

Preparing for an OCR Audit

“How you doin’?”

Tom Walsh, CISSP

tw-Security
Overland Park, KS

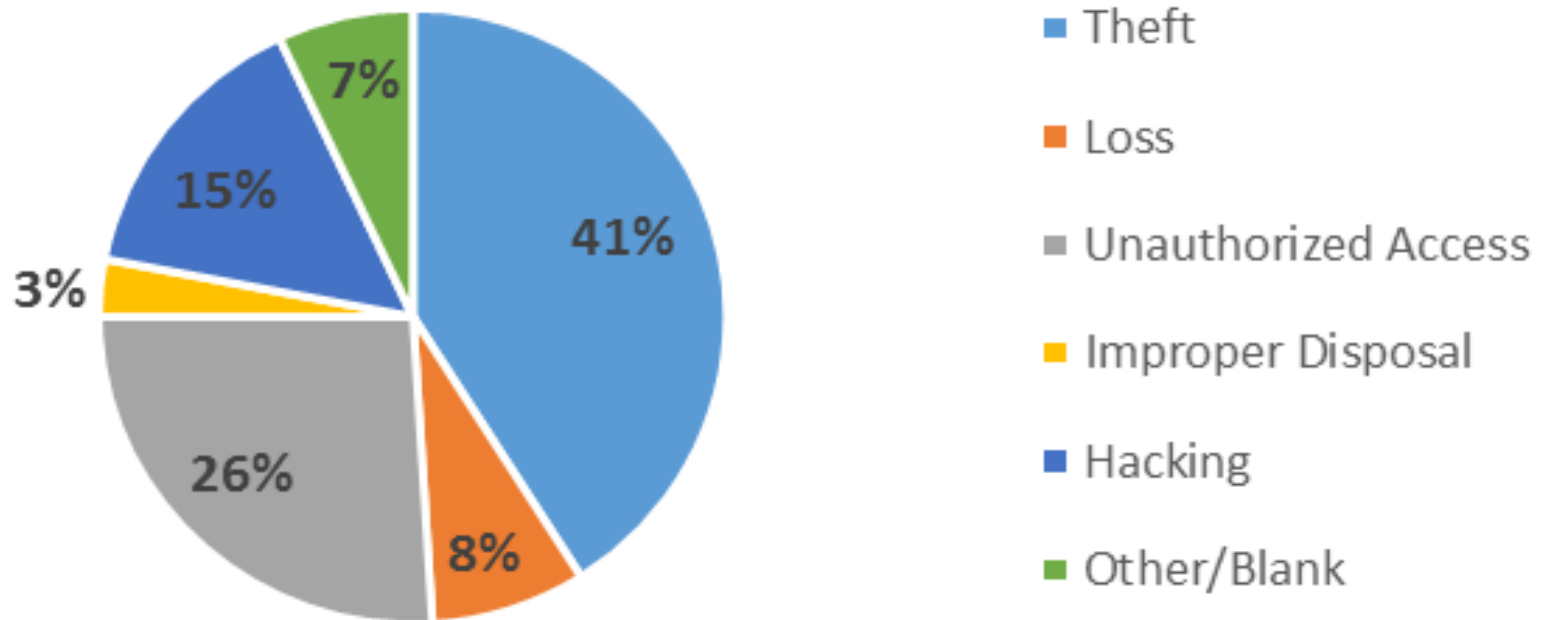
Hacking and Healthcare Breaches

- The Federal government cannot ignore the number of breaches in healthcare

Year Hacking Events Reported to HHS	Number of Hacking Events Reported	Number of Patients Affected in Hacking Events for the Year
2010	8	92,358
2011	17	297,775
2012	16	900,684
2013	24	238,207
2014	34	1,796,755
2015	57	111,812,172
2016	107	13,345,573

