

Legal, Compliance & Regulatory

**Preparing for an Audit—A
Proactive Approach to HIPAA
Privacy Compliance**

March 15, 2016
San Antonio, TX



16th Annual Intercompany Long Term Care Insurance Conference

Agenda



- Legal Landscape
- History of OCR Enforcement Activity
- OCR's 2016 Audit Program
- How to Prepare for an Audit

Legal Landscape

A patchwork of federal and state laws



- HIPAA (amended by HITECH)
 - Governs use/disclosure of Protected Health Information
 - Significant financial consequences for violations
 - Establishes breach notification obligations
 - HITECH extends HIPAA rules to business associates
 - Mandates that the OCR initiate an audit program to ensure compliance
- Gramm Leach Bliley (GLB)
- Section 5 of the FTC Act



- NAIC Draft Insurance Security Model Law
- State Insurance Privacy Laws
 - Some require implementation of active security measures to prevent data breaches (AR, CA, MD, MA, RI, OR, TX, UT)
 - Unfair and Deceptive Trade Practices Acts – Variation on Consumer Protection Act; Enforced by attorney general
- SBNAs



History of OCR Enforcement Activity

The Early Years



- OCR imposed its first penalty in 2008
- OCR only imposed seven penalties through 2011
- 2012-2015—OCR imposed 21 penalties
 - Ranging from \$50k to almost \$5M
 - Seven penalties exceeded \$1 million



Recent OCR Enforcement Actions



To date, OCR has levied nearly \$30 million in penalties from covered entities and business associates

- May 2014 - NY Presbyterian/Columbia U. Hospital - 6,800 records - **\$4.8 M**
- April 2014 - Concentra - 870 records - **\$1.7 M**
- July 2013 - WellPoint - 612,402 records - **\$1.7 M**
- Sept. 2012 - Mass. Eye & Ear - 3,621 records - **\$1.5 M**
- March 2012 - BCBS of Tenn. - 1M+ records - **\$1.5M**

More Than Just a Fine



- Lost Business/Lost Reputation
- Class Action Lawsuits
 - Shareholders (if applicable)
 - Affected customers
 - Affected financial institutions (if applicable)
- Prepare for breach investigations and remediation
 - Potential Operational Changes
 - Breach Notification Letters
 - Identity Theft Prevention/Free Credit Monitoring
- Criminal Prosecution (rare, but 566 referrals)

NY Presbyterian and Columbia (2014)



- In 2010, a doctor who worked for both hospitals accidentally deactivated the hospitals' network, nullifying safeguards and rendering 6,800 patient ePHI accessible through the internet
- Hospitals signed consent agreement with OCR, settling for **\$4.8 million**
- Lesson: Be prepare for breaches and security incidents – ensure effective breach response plan and readiness protocols are in place



Lesson: No matter what industry you are in, persistent vigilance in updating security measures is paramount

- Protective measure: Conduct an information privacy/security audit at least every few years
- Mitigation Technique: Comprehensive breach response planning

The Hospice of North Idaho “HONI”



- An unsecured laptop, containing PHI of *441* HONI patients, was stolen
- HONI required to pay **\$50,000** fine



HOSPICE
OF NORTH IDAHO



Lesson: encrypt your laptops; a stolen encrypted laptop may not constitute a breach

- The increase in use of BYOD may lead to more “small-scale” breaches, with “full scale” repercussions

“Encryption is an easy method for making lost information unusable, unreadable and undecipherable”

- Former OCR Director Leon Rodriguez



HOSPICE
OF NORTH IDAHO



OCR's 2016 Audit Program



- Initiated in 2011
- Three-step process:
 1. Developed audit protocols;
 2. Tested protocol in limited wave (20) of audits;
 3. Conducted full range of audits (115) using revised protocols
- Who was audited? **Not business associates**



Audit Process:

- Document request and desk review
- Site visit
- Interviews (Privacy officers and others)
- Report and comment period
- Potential subsequent enforcement action





Audit Protocols:

- Covers Privacy Rule requirements for 1) notice of privacy for PHI; 2) rights to request privacy protection for PHI; 3) access of individuals to PHI; 4) administrative requirements; 5) uses and disclosures of PHI; 6) amendment of PHI; and 7) accounting of disclosures
- Covers Security Rule requirements for administrative, physical, and technical safeguards
- Covers requirements for the Breach Notification Rule



- What was the purpose?
 - Assessed overall HIPAA compliance and determined what type of technical assistance that should be developed moving forward
- Results?
 - OCR found numerous violators and action plans were issued to help those organizations achieve compliance
 - Initial violators were given lenient penalties/treatment

HIPAA violations commonplace?



