



HIPAA Privacy, Security and Breach Notification Audits

Program Overview & Initial Analysis

Linda Sanches, MPH

HCCA 2013 Compliance Institute

April 23, 2013



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

HCCA April 23, 2013
3

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

HCCA April 23, 2013
4



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)

HCCA April 23, 2013

5



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)

HCCA April 23, 2013

6



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

HCCA April 23, 2013

7

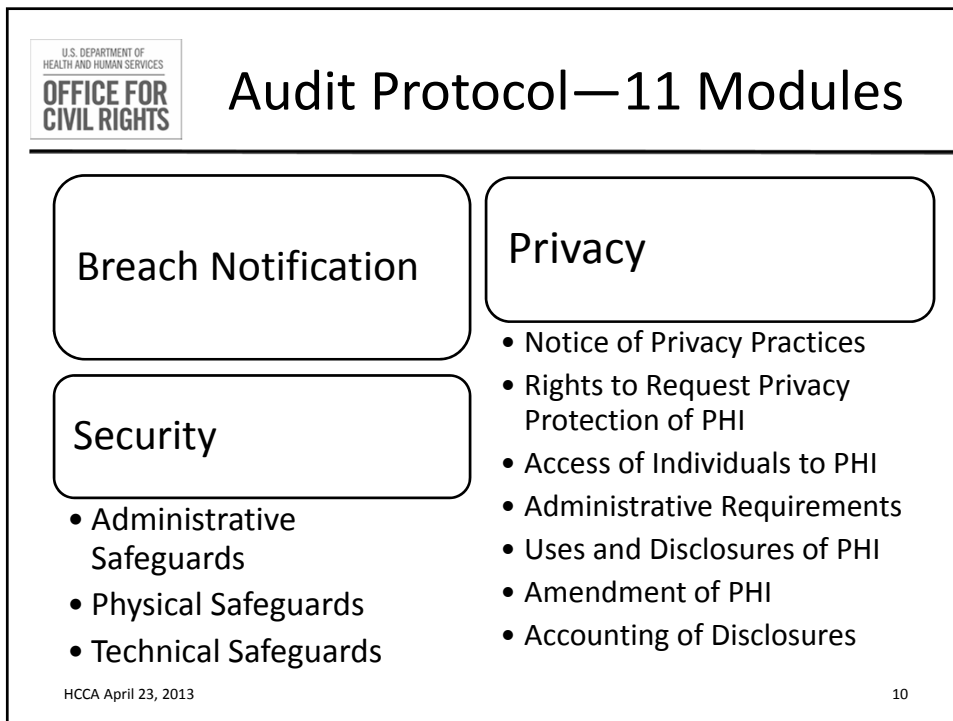
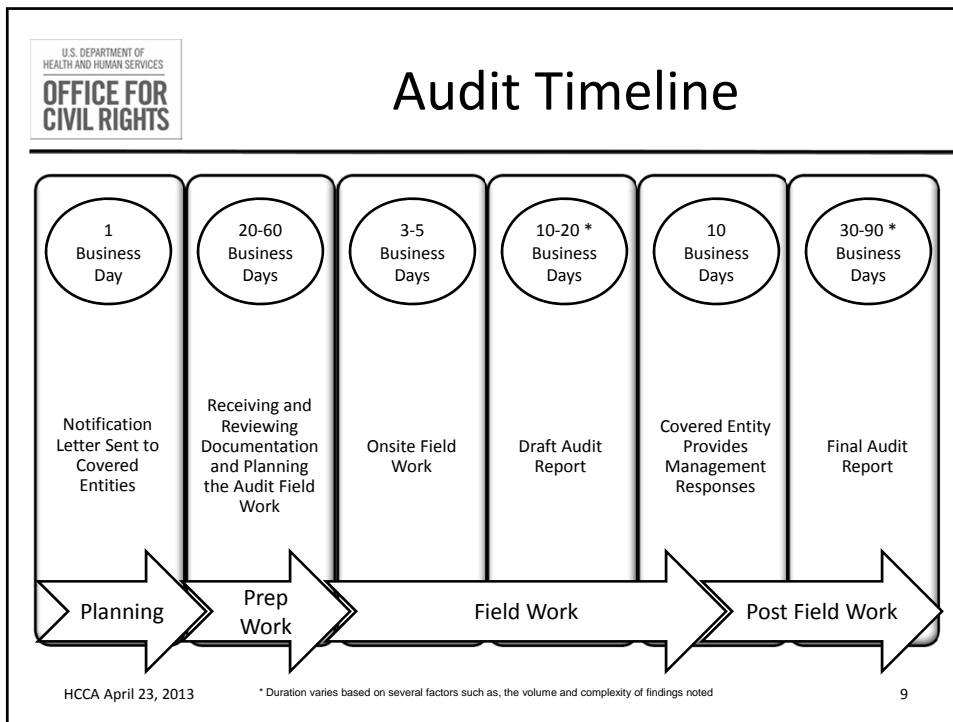