Types of Reported Breaches

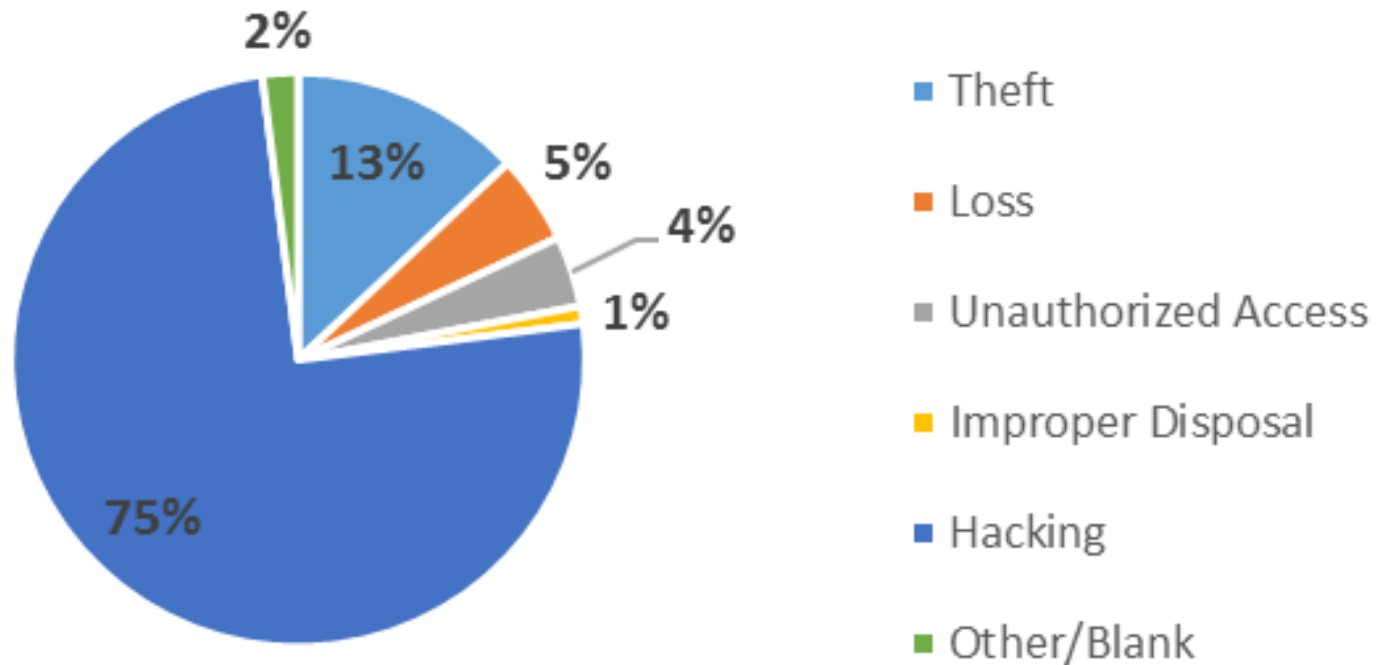
Q1-2017
Reason for Breach Number of Events



Patients Impacted by Breaches

Q1-2017

Reason for Breach - Patients Impacted



Session Objectives

Agenda

- **Review the three types of OCR audits**
- **Explain how the OCR is getting tougher –**
 - Larger fines; challenging corrective action plans
- **Discuss a free tool available for assessing HIPAA compliance and the pros and cons of the using the tool**
- **Identify ways for building a “book of evidence”**

Introduction – Tom Walsh

- **Certified Information Systems Security Professional (CISSP)**
- **14+ years – tw-Security** (formerly: Tom Walsh Consulting, LLC)
- **Co-authored four books on healthcare security**
 - Published by AMA, AHIMA, and HIMSS (two books)
- **Former information security manager for large healthcare system in Kansas City metro area**
- **Started working in information security in 1992**
- **A little nerdy, but overall, a nice guy 😊**

Audits from the Office for Civil Rights (OCR)



Common mistake – “Office of Civil Rights”
Your audit may be off to a bad start if you get their name wrong.

Office for Civil Rights (OCR)

- **The Office for Civil Rights (OCR) is an organization within the U.S. Department of Health and Human Services (HHS)**
 - HHS makes the rules
 - OCR works closely to ensure patient rights to privacy
 - The OCR is responsible for **enforcement** of the **HIPAA Rules** (Privacy, Security, and Breach Notification)

Three Types of “Audits”

1. Investigation

- Trigger: Reported breach or patient complaint

2. Random (HIPAA Compliance) – two types:

- Desk audit – limited focus; conducted offsite
- Comprehensive – broader focus; conducted onsite
- Trigger: “Selected” from a pool of organizations

3. Meaningful Use

- Trigger: Entity received incentive money

#1 Investigations



Investigations

- **OCR has renewed motivation to conduct audits and levee fines for those organizations that are still not complying with HIPAA**
- **The results of an investigation or audit often lead to settlements that include fines and Corrective Action Plans (CAPS)**

Common Reasons Given for Fines

Failure to:


- Conduct an accurate and thorough **risk analysis** that incorporates all information technology equipment, applications and data systems storing PHI
- Create and maintain a **risk management** plan
- Implement **policies and procedures** and **retain** for six years
- **Reasonably safeguard the ePHI** (prevailing practices)
 - **Unencrypted devices and media**
- **Obtain satisfactory assurances** in the form of a written **business associate** contract

Resolution Agreements


HHS.gov U.S. Department of Health & Human Services
Health Information Privacy

I'm looking for... 