- Since 2009, over 1,000 large (over 500 people affected) breaches have been reported and over 120,000 small breaches, affecting over 41 million people
- Despite the high number of breaches, from 2009-2015, OCR levied fines against violators just twenty-two times



- In September of 2015, Office of the Inspector General for the Department of Health and Human Services (OIG) issued two reports critical of OCR enforcement efforts concluding:
 - OCR Should Strengthen Its Followup of Breaches of PHI Reported by Covered Entities
 - OCR Should Strengthen Its Oversight of Covered Entities' Compliance with HIPAA Privacy Standards



The Reports' Findings:

- OCR failed to fully implement the HITECH required audit program to **proactively** identify non-compliance
- Of violations investigated, 54% demonstrated non-compliance with at least one standard
- OCR only documented corrective actions in 74% of cases
- 21% of OCR staff reported that they rarely or never determined whether OCR had previously investigated a covered entity (23 had been investigated at least five times each)
- Did not record small breach incidents (breaches affecting less than 500 people)



OIG's Recommendations

- Implement a permanent audit program
- Document all corrective action plans
- Develop efficient method to search for and track previous investigations
- Require OCR staff to identify repeat violators and impose statutorily-mandated fines
- Expand outreach and education programs



Audits Are Coming

OCR's Reaction



- OCR's increased its budget by \$4 million dollars (10%) to support audit program and add 18 full-time staff members
- OCR, through Director Jocelyn Samuels, and OIG both indicated that the second phase of the audit program will begin in early 2016 (though the protocols have not yet been released)
- OCR hired vendor FCi Federal to assist in the audit program
- Expect a more aggressive OCR enforcement scheme...



- Employee's laptop was stolen by a scorned spouse, putting less than 500 hundred patients of a home health provider at risk
- OCR conducted investigation, determined that Lincare violated HIPAA by failing to reasonably safeguard PHI and take steps to prevent further disclosures, and assessed penalty of \$239,800
- In February 2016, Lincare filed administrative challenge
- ALJ found in favor of OCR
- Only the second time OCR has sought civil money penalties for a violation
- Lesson: Even small providers and relatively minor violations will be prosecuted; evidences proactive and more aggressive OCR



No updated audit protocols yet, but common projections include:

- 200 desk audits and 24 on-site audits will be completed in 2016
- Audits will focus on HITECH laws and compliance, breach notification, patient access to ePHI, and patient privacy rights
- Only two business days to reply to an audit request
- Business associates likely included in audits—a top three priority for OCR in 2016

What Should You Be Doing?



- Prepare: conduct self-assessments to determine compliance with HIPAA
- Address areas of vulnerability (look at flow of PHI through the organization, policies and procedures, HIPAA requirements, current practices)
- Collect and review previous audit reports and risk assessments related to security implementation, privacy, and breach notification requirements
- Review business associate and subcontractor agreements
- Involve legal counsel, privacy officers, and CEO/management early

So What Does All This Mean?



- ORC is stepping up its game
- For the first time since 2012, random audits will be coming, and they will be far more strict
- Prepare ahead of time – don't be blindsided by a more aggressive ORC



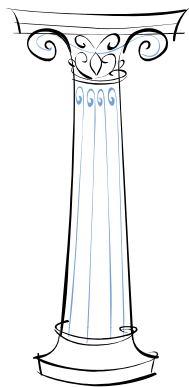
How to Prepare for an Audit



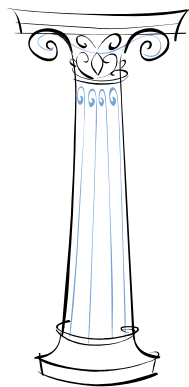
Key—Aggressive Offense

Five Pillars Essential to a Privacy Compliance Program Focused on “Culture of Compliance”