Auditees by Type & Size

	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

HCCA April 23, 2013

8



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

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.

HCCA April 23, 2013
11

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

2) Audit Testing Procedures

3) W/P Ref.

4) Applicability

<p><small>§164.508 - Uses and disclosures for which an authorization is required</small></p> <p><small>§164.508(b) (6) A covered entity must document and retain any signed authorization under this section as required by §164.530(j).</small></p> <p><small>§164.508(c) (1) A valid authorization must contain core elements.</small></p> <p><small>§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:</small></p> <ul style="list-style-type: none"> (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. <p><small>§164.508(c) (3) The authorization must be written in plain language.</small></p> <p><small>§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.</small></p> <p><small>§164.508(b)(1)(ii) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (c) (1), and (c) (2) of this section, applicable.</small></p> <p><small>(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.</small></p> <p><small>§164.508(b)(2) An authorization is not valid, if the document submitted has any of the following defects:</small></p> <ul style="list-style-type: none"> (i) The expiration date 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. <p><small>Require of management as to whether a process exists to determine when authorization is required</small></p> <p><small>Obtain and review a sample of instances where authorization is required to determine if a valid authorization was obtained:</small></p> <p><small>Evidence that an authorization was valid.</small></p> <p><small>For providers only: obtain and review all patient intake forms for both inpatient and outpatient services, including consent and authorization forms, if any.</small></p>	<p>Applicability:</p> <p>Provider <input type="checkbox"/></p> <p>Health Plan <input type="checkbox"/></p> <p>Group Health Plan (GHP) <input type="checkbox"/></p> <p>GHP with a Full Service TPA <input type="checkbox"/></p> <p>Fully Insured GHP <input type="checkbox"/></p> <p>Clearinghouse <input type="checkbox"/></p> <p>Clearinghouse (164.508(b)) <input type="checkbox"/></p> <p style="font-size: 8px; margin-top: 10px;">If None, indicate why (1)(i) per COC, this section of the Rule does not apply to fully insured group health plans. Refer to HIP reference 100.</p>
<p><small>EF-500.FF</small></p>	<p><small>EF-500.FF1</small></p> <p><small>EF-500.FF2</small></p> <p><small>EF-500.FF3</small></p>

HCCA April 23, 2013
12



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.

HCCA April 23, 2013

13



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.

