OCR Is Coming! Be Prepared for OCR Audits and Breach Investigation


Presented by: **Andrew Mahler, JD, CIPP/US, CHRC**
HIPAA Privacy Officer
The University of Arizona

John Bailey, JD
HIPAA Privacy Officer
St. Jude Children's Research Hospital

About Us


- **Andrew Mahler, JD, CIPP/US, CHRC**
  - HIPAA Privacy Officer, The University of Arizona (2013-Present)
  - OCR Investigator, Region IV (2011-2013)
    - Investigated/closed hundreds of cases
    - Drafted data requests, closures, settlement agreements
    - Regional representative, OCR Academy of Civil Rights Investigators (2012)
- **John Bailey, JD**
  - HIPAA Privacy Officer, St. Jude Children's Research Hospital (2012-Present)
  - OCR Investigator, Region IV (2009-2012)
    - Investigated/closed hundreds of cases
    - Drafted data requests, closures
    - Conducted on-site investigations and interviews

Agenda

1. Background: The Breach Notification Rule and Updates
2. OCR Investigations
3. History: OCR Audits
4. OCR Audits: Phase II
5. Questions?

**The information provided in this presentation does not constitute legal advice and is intended to be used for guidance. The opinions and comments expressed during this presentation are those of the speakers and not of HHS/OCR, St. Jude Children's Research Hospital or The University of Arizona.*

Breach Notification Rule: Basics

Breach

- "Breach" means the acquisition, access, use or disclosure of protected health information (PHI) which compromises the security or privacy of the information.
- "Unsecured Protected Health Information" (UPHI) means PHI that is not unusable, unreadable, or indecipherable to unauthorized persons.
- 3 Exceptions:
  1. Unintentional use by workforce member ("good faith," scope of authority);
  2. Inadvertent disclosure by a CE/BA to another CE/BA;
  3. "Good faith belief" that the unauthorized person cannot retain.

45 CFR § 164.402(1)

Breach

- Omnibus changed the standard!
- Risk of harm?
- A breach is presumed *unless* a CE can demonstrate that there is a low probability that the data has been compromised.

Risk Assessment (Not Analysis)

- Has PHI been breached or compromised?
- A Breach is "discovered" by a CE or by a BA as of the first day on which such a Breach is known or by exercising reasonable diligence would have been known.
- Assessment:
  1. Nature and extent of PHI involved;
  2. Who received/accessed information;
  3. Potential that PHI was actually viewed or acquired; and
  4. Extent to which the risk to the data has been mitigated.

45 CFR § 164.402(2)

Breach Notification

- The notice shall include the identification of each individual whose UPHI has been or reasonably believed by the BA to have been accessed, acquired, or disclosed during such Breach.
- All notifications shall be without unreasonable delay and no later than **60 calendar days** after discovery of a Breach. The CE or BA has the burden of proof demonstrating that all notifications met such requirements including the necessity of any delay.

45 CFR § 164.404(a)

Content of Notification

1. A brief description of what happened, including date of breach and discovery date;
2. Description of types of UPHI;
3. Steps individuals can take to protect themselves;
4. A brief description of what the CE is doing to mitigate harm;
5. Contact information for individuals to ask questions;
6. Plain language!

45 CFR § § 164.404-164.408

Breach Notification

1. Written notification by first class mail to the individual

2. Special rule for out of date contact information
3. Emergency situation
4. Deceased individual

Breaches affecting less than 500

- Notice to Individual
- Notice to the Secretary
- Omnibus change: discovered vs. occurred

Breaches affecting more than 500

- Notice to the Individuals
- Notice to the Media
- Notice to the Secretary
- “Wall of Shame”

State Breach Notification Laws

- **State law:** Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.
- **PII (TN Code example)**: Personal Identification Information (PII) means an individual's first name or first initial and last name in combination with any one or more of the following data elements: (1) Social security number; (2) Driver's license number or Tax ID number; (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (4) Medical information; or (5) Health insurance information.

Once Breach Notification is Submitted

- Secretary receives report
- Prepare for the possibility of an OCR investigation!