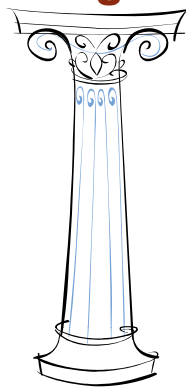
Policies & Procedures



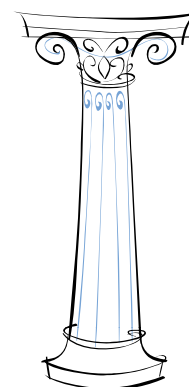
Data Governance



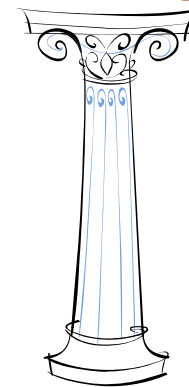
Risk Identification & Mitigation



Business Associates



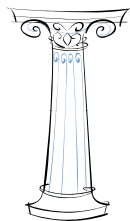
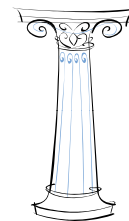
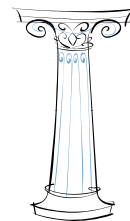
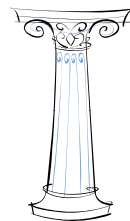
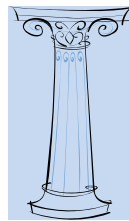
Training



Pillar 1: Policies and Procedures



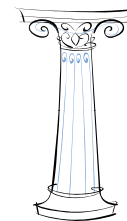
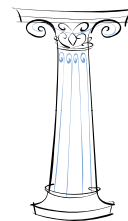
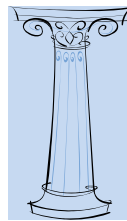
- Robust information and data use privacy and security policies
- Current document retention and destruction policy
- Breach response plan
 - Incident response team / call list
- Notice of Privacy Practices
- Procedures to implement the policies



Pillar 1: Policies and Procedures



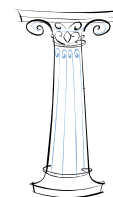
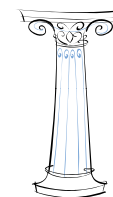
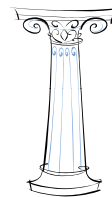
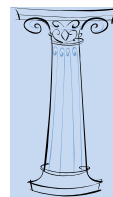
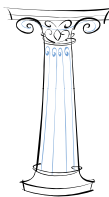
- Are your policies and procedures stale?
- Are document retention and destruction guidelines and procedures part of your offensive playbook?
- If yes, are they clear and useful?
- Is your notice of privacy practices revised and redistributed?



Pillar 2: Data Governance



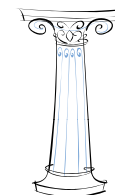
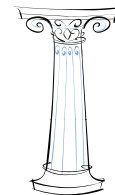
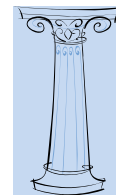
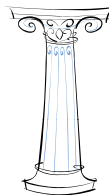
- All business leaders (Privacy Officer, CEO, CISO, Dept. Heads) and compliance professionals should understand the organization's data infrastructure
- Preparing data for OCR reporting
- Regular risk assessments to identify weaknesses and adjust controls
 - Preserve the privilege!



Pillar 2: Data Governance



- Have you designated a Security Officer?
- How do you stay abreast of emerging threats, best practices?
- Have you conducted a security audit, best practices?
- Do you carry cyber liability insurance coverage?





- Some reports estimate annual cyber insurance premiums are estimated to grow from \$2.5 billion in 2014, to \$5 billion by 2018, and to at least \$7.5 billion by 2020
- Currently, only around 1/3 of companies have some form of cyber coverage
- However, coverage varies considerably by industry
- And companies face increased pressure from regulators to disclose coverage

Pillar 3: Risk Identification & Mitigation

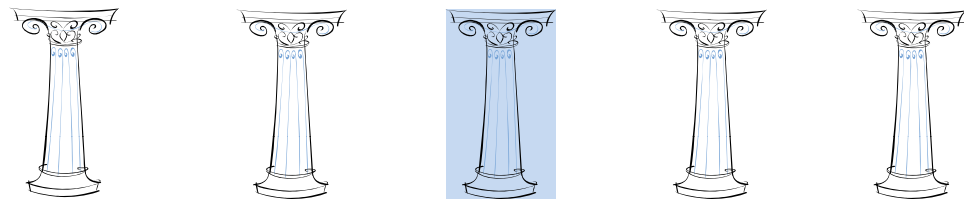


- Written policies and procedures paired with audit/quality assurance reviews (internal vs. external)
 - *E.g.*, Minimum necessary access paired with systematic controls and routine access audits
- Accounting of disclosures system, paired with a breach notification process
 - *E.g.*, Risk Analysis document for each incident “feeding” breach notification
 - “Harm” standard replaced with “probability of compromise” standard