HCCA April 23, 2013

14

U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES

OFFICE FOR
CIVIL RIGHTS

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

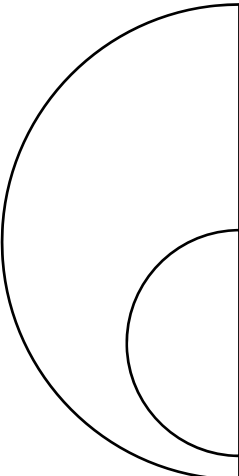
HCCA April 23, 2013

15

U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES

OFFICE FOR
CIVIL RIGHTS

Program Deliverables



Final Audit Reports

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

Leading Practices

HCCA April 23, 2013

16



Exceptions Affect Audit Scope

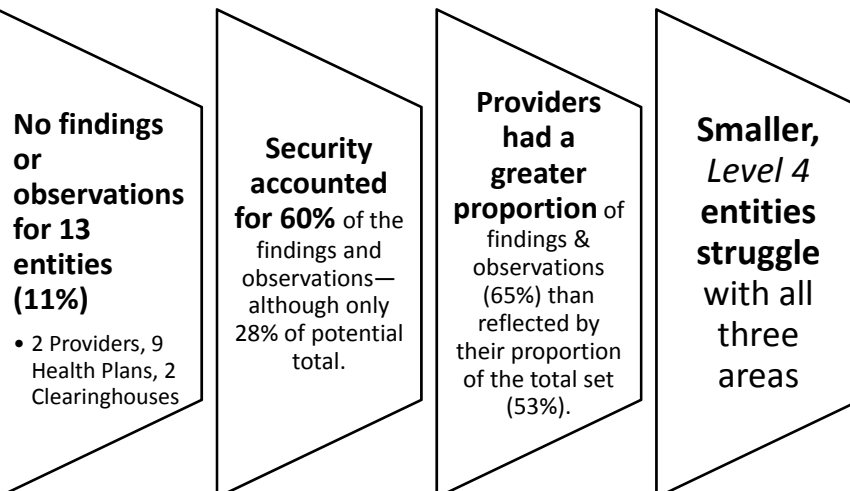
- What did we audit? Varied by type of entity.
- Exceptions to certain requirements applied to several audited entities
 - 6 of the 7 clearinghouses asserted they only act as a business associate to other covered entities; in accordance with §164.500(b) few privacy procedures applied
 - 8 of the 47 health 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.