New CMP Structure Under HITECH

VIOLATION TYPE	MIN. PENALTY	MAX. PENALTY
Did Not Know	$100/violation; annual max of $25,000/repeat violations	$50,000/violation; annual max of $1,500,000
Reasonable Cause	$100/violation; annual max of $[illegible]/repeat violations	$50,000/violation; annual max of $1,500,000
Willful Neglect – Corrected	$10,000/violation; annual max of $250,000/repeat violations	$50,000/violation; annual max of $1,500,000
Willful Neglect – Not Corrected	$50,000/violation; annual max of $1,500,000	$50,000/violation; annual max of $1,500,000

The new penalty structure is as follows:

VIOLATION TYPE	EACH VIOLATION	REPEAT VIOLATIONS/YR
Did Not Know	$100 – $50,000	$1,500,000
Reasonable Cause	$1,000 – $50,000	$1,500,000
Willful Neglect – Corrected	$10,000 – $50,000	$1,500,000
Willful Neglect – Not Corrected	$50,000	$1,500,000

Other Costs

- $$$ for location services and US Mail;
- Countless employee hours;
- Employee sanctions;
- Increased expense to fast track encryption;
- Establish a call center;
- Credit monitoring;
- May take years to close investigation;
- Name in Press.

Post-Breach:
Preparing for an Investigation/Audit by OCR

About OCR

- The Office for Civil Rights (OCR)
  - U.S. Department of Health & Human Services civil rights and health privacy rights law enforcement agency
  - Mission:
    - Enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security and Breach Notification Rules;
    - Ensuring that the privacy practices of several million health care providers, plans, and clearinghouses adhere to Federal privacy requirements under the Health Insurance Portability and Accountability Act (HIPAA).;
    - Ensuring that the more than 245,000 recipients of Federal financial assistance comply with the nation's civil rights laws;
    - Annually resolving more than 10,000 citizen complaints alleging discrimination or a violation of HIPAA.

OCR Investigations

1. OCR receives a complaint, breach notification, or other report (media, etc.)
2. Valid allegations?
   - Incidental disclosure?
   - Timely?
   - No valid allegation?
   - Investigator may review CE website.
3. Strategy sent to management (OCR)

OCR Investigations

1. Data Request Letter drafted, approved, sent to CE.
2. Investigator may contact CE (Privacy Officer) by phone or email (but may not). Verify people in your organization know who to go to with a letter!
3. Short time frame for CE to respond.
4. Response from OCR can range from closure to technical assistance, to an on-site visit and settlement.

Preparation

- Policies and procedures
  - Have they been updated?
- Internal investigation
  - Document, document, document!
  - Counsel?
  - Do you/your employees know who to go to?
- Sanction offending employee(s)
  - Policy?
  - HR, Legal?
- Retrain staff
  - Document, document, document!

If You Receive a Letter from OCR

- Engage OCR and the issue immediately.
  - Consider engaging outside counsel
- Don't be afraid to contact the investigator; you might learn something helpful!
- Ask!
  - Ask for an extension;
  - Ask questions; BUT
  - Avoid arguing, debating, etc. with the investigator
- Spell HIPPO correctly!

Possible Items Requested by OCR

- Internal Investigation and incident report (assessment);
- Proof of corrective action;
- **Policies and Procedures** (use and disclosures, minimum necessary, safeguards, security incident, access controls, authentication, technical safeguards, physical safeguards, secure passwords, etc.);
- Proof of any **sanctions** against employees;
- Retraining Employees (proof of logs);
- Copy of Risk Analysis;
- Actions to mitigate risk;
- **Proof of Training** (copy of training and privacy/security logs);
- Proof of notification to affected individuals;

Possible Items Requested by OCR

- Evidence of mitigation (credit monitoring services, credit reporting for credit freeze);
- Security measures to reduce risks;
- Evidence of physical safeguards (physical security, photos);
- Encryption (screenshots of configuration settings), complete list of encrypted laptops;
- Copy of letter of affected individuals (US mail);
- List of letters that were returned;
- Copy of Press Release, if applicable;
- Copy of Risk Management plan;
- Documentation that effectuated substitute notice;
- Proof of Accounting in the affected individuals disclosure log;
- Network diagrams (physical and logical).