Pillar 3: Risk Identification & Mitigation




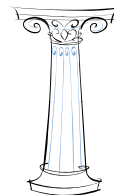
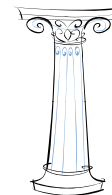
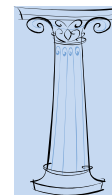
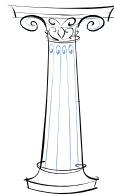
- Do you use internal or external auditors?
- Which audit source qualifies as the “best practice”?
- Have you prepared a communication strategy?



Pillar 3: Risk Identification & Mitigation



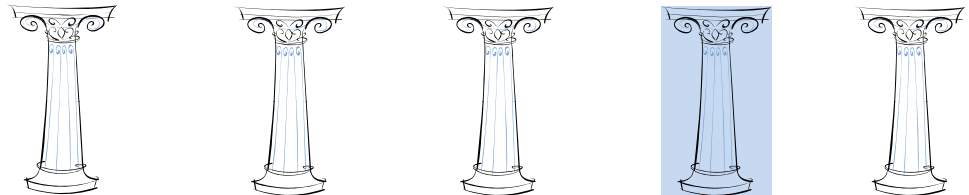
- Harm Standard Out  Compromise In
- Policies and Procedures to:
 - Detect and escalate disclosures
 - Risk assessment performed and documented for each disclosure (defensible analysis; AOD system)
- Notification Decision: burden on carrier
- Must occur “without unreasonable delay”; no later 60 days; over 500 records yields additional hurdles
- AOD Archive Tool



Pillar 4: Business Associates



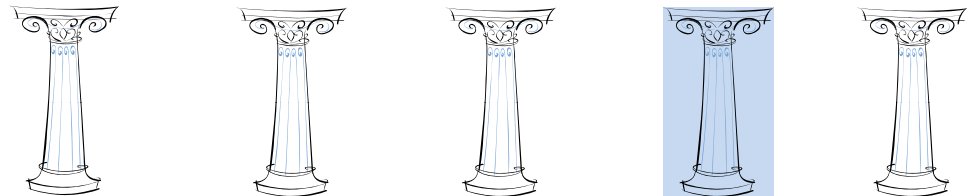
- Business Associate Agreements (“BAA”) (revision required by Omnibus)
- Communication of enhanced expectations (given expanded obligations under Omnibus)
- Audit/Quality Assurance Review



Pillar 4: Business Associates



- What experiences have you had with obtaining BAAs and communicating with business associates?
- Do you perform internal or external audits/quality assurance reviews?
- What do you consider to be the best practice?



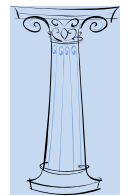
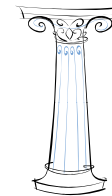
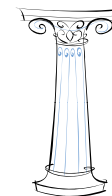
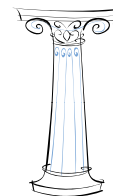
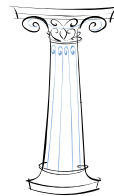


www.jklossner.com
copyright 2006 John Klossner, www.jklossner.com

Pillar 5: Staff Training & Education



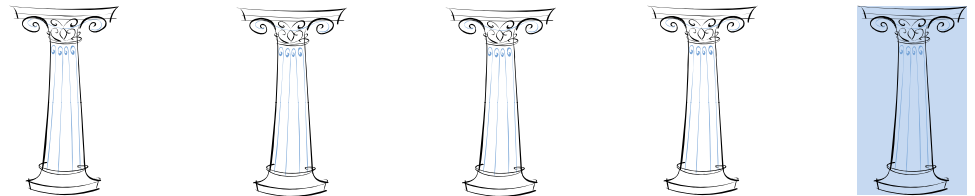
- Code of Conduct
- Mandatory employee training
 - On-boarding
 - Routine/Annual (including annual HIPAA training)
 - Ad Hoc (in response to trends or incidents),
 - Varied Media (on-line, e-mail, video, posters, etc.)
 - Documented!



Pillar 5: Staff Training & Education



- Is there a training you employ that you consider to be a “best practice”?
- Do you have a positive experience with an employee training program?



Questions?