Anatomy of an OCR Breach Investigation

HCCA 18th Annual Compliance Institute

San Diego, CA

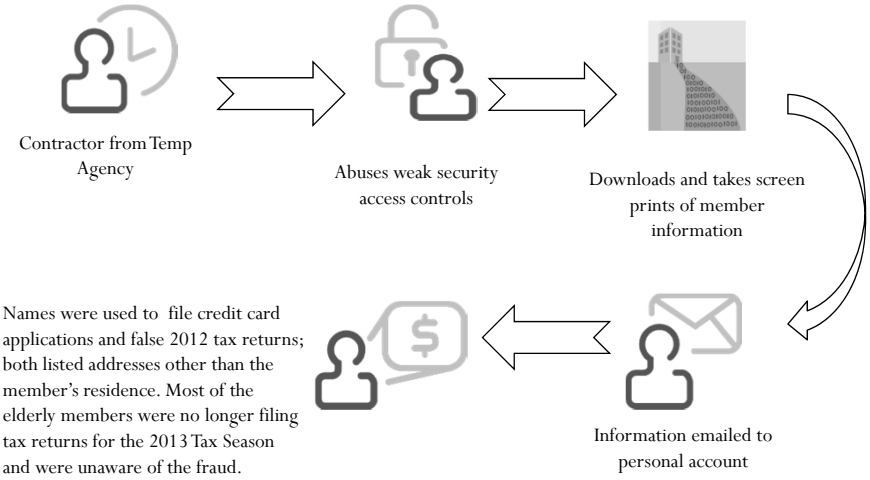
April 1, 2014

Objectives

- Learn key steps involved in responding to an incident
- Understand timeframes and review key documentation requirements
- Learn best practices to enhance oversight

2

Breach Scenario



Could this happen at your organization?

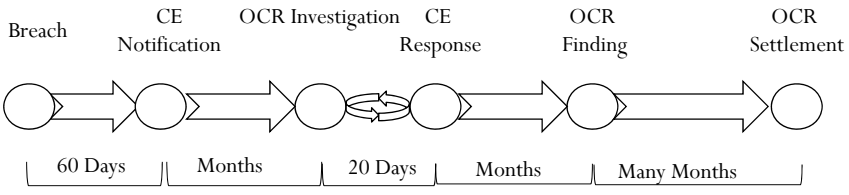
What would you do?

4

The OCR Investigation

5

Timeframe



OCR Investigation and multiple responses may be required over many months

Case cleared or moved to settlement proceedings

6

Immediate Next Steps

1. Assess situation to stem further disclosure
2. Complete an Incident Report
3. Determine if incident is a breach
4. Gather documentation
   - Try to obtain signed attestation from employee/temp
   - Ensure file is deleted, if possible
5. Mobilize incident response team
   - Privacy Office, Information Security, Human Resources, Member Services/Customer Service, Security, Breach Response specialist

7

Stakeholders

- Department Involved and contingency agencies
- Customer Service
- Finance
- IT
- Human Resources
- Consultants
- Legal Counsel
- Credit Monitoring Services
- Corporate Communications / PR Team

8

Notification Process

1. Notify impacted members, patients
2. Place ad in local paper
3. Notify OCR, CMS, if applicable and State Attorney General (depending on your State law requirements)
4. Train customer service, develop FAQ
5. Contact Business Associates, vendors if involved

9

The waiting begins….

- ❑ Gather documentation to build your case file – training materials, Privacy & Security policies and procedures, disciplinary action policies
- ❑ Further assess risks

  Consider whether you have adequate resources to do risk analysis or hire consultant with expertise in HIPAA Privacy & Security
- ❑ Finalize risk assessment, if needed
- ❑ Consult with HIPAA counsel

10

Case Study – OCR Request

- Within 4 months, OCR responded to the online breach notification with a request for the following items:
  - Press Release
  - List of complaints received from members and resolution of complaints
  - List of staff participating in training in response to the breach
  - Risk Assessment as a result of the breach
  - P&Ps
- Response due within 20 days

11

Additional Requests & additional details

- Follow-up requests may not be directly related to incident
- Requests may extend back many years
- Every response requires corresponding documentation
- Example of requests:
  - Incident Report – internal documentation or tracking of what occurred
  - Evidence of regular system activity and audit log reviews
  - Risk Analysis
  - Vulnerability scan results
  - Corrective action plans
  - Disciplinary Action
  - Safeguards for the transmission of ePHI
  - Privacy & Security Awareness Reminders

12

System activity and log review

- Evidence of regular system activity and audit log reviews
  - Must be able to demonstrate that logs are captured and reviewed
  - Configuration and log samples for the systems
  - Procedure documents for monitoring logs and following up on incidents
  - Signed document by administrators that logs are reviewed