[HHS A-Z Index](#)

 **HIPAA for Individuals**

 **Filing a Complaint**

 **HIPAA for Professionals**

 **Newsroom**

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [Compliance Enforcement](#) > Resolution Agreements

HIPAA for Professionals	
Privacy	+
Security	+
Breach Notification	+
Compliance & Enforcement	-
Enforcement Rule	
Enforcement Process	
Enforcement Data	
Resolution Agreements	
Case Examples	
Audit	

Text Resize **A A A** Print  Share   

Resolution Agreements

Resolution Agreements and Civil Money Penalties

A resolution agreement is a settlement agreement signed by HHS and a covered entity or business associate in which the covered entity or business associate agrees to perform certain obligations and make reports to HHS, generally for a period of three years. During the period, HHS monitors the covered entity's compliance with its obligations. A resolution agreement may include the payment of a resolution amount. If HHS cannot reach a satisfactory resolution through the covered entity's demonstrated compliance or corrective action through other informal means, including a resolution agreement, civil money penalties (CMPs) may be imposed for noncompliance against a covered entity.

- [\\$5.5 million HIPAA settlement shines light on the importance of audit controls](#) - February 16, 2017
- [Lack of timely action risks security and costs money](#) - February 1, 2017
- [HIPAA settlement demonstrates importance of implementing safeguards for ePHI](#) - January 18, 2017
- [First HIPAA enforcement action for lack of timely breach notification settles for \\$475,000](#) - January 9, 2017

<https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/>

Largest Fines for HIPAA Violations

- Advocate Health Care \$5.55 M ([August 4, 2016](#))
- Memorial Healthcare System \$5.5 M ([February 16, 2017](#))
- New York Presbyterian Hospital and Columbia University \$4.8 M (May 7, 2014)
- Cignet Health \$4.3 M (February 4, 2011)
- Feinstein Institute for Medical Research \$3.9 M ([March 17, 2016](#))
- Triple-S Management Corp. \$3.5 M (November 30, 2015)
- Children's Medical Center of Dallas \$3.2 M ([February 1, 2017](#))
- University of Mississippi Medical Center \$2.75 M ([July 21, 2016](#))
- Oregon Health & Science University \$2.7 M ([July 18, 2016](#))
- CVS Pharmacy \$2.25 M (January 16, 2009)
- New York Presbyterian Hospital \$2.2 M ([April 21, 2016](#))
- MAPFRE Life Insurance Company of Puerto Rico \$2.2 million ([January 2017](#))
- St. Joseph Health (SJH) \$2.14 M ([October 18, 2016](#))

Smaller Data Breaches

- **Misdirected faxes**
- **Paperwork handed to the wrong patient**
 - Prescription, discharge summary, lab results, etc.
- **Patient bill mailed to the wrong patient**
- **Unauthorized access by employee (snooping)**

The most common types of breaches which generally affect a small number of patients; in many cases only one or two patients

#2 Random Audits



OCR Phase 2 – Random Audits

- **Most audits will be desk audits**
 - Submission of requested documents for review (policies, procedures, risk analysis reports, etc.)
 - A failed desk audit may lead to an onsite audit
- **Some onsite audits**
 - These will be much greater in scope
- **Unlike past audits...**
 - OCR staff will conduct – not contractors
 - Findings of noncompliance may result in fines; monies collected in fines will help fund future audits (*conflict of interest?*)

OCR Phase 2 – Random Audits

- ≈1,200 notification emails (March – May 2016) and were typically received by the Privacy Officer
- **To confirm:**
 - Correct address
 - Contact person
 - Size of organization
 - Functions
 - Research

Because the emails had active hyperlinks, some of the emails from the OCR were treated as spam