HCCA April 23, 2013

17



Overall Findings & Observations



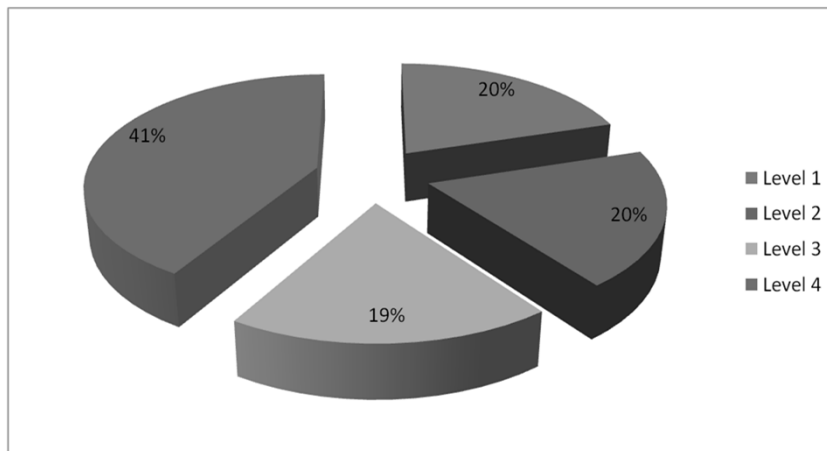
HCCA April 23, 2013

18



Audit Findings & Observations By Level

AUDIT FINDINGS AND OBSERVATIONS BY LEVEL OF ENTITY

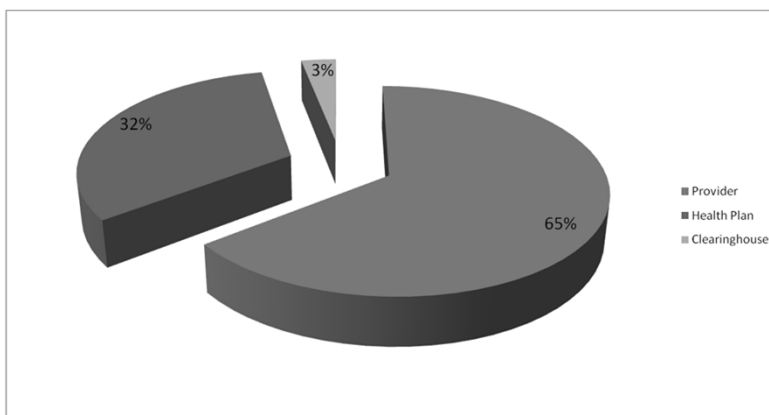


HCCA April 23, 2013

19



Proportional by Entity Type



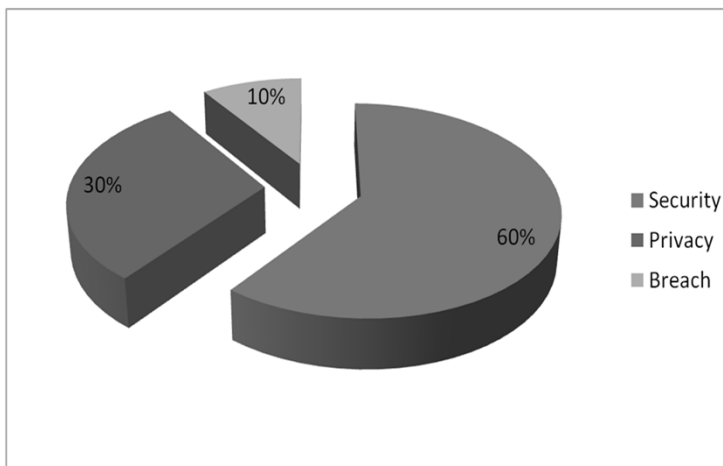
AUDIT FINDINGS AND OBSERVATIONS BY TYPE OF COVERED ENTITY

HCCA April 23, 2013

20



Proportional Findings by Rule



Audit Findings and Observations by Rule

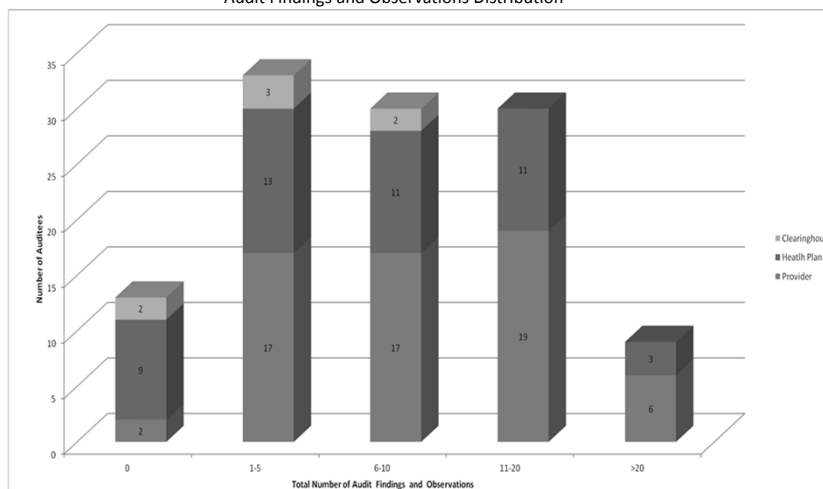
HCCA April 23, 2013

21



Element Exposure by Entity Type

Audit Findings and Observations Distribution

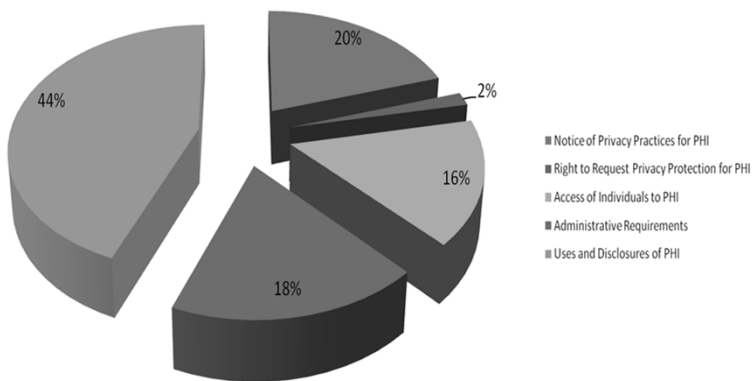