13

Risk Analysis

- Risk Analysis – Included a detailed review of Security process including

P&Ps
End Point Security
Mobile Media and Device Security
Wireless Security
Malware Protection
Configuration Management
Vulnerability Management
Secure Disposal
External Breach Protection
PHI Transmission Protection
Password and Account Management
Access Control & Management
Remote Access & Authentication
Training and Awareness
Incident and Breach Response
Third Party Security Management and hosted systems
Business Continuity Management
Risk Management
Physical Security

14

Corrective Action Plan

- OCR may request prior risk assessments to better understand unresolved issues over the years
- A corrective action plan associated with findings from a risk assessment must be documented
- Building a corrective action on short notice is costly and may commit you to security strategies and timelines that are onerous and not completely necessary

15

Security Rule Policies &Procedures (P&Ps)

- Must be approved and dated and include the following:
  - Sanctions
  - Termination Procedures
  - Contingency Plan
  - Facility Security Plan
  - Password Management
  - Data Backup
  - Device & Media Controls
  - Authorization & Supervision

16

Other Safeguards

- Disciplinary Action – demonstrate that immediate action was taken to sanction the employee/contractor
  - Ensure safeguards for the transmission of ePHI
- Privacy & Security Awareness Reminders offered to workforce members including contingent workers regarding the protection of ePHI and industry best practices
- Conduct regular site audits

17

What's Next?

- OCR accepts evidence and documentation as a Corrective Action Plan (CAP) and closes breach investigation

• or

- OCR moves the investigation over to the settlement phase:
  - Possibly more data requests to solidify the government's case
  - Offer to settle through resolution agreement and corrective action plan (possibly through meeting)
  - May indicate potential civil monetary penalties (CMP) that may be exposed, which may be tens of millions due to multiple alleged violations over multiple years
  - May be some room for negotiation, but high potential CMPs may limit health care provider's leverage

18

Settlement

- Recent settlements have had less stringent corrective action plans (e.g., shorter and no independent monitoring)
- If you do not agree to resolution agreement:
  - Letter of opportunity providing 30 days to provide affirmative defenses and mitigating factors
  - Notice of proposed determination indicating proposed CMP and providing 90 days to appeal to administrative law judge (ALJ)
  - If appeal to ALJ judge, can appeal ALJ decision to HHS Departmental Appeals Board, and can appeal DAB decision to U.S. Court of Appeals
  - If no appeal, HHS imposes the CMPs

19

How Much Does A Breach Cost?

1. OCR sends organization letter, requesting evidence to a list of questions. **20 days** to respond.

2. OCR sends a 2nd letter asking for more details.

Steps	Approx. Cost
Internal discovery	a. $5,000 – 10,000 b. $10k – 15,000 c. $15k – 20, 000
Breach Notification & Response	a. $10k – 20,000 b. $20k – 30,000 c. $40k – 50,000
OCR LETTER RECEIVED	
OCR Response #1 and #2	a. $10k – 20,000 b. $20k – 30,000 c. $40k – 50,000
OCR negotiates a settlement	a. $50k — 100,000 b. $100k — 250,000 c. $250k — 1 Million
OCR requires Org to perform annual audits	a. $5k — $25,000 b. $25 — $50,000 c. $50k — $100,000
Approx. Total?	**a. $80k - $165,000** **b. $165k - $356,000** **c. $395k - $1.2Million**

20

Costs add up

Steps	Approx. Cost
Internal discovery	$10-15k
Breach Notification & Response	$20-30k
OCR Response #1 and #2	$40-50k
OCR negotiates a settlement for Company	$250k- 1 million
OCR requires Company to perform annual audits	c. $50-100k
TOTAL	$370,000-1.2 million

21

How May a Breach Affect You?

1. **Patient Loyalty**
2. **Financial loss**
   - Average cost of a breach is **$194/ record**
   - OCR can fine an organization up to **$1.5 million per incident**
3. **Reputational damage**
4. **System downtime**
5. **Litigation**

Table: Categories of HIPAA Violations & Penalty Amounts

Violation category	Each violation	Violations of an identical provision (in a calendar year)
Did Not Know	$100- 25,000	$1.5 million
Reasonable Cause	$1,000- 100,000	$1.5 million
Willful Neglect— *Corrected*	$10,000-250,000	$1.5 million
Willful Neglect— *Not Corrected*	$50,000-1.5M	$1.5 million

22

Lessons Learned

- Established HIPAA Governance Committee – confirm that CAP and risk analyses are current
  - Created a 'watch list' of employees who could send ePHI externally
  - HIPAA Security & Training for contingent workers
  - Limited temp access to certain websites and personal email
- Ongoing Risk Analyses and evaluation of HIPAA Privacy and Security program effectiveness.
- Stronger communication with and oversight of temp agencies; regularly evaluate contract terms.

23