OCR Phase 2 – Desk Audits

- **Desk audits began in 2016 - notification letters were delivered via email to the first wave of:**
 - **167** selected covered entities
 - **45** selected business associates (selected from a “pool”)
- **Organizations should monitor their spam filtering and junk mail folders for emails from:**
OSOCRAudit@hhs.gov
- **If an organization received a confirmation email regarding the point of contact, odds are high of an upcoming desk audit at some later point in time**

OCR Phase 2 – Desk Audits

- **For the 167 selected entities, they had:**
 - 10 business days (July 22, 2016) to respond to the document requests
 - To send an inventory of all of their business associates with the addresses and contact info
- **Desk audits of business associates (BAs)**
 - Began in October 2016
 - Selected BAs were from a “pool” provided by covered entities being audited

OCR Phase 2 – Desk Audits

- **Breach Notification Rule (BNR)** only **2** of 19 criteria
 - BNR12 Timeliness of Notification
 - BNR13 Content of Notification
- **Privacy (P)** only **3** of 89 criteria
 - P55 Notice of Privacy Practices - Content requirements
 - P58 Provision of Notice - Electronic Notice
 - P65 Right to access
- **Security (S)** only **2** of 70 criteria
 - S2 Security Management Process - **Risk Analysis**
 - S3 Security Management Process - **Risk Management**

The letters and numbers associated with the desk audit align with the numbering in OCR's *HIPAA Audit Program Protocol*

Random Onsite Audits

- **Onsite audits of both covered entities and business associates are scheduled for 2017**
- **After the completion of the desk audit process, onsite audits may be conducted by the OCR to evaluate against a comprehensive selection of controls in protocols**

HIPAA Audit Program Protocol

#3 Meaningful Use



Failure to complete a risk analysis is the most common reason why covered entities fail a Meaningful Use audit

Meaningful Use Audits

Core Objective - Protect Electronic Health Information (*Eligible Professionals*)

“Proof that a **security risk analysis** of the certified EHR technology was performed **prior to the end of the reporting period** (i.e. report which documents the procedures performed during the analysis and the results of the analysis). If deficiencies are identified in this analysis, please supply the **implementation plan**; this plan should include the **completion dates**.”

Free Tool for Assessing HIPAA Compliance

(“Audit Test Procedures” for onsite audits)



Audit Test Procedures

OCR's HIPAA Audit Program Protocol

- Privacy = **89** requirements; was 81
- Breach = **19** requirements; was 10
- Security = **70** requirements; was 77

*Original protocol
was released in
June of 2012*

HHS.gov U.S. Department of Health & Human Services
Health Information Privacy

I'm looking for... HHS A-Z Index

HIPAA for Individuals Filing a Complaint HIPAA for Professionals Newsroom

HHS Home > HIPAA > For Professionals > Compliance Enforcement > Audit > Audit Protocol

HIPAA for Professionals Text Resize AAA Print Share Facebook Twitter

Audit Protocol – Updated April 2016

The HHS 2012 HIPAA Audit Program reviews the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These analyses are conducted using a comprehensive audit protocol that has been updated to reflect the Omnibus Final Rule. The audit protocol is organized by Rule and regulatory provision and addresses separately the elements of privacy, security, and breach notification. The audits performed assess entity compliance with selected requirements and may vary based on the type of covered entity or business associate selected for review. You may submit feedback about the audit protocol to OCR at OSCCBAudit@hhs.gov.

Source: <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html>

Audit Test Procedures

A common “Audit Procedure” that would pertain to standards, policies, procedures, plans, or any other forms of documentation...

Determine if the covered entity's formal or informal policies and procedures have been updated, reviewed, and approved and on a periodic basis.

- 1. Reviewed**
- 2. Updated**
- 3. Approved**



Missing from the Protocol?

- **Hack, hacker, hacking**
- **Tablet**
- **Smartphone**
- **Personally-owned devices**
- **Portable media**
 - External hard drives and USB thumb drives
- **Data loss prevention**
- **Data leakage**
- **Change control**
- **Configuration management**
- **Bring your own device (BYOD)**
- **Mobile device management (MDM)**
- **Texting**
- **Secure messaging**
- **Web portal**
- **Secure website (https)**
- **Router, switch, firewall**
- **Networking scans**
- **Penetration testing**

Also Missing...

