What Are The Odds Of a HIPAA Audit?
Outline

- Random Odds
- The law
- Why is enforcement up?
- What types of audits and what causes them
- Examples of enforcement
- What can you do to avoid audits and fines
The following report contains graphic content. Viewer discretion is advised.
Random odds ....

- Winning Lotto: 1 in 175 Million
- Attacked by a shark: 1 in 11.5 Million
- Hit by Lightning: 1 in 960,000
- Hole in One: 1 in 12,500
- Random HIPAA Audit: 1 in 10,000
- Meaningful use Audit: 1 in 10
- Breach-Related Audit: 1 in ?
HIPAA Overview

- HIPAA
  - Protect patient confidentiality while furthering innovation and patient care.
- Omnibus
  - Business Associates must protect PHI.
- HITECH/Meaningful Use
  - Accelerate adoption of EHR (electronic Health records).
- Corrective Actions or Fines
HIPAA Enforcement

Who is being fined?

- Settlemens so far in 2016 have totaled more than any year prior $8,664,800

- Three Prison Sentences
- Medical License Revoked
- State Attorney General levying fines

“All too often we see covered entities with a limited risk analysis”

“Organizations must have in place compliant business associate agreements as well as an accurate and thorough risk analysis”

“We take seriously all complaints filed by individuals, and will seek the necessary remedies to ensure that patients’ privacy is fully protected.”

- Jocelyn Samuels, Director of OCR

* As of May 2016

Copyright 2007-2016
Compliance Group
855-85-HIPAA
www.compliancycroup.com
Why is Enforcement Up ↑

Anthem Blue cross Breach (2014)
• 1 in 4 Americans affected
• Omnibus Rule

Jocelyn Samuels New OCR Director (2015)
• “Education is over this is about enforcement”

Record Enforcement (2015)
• 3 Prison Sentences
• License revocation
• Heavy Fines
• Broad Targets

Phase 2 Audits (2016)
• CE’s & BA’s
• Increased Budget
• More Auditors
• We are all connected
Causes Of A HIPAA Audit

- Breach Notification
- Business Associates
- Phase 2 Random
- Meaningful Use Failure
- Reported
  - Whistleblower
  - Complaint

HHS is REQUIRED by law to investigate ALL HIPAA violation complaints
Phase 2 Random Audits

- Covered Entities and Business Associates will be randomly audited
- Began: March 22, 2016
- New funding for FCI federal to support the audits
- The friends you keep can get you audited

Audit Risk-O-Meter

Low  Medium  High

855-85-HIPAA
www.compliancygroup.com

Copyright 2007-2016
What If I Attest For Meaningful Use?

- Random **5-10%** of providers will be audited by CMS
  - Failure rate as high as **79%**
  - Failure may be reported to OCR
- Security Risk Assessment for Meaningful Use **DOES NOT** make you HIPAA Compliant
What Causes a HIPAA Audit?

- Complaint of Security/Privacy violation
  - HHS is REQUIRED by law to investigate ALL HIPAA violation complaints

- Whistleblower
  - Anonymous
  - % of Money Collected
Breach Notification Rule

- **Affects < 500 PHI**: must notify all breaches of calendar year by a deadline
- **Affects > 500 PHI**: must notify HHS immediately, publicized in HHS Wall of Shame

**Audit Risk-O-Meter**

Low | Medium | High

---

**HHS Breach Portal AKA “Wall of Shame”**
HHS Wall of Shame

- **56%**
  - Caused by Theft or Loss-related reasons

- **11%**
  - Caused by Hacking or IT incident

- **20%**
  - Involved Business Associates

I have to worry about... Business Associates?!

- > 59% of BAs reported a data breach in the last two years that involved the loss or theft of patient data.
- > 29% experienced two breaches or more.

Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data conducted by Ponemon Institute
Computer and Device Theft

- **90%** of Healthcare Professionals use personal phones for work
- **4.5 Million** smart phones lost/stolen (2013)
  - Only 11% use STRONG passwords
  - Only 7% used encryption
- **91.4%** of organizations report loss of mobile device(s)
- **1 out of 10** laptops are lost/stolen

http://www.naswassurance.org/malpractice/malpractice-tips/computer-device-theft/
Leading Causes Of Data Breaches

Since 2010

- 23% Data breaches due to hacking
- 68% Data breaches due to loss or theft.

