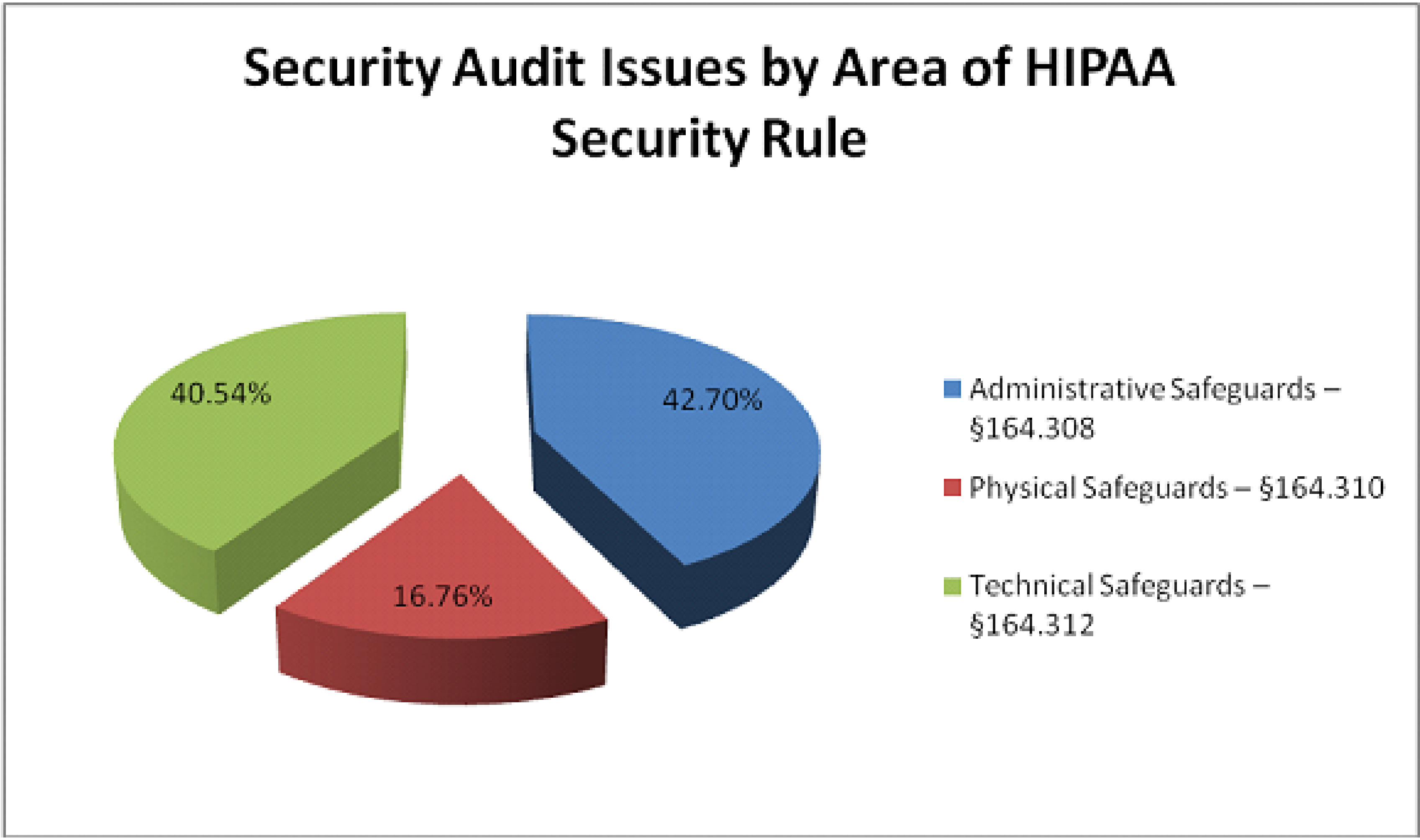
# Initial 20 Findings Analysis
# Security Issues