HCCA April 23, 2013

22

Privacy Findings & Observations

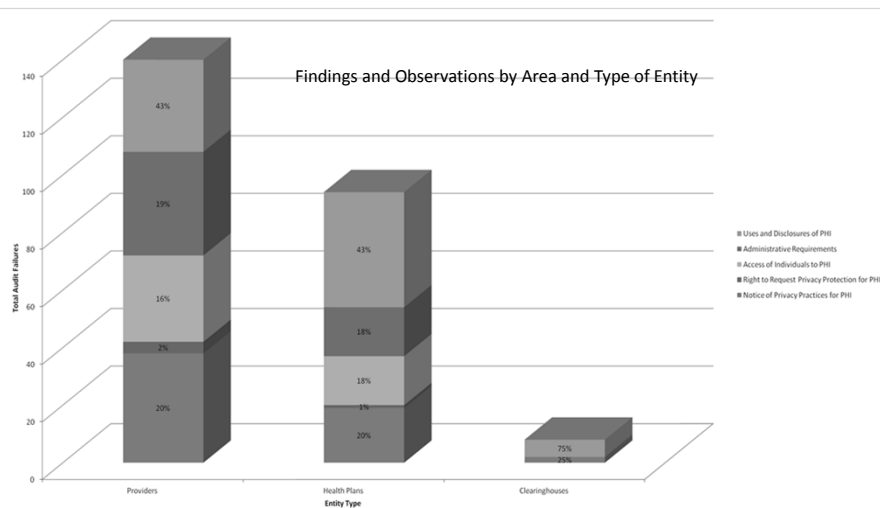
PERCENTAGE OF FINDINGS AND OBSERVATIONS BY AREA OF FOCUS



HCCA April 23, 2013

23

Privacy Results by Entity Type

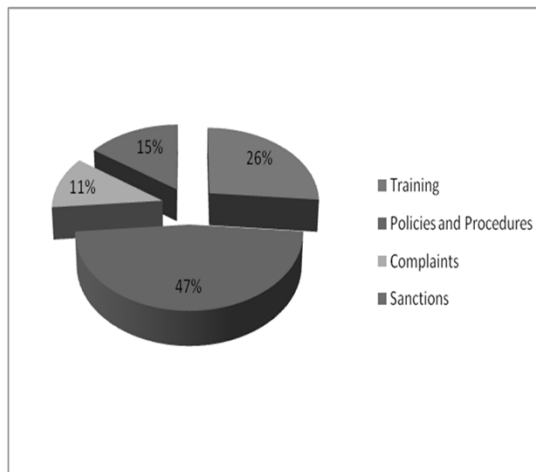


HCCA April 23, 2013

24

Privacy Administrative Elements

ADMINISTRATIVE REQUIREMENTS FINDINGS AND OBSERVATIONS

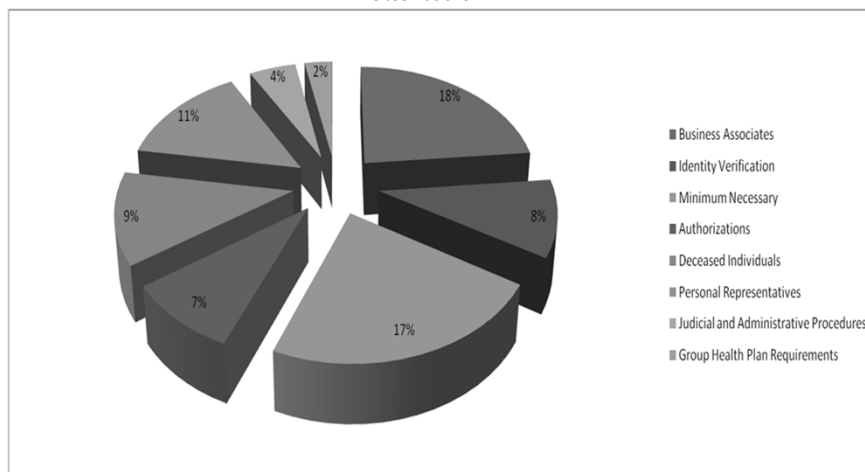


HCCA April 23, 2013

25

Privacy -- Uses and Disclosures

Uses and Disclosures of PHI Findings and Observations



HCCA April 23, 2013

26

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: Almost every entity without a finding or observation met by fully implementing the addressable specification.

