Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

HIPAA Is Not Optional, It's REQUIRED

AOA excel
Your Business Advantage

855 85 HIPAA (855-854-4722)
www.CompliancyGroup.com

AOA excel
Endorsed Business Partner

HIPAA Compliance Simplified

Marc Haskelson, President Compliancy Group

Agenda

- Why HIPAA?
- Common misunderstandings
- What is a Audit?
- Real World Stories
- How do I protect my practice?

Compliancy Group

AOA excel
Endorsed Business Partner

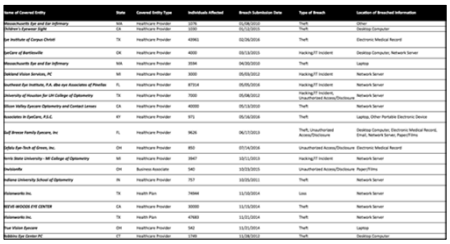
HHS Wall of Shame

	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	St. Joseph's Hospital and Medical Center	AZ	Healthcare Provider	623	02/13/2017	Unauthorized Access/Disclosure	Electronic Medical Record
	Benesch, Friedlander, Coplan & Aronoff LLP	OH	Business Associate	1134	02/10/2017	Theft	Paper/Films
	Family Medicine East, Chartered	KS	Healthcare Provider	6800	02/03/2017	Theft	Desktop Computer
	Catalina Post-Acute Care and Rehabilitation	AZ	Healthcare Provider	2953	02/02/2017	Improper Disposal	Paper/Films
	Jeffrey D. Rice, O.D., L.L.C.	OH	Healthcare Provider	1088	02/02/2017	Theft	Paper/Films
	Vertiv Co. Health & Welfare Plan	OH	Health Plan	955	01/31/2017	Unauthorized Access/Disclosure	Paper/Films
	WellCare Health Plans, Inc.	FL	Health Plan	24809	01/27/2017	Hacking/IT Incident	Network Server
	Shiel Sexton	IN	Health Plan	710	01/27/2017	Unauthorized Access/Disclosure	Other
	Synergy Specialists Medical Group, Inc / Jay S. Bererter, DPM	CA	Healthcare Provider	569	01/27/2017	Hacking/IT Incident	Email
	Princeton Pain Management	NJ	Healthcare Provider	4668	01/27/2017	Hacking/IT Incident	Desktop Computer, Electronic Medical Record
	THE R.O.A.D.S. Foundation Inc. DBA R.O.A.D.S. Community Care Clinic	CA	Healthcare Provider	670	01/26/2017	Loss	Paper/Films
	MultiCare Health System	WA	Healthcare Provider	1249	01/26/2017	Hacking/IT Incident	Email
	Roper St. Francis Healthcare	SC	Healthcare Provider	576	01/24/2017	Loss	Other Portable Electronic Device
	Stephenville Medical & Surgical Clinic	TX	Healthcare Provider	79000	01/23/2017	Unauthorized Access/Disclosure	Desktop Computer
	Multnomah County	OR	Healthcare Provider	1700	01/20/2017	Unauthorized Access/Disclosure	Email
	Wonderful Center For Health Innovation	CA	Healthcare Provider	3368	01/20/2017	Theft	Laptop
	Covenant Medical Center, Inc.	MI	Healthcare Provider