- **Cyber, phishing, social engineering, malware, ransomware**
- **Denial of service attack**
- **Biomed or biomedical devices**
- **Cloud**
- **Wireless, WPA, WPA2, SSID, access point**
- **Virtual, virtualization**
- **Telecommuting**
 - (such as remote coding and remote transcription)
- **Telemedicine, teleradiology**

HIPAA Compliance \neq Security

Proof of Compliance



Proof of Compliance

- Policies and procedures
- Plans
- Reports
- Forms
- Signed agreements
- Training content and records
- Others?



“If it hasn’t been documented, it hasn’t been done!”

Documentation for a Desk Audit

Documentation for a desk audit includes:

- Risk analysis and risk management
- Policies and procedures (Privacy and Security)
- Breach notification policies and example notices
- Notice of Privacy Practices
- Sanction policy
- A list of Business Associates/w contact information

Proof of Compliance - Examples

- **Other evidence or proof of compliance** (practices)
 - Is there a culture of compliance?
 - Is your staff even thinking about Privacy and Security in their jobs?
 - Does your staff know the names of their Privacy and Security officers?
 - Is there evidence of incident reports, breach reports, and sanctions to workforce offenders?
 - Has the organization identified risks and implemented safeguards and controls to manage risk?

Policies and Procedures

- **HIPAA Security Rule**

- **§ 164.316 Policies and procedures and documentation requirements states:**

- (i) Time limit – Retain the documentation for 6 years
 - (ii) Availability – Make documentation available to workers
 - (iii) Updates – Periodically review, update, [and approve]

- **Create a policy roadmap or framework**

- Consider two types of audience when writing policies:
 - Workforce (organizational-wide)
 - More technical for IT or IS staff

Final Thoughts on Audits



Chances of Being Audited

- **Odds of getting selected for a random audit are slim***
 - ≈5,565 hospitals in the United States * *A breach triggers an investigation*
 - ≈230,187 physician practices in the United States
- **Phase 1 - Random audits began in 2011– 2012**
 - 115 covered entities were randomly audited in Phase 1
- **Phase 2 - Desk audits began in 2016**
 - 167 selected covered entities
 - 45 selected business associates
- **But if you are audited, you better pass, or else...**

No Time for HIPAA Compliance?

I don't think so...

- The final HIPAA Security Rule was released in February 2003 with an effective deadline of April 21, 2005 (*12 years ago!*)
 - The Proposed Security Rule was released **19 years ago** – plenty of advance notification by the government of what is required and expected
 - Organizations that have not conducted a risk analysis for *all* of their applications and systems; are now acting with “willful neglect”
 - Receiving the highest level of enforcement penalties

Analogy: Operating a vehicle

When operating a motor vehicle, there are at least three items you must have:

1. Valid driver's license
2. Vehicle registration; current license plate
3. Proof of insurance

What would happen if the police could prove you have been operating a vehicle for more than 12 years without the required documents?



Minimum Items for the OCR

If being investigated or audited by the OCR for security, there are at least three items you must have:

1. Proof of a thorough **risk analysis** (all applications and systems that store PHI)
2. **Risk management** – a plan for remediation of risks and compliance gaps
3. Policies, procedures, plans, etc. – **documentation** that supports and drives the security program

A risk analysis a systematic process for identifying the reasonably anticipated threats, controls, vulnerabilities, possible impacts if the threat was realized, likelihood that the threat will be realized, risk score, and suggested controls to address identified vulnerabilities

Security Risk Assessment (SRA) Tool

- **ONC created the SRA Tool for small providers**
- **When printed, the SRA Tool = 436 pages**
- **ONC estimates it will take 6 hours to complete**
- **The tool is for evaluating compliance gaps with HIPAA – it is not a true risk analysis**
- **There is a lot of critical security topics missing from the tool (*similar to the audit protocol*)**

ONC = Office of the National Coordinator

Summary



During this session, we...

- Described the three types of OCR audits
- Demonstrated how the OCR is getting tougher – larger fines; challenging corrective action plans
- Explained how organizations can use the *HIPAA Audit Program Protocol* to assess compliance and discussed the downsides to the tool
- Identified ways to build a “book of evidence”



Tom Walsh, CISSP

tw-Security

Overland Park, KS

www.tw-Security.com

tom.walsh@tw-Security.com

913-696-1573

tw-Security, a nationally recognized healthcare IT security consulting firm is dedicated to helping healthcare organizations protect their information resources with hands-on experience in creating and managing information security programs.