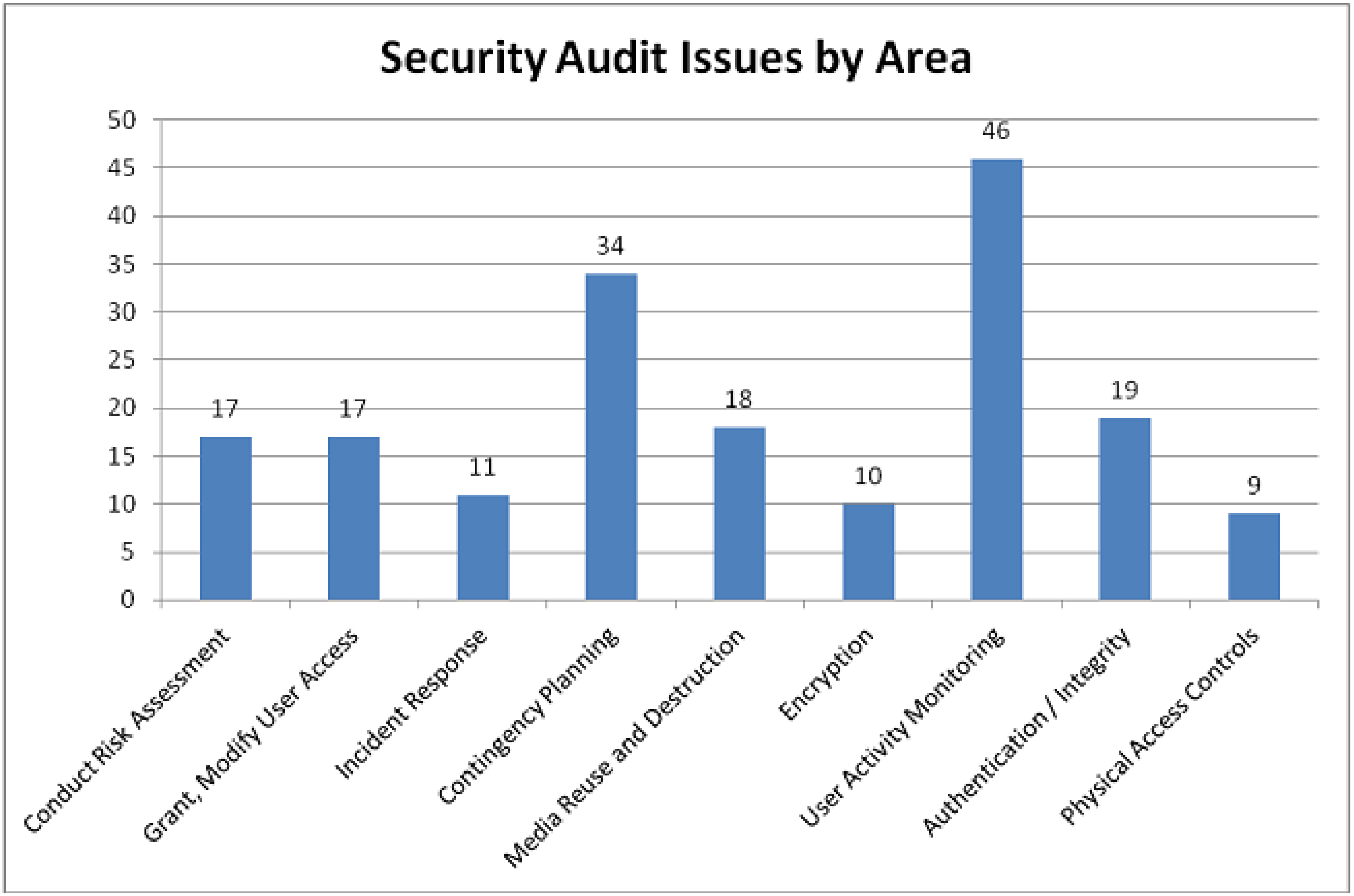
# Initial 20 Findings Analysis Security Issues



# Initial 20 Findings Analysis
# Security Issues



# Initial 20 Findings Analysis
# 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

# Next Steps to Consider

- Conduct a robust Assessment with an Annual or Bi-Annual reassessment for compliance
- Determine Lines of Business affected by HIPAA
- Consider internal employee information in evaluation
- Map/Flow PHI movement within your organization, as well as flows to/from third parties
- Perform Data discovery to find all of your PHI
- See guidance available on OCR web site

# Summary

- How can you prepare?  Some key take aways…
  - Ensure the appropriate infrastructure is in place (policies, procedures, contingency plans, notice of privacy practices and other required documentation)
  - Hold an annual meeting with your teams and conduct training/awareness on Healthcare Privacy and Security
  - Understand where your PHI, ePHI exists and in what formats (reports, paper files, EMR, billing systems, laptops, hard drives)
  - Understand who has what access (employees, physicians, business associates)
  - Do a risk assessment (this is more than a simple check list approach)
  - Have a process in place when bad things happen

# Conclusions & Final Thoughts

- Plan ahead for impact of HIPAA across the organization
    - Determine possible common responsibilities and oversight of IT, Information Security, and Internal Audit
    - Assess overlap between controls oversight and management
- Determine control and safeguard catalogue for HIPAA prior to remediation – know what you’re going after
- Engage affected departments (IT, HR, Business, IA) early in the planning
- Assess your ability to combine HIPAA compliance activities with other compliance activities like PCI, (Unified Compliance), to increase the effectiveness & efficiency of your compliance programs

# *Q&A*

# Presenter Contact Info

Mari Turvey
mturvey@kpmg.com
415-297-6274
Doron Rotman
drotman@kpmg.com
650 868-8880