- 48% involved Laptop/Desktop/Mobile Device

Causes Of A HIPAA Audit

Phase 2 Random

Business Associates

Meaningful Use Failure

Breach Notification

Reported
- Whistleblower
- Complaint

Audit Risk-O-Meter
- Low
- Medium
- High

HHS is REQUIRED by law to investigate ALL HIPAA violation complaints

855-85-HIPAA
www.compliancygroup.com
The Process Of An Audit

Desk Audit
Request for Gap and Remediation Report

On Site Audit
Review of all 7 Elements of Effective Compliance

Results
Corrective Action Plan | Fines
Laptop Theft

- **Who**: A radiation oncology private physician practice, Cancer Care Group, P.C.
- **What**: A laptop theft lead to breach
- **Why**: But lack of comprehensive risk analysis and device and media control policy lead to a steep penalty
- **Settlement**: $775,000 and CAP (Corrective Action Plan) (9/2/15)
Importance of BAA & Complete Risk Analysis

- **Who**: North Memorial Health Care of Minnesota
- **What**: Laptop theft, 6,497 patient records
- **Why**: No BAA with Billing firm, **failed to complete a risk analysis** to address all potential risks and vulnerabilities to ePHI
- **Settlement**: **$1,550,000 and CAP (3/19/16)**

“Two major cornerstones of the HIPAA Rules were overlooked by this entity,” said Jocelyn Samuels, Director of OCR. “Organizations must have in place compliant Business Associate Agreements as well as an accurate and thorough risk analysis that addresses their enterprise-wide IT infrastructure.

The NEED for BAAs

- **Who**: Raleigh Orthopaedic (North Carolina)
- **What**: Breach report, 17,300 patient records
- **Why**: Handed over x-rays and associated PHI to potential business partner without first executing a **business associate agreement**.
- **Settlement**: $750,000 and CAP (4/20/16)

“HIPAA’s obligation on covered entities to obtain business associate agreements is more than a mere check-the-box paperwork exercise,” said Jocelyn Samuels, Director of OCR. “It is critical for entities to know to whom they are handing PHI and to obtain assurances that the information will be protected.”

Avoidable Breach

- **Who**: Anchorage Community Mental Health Services (ACMHS) - Nonprofit org.
- **What**: Malware caused breach of unsecured ePHI
- **Why**: “ACMHS had adopted policies and procedures in 2005, but these policies and procedures were not followed and/or updated.” ACMHS could have avoided the breach (and not be subject to the settlement agreement), if it had followed its own policies and procedures
- **Settlement**: $150,000 and CAP (12/2014)
Physical Security

- **Who:** Lahey Hospital and Medical Center (Mass.)
- **What:** Portable CT scanner stolen from **unlocked room** overnight
- **Why:** Failure to conduct a thorough risk assessment for all ePHI, **failure to physically safeguard workstation** with ePHI, failure to implement unique user names to identify and track users, and failure to document workstation activity.
- **Settlement:** $850,000 and 3 year CAP (11/24/15)
How Do Your Patients Feel About HIPAA?

Are You Confident Your Healthcare Providers’ Security Measures Protect Your Medical Records

- Not confident: 68%

Did Your Provider’s Negligence Cause Or Contribute to Identify Theft

- Yes, they caused or contributed to it: 53%

HIPAA compliance as a differentiator

- Fitbit Inc. – announces its HIPAA compliance, stock price soared (26%)

The Seven Fundamental Elements of an Effective Compliance Program

Compliance according to HHS:

1. Implementing written policies, procedures and standards of conduct.
2. Designating a compliance officer and compliance committee.
3. Conducting effective training and education.
4. Developing effective lines of communication.
5. Conducting internal monitoring and auditing.
7. Responding promptly to detected offenses and undertaking corrective action.

*Source HHS & OIG
The HIPAA Compliance Puzzle

Audits
SRA (Security Risk Assessment), Administrative, Privacy

Remediation Plan

Incident Management & Remediation

Remediation Plan

Business Associate Management

Policies, Procedures & Training

Document Version
Employee Attestation & Tracking

Employee Attestation & Tracking

Compliancy Group
Achieve. Illustrate. Maintain. Compliance Simplified

855-85-HIPAA
www.compliancygroup.com

Copyright 2007-2016
Compliance Questions?

For more information, contact:

Marc Haskelson
855.854.4722 ext 507
marc@compliancygroup.com