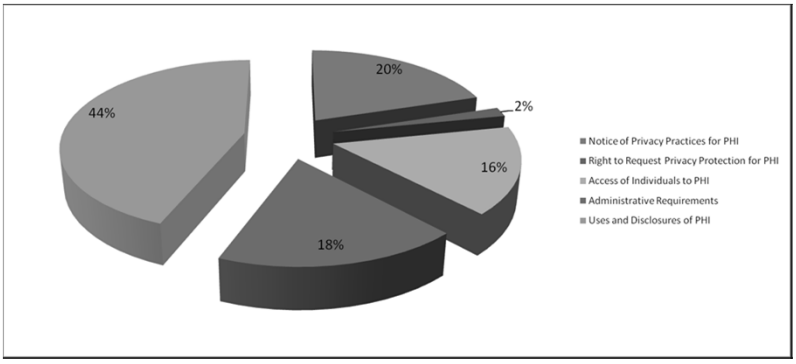
OCR PHASE I AUDITS

Phase 1 Audits (2012)

- Scope
  - 115 CEs randomly selected
  - (61) Providers, (47) health plans, (7) clearinghouses
  - On-site visit: interviews, walkthroughs, review of documents.
- Timeline

Source: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/auditpilotprogram.html

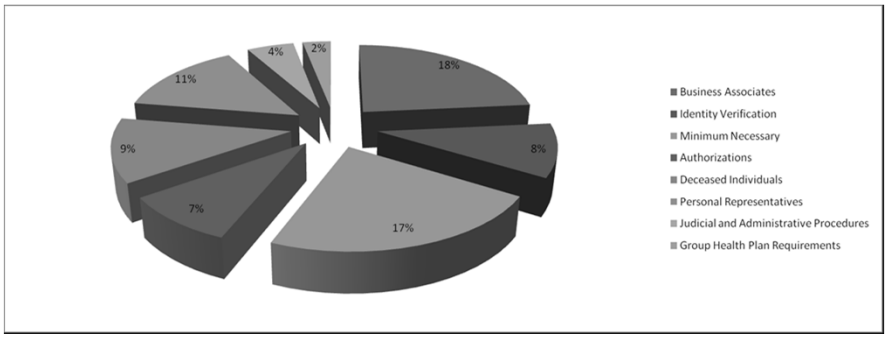
Phase 1 Findings



Source: Sanches, Linda and Rinker, Verne.
"Lessons Learned from OCR Privacy and Security Audits." IAPP Global Summit. 2013.

Phase 1 Findings

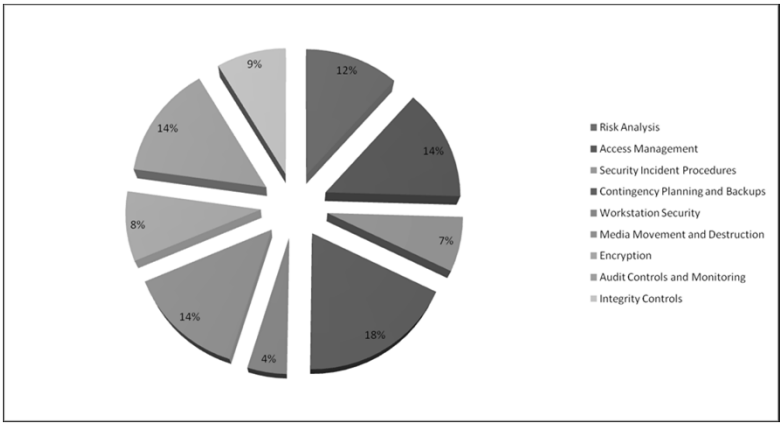
Uses and disclosures of PHI findings:



Source: Sanches, Linda and Rinker, Verne.
"Lessons Learned from OCR Privacy and Security Audits." IAPP Global Summit. 2013.