HCCA April 23, 2013

27

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE FOR CIVIL RIGHTS

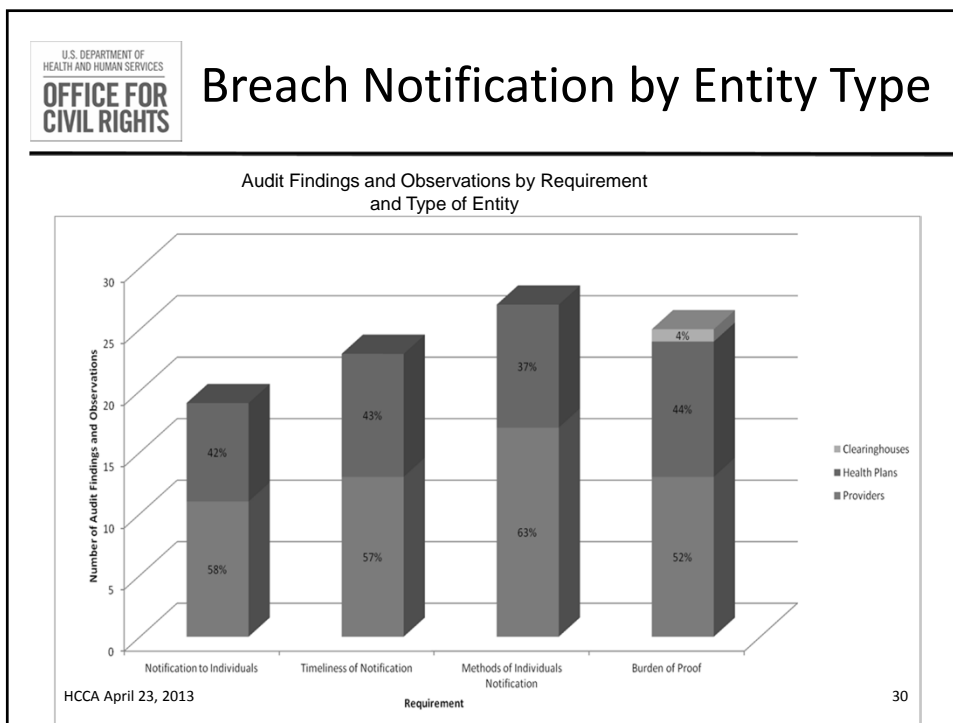
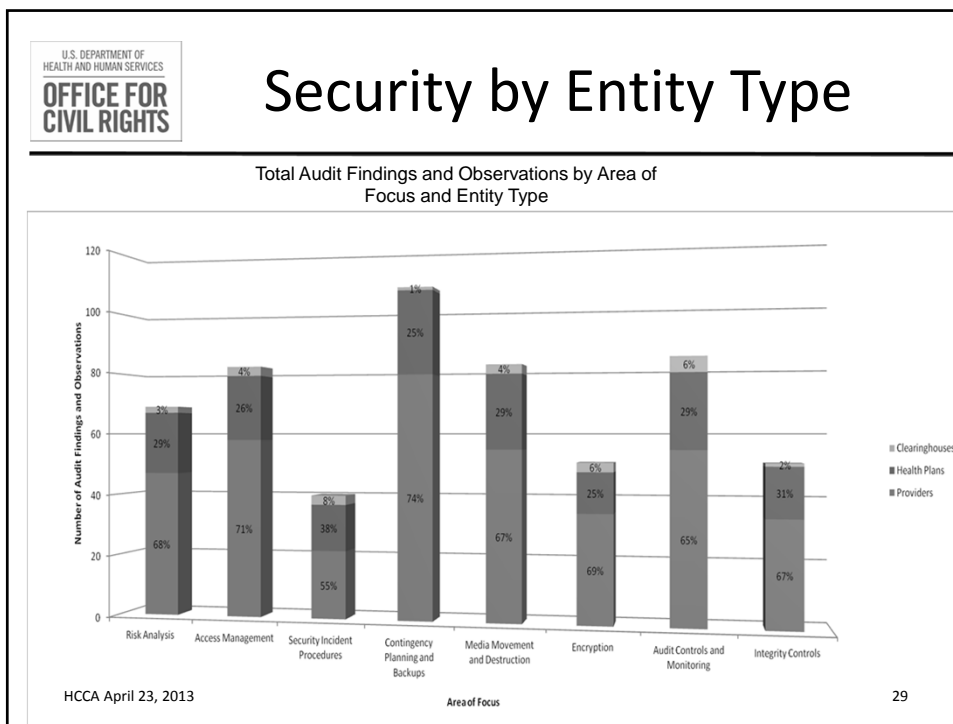
Security Elements