Phase 1 Findings

Security of PHI findings:



Source: Sanches, Linda and Rinker, Verne.
"Lessons Learned from OCR Privacy and Security Audits." IAPP Global Summit. 2013.

Phase 1 Audits: Summary

- No findings: ONLY 11% (2 providers, 9 health plans, 2 clearinghouses)
- Security Rule findings: 60% (58-59 providers had at least one finding)
  - BUT accounted for only 28% of the audit standards!
- Risk Analysis: missing in 2/3!
- Small entities (revenues less than $50 mil.) struggled with all three Rules.
- CEs were generally unaware of:
  - NPP; Access; Minimum Necessary; Authorizations
  - Risk Analysis; Media/Disposal; Audit Controls/Monitoring

OCR PHASE II AUDITS

OCR Audits Phase II (2014, 2015+)

- Quotes from Linda Sanches, Sr. Advisor, Privacy, OCR, September 9, 2014:

- "Stay tuned…OCR has held off on the start of audits so we could implement…new technology. I'm ready to go, but our technology isn't quite there yet."
- "We're planning to conduct the pre-audit survey screening tool. We'll have entities enter the data online through our portal. When we conduct the audits, we'll have entities go through the portal as well."
- "We'll be looking for periodic risk analysis and evidence of compliance, as well as documentation of policies and procedures being in place. For example, if we're doing a comprehensive audit and looking at you sanction process, we'll want to see instances where you've sanctioned people and whether it was consistent with your sanctions policy."

OCR Audits Phase II

- Approx. 200 (maybe less) audits of CEs.
- Includes on-site audits (many desk audits).
- Approximately 2-week response time.
- Approximately 50 audits of BAs in 2015

OCR Audits Phase II

- Only requested data submitted on time will be assessed.
- All documentation must be current.
- No opportunity to clarify requests.
- Do not submit extraneous information.
- Failure to submit responses may lead to investigation.

OCR Audits Phase II: How to Prepare

- Risk analysis;
  - Don't forget the Addressable Standards: (1) Why any such addressable implementation standard was not reasonable and appropriate and (2) all alternative security measures that were implemented.
  - Mobile devices? Encryption?
- Complete inventory of business associates (updated BAA?);
- Content and timeliness of breach notifications;
- Updated NPP (online?);
- Updated training (new employee and annual);

OCR Audits Phase II: How to Prepare

- Emergency response plan;
- Audit logs;
- Authorization forms;
- Accounting for disclosures;
- Breach notification plan;
- All required policies/procedures.

OCR Audits Phase II: How to Prepare

- Policies/procedures may not be enough. Do you have *"evidence?"*
- Example: Patient rights
  - Are your policies and procedures being followed?
    - Can you demonstrate this?
  - Training?
  - State laws?

OCR Audits Phase II: How to Prepare

- Do you have *"evidence?"*
- Example: Safeguards
  - Facility access controls?
  - Device and media controls?
  - Transmission security?
  - Encryption?
  - Training?
  - Can you track the flow of ePHI?

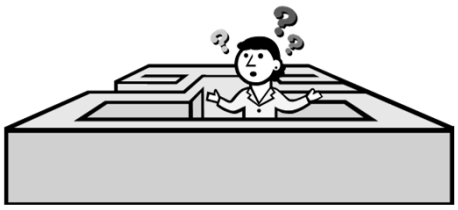
OCR Audits Phase II: How to Prepare

- Remember: this is an audit, not an investigation.
- You should expect a detailed review of your organization's program. You may be asked to walkthrough a past breach, incident or even a non-incident with the investigator(s).
- Do you know the right people?
  - Management, in-house counsel; outside counsel; CIO; Privacy Officer; others.
  - Schedule prep time.

OCR Audits Phase II: How to Prepare

- Summary
  - Have you identified internal risks?
  - Are your controls working?
  - Are you conducting routine audits?
  - Are you documenting?
  - Is your documentation "centralized?"

Questions



Thank you!

Presented by: **Andrew Mahler, JD, CIPP/US, CHRC**
amahler@email.arizona.edu

John Bailey, JD
John.Bailey@stjude.org