Percentage of Audit Findings and Observations by Area of Focus

Area of Focus	Percentage
Risk Analysis	12%
Access Management	14%
Security Incident Procedures	14%
Contingency Planning and Backups	7%
Workstation Security	18%
Media Movement and Destruction	4%
Encryption	8%
Audit Controls and Monitoring	14%
Integrity Controls	9%
(Unlabeled)	14%

HCCA April 23, 2013

28





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

HCCA April 23, 2013

31



Cause Analysis – Top Elements *Unaware of the Requirement*

Privacy

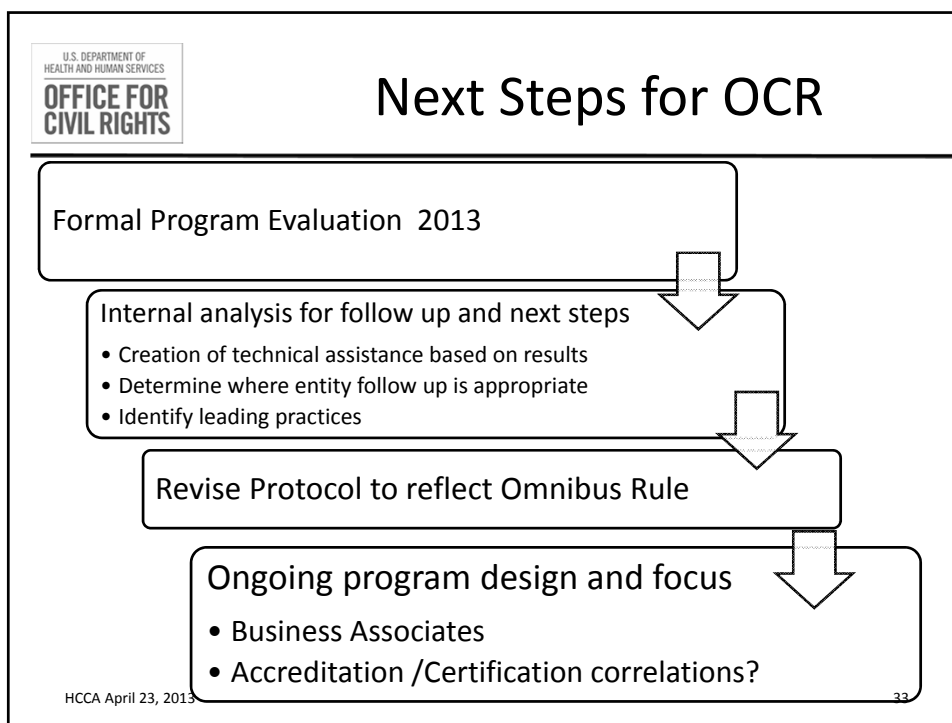
- Notice of Privacy Practices;
- Access of Individuals;
- Minimum Necessary; and,
- Authorizations.

Security

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

HCCA April 23, 2013

32



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/>

Linda Sanches linda.sanches@hhs.gov

HCCA April 23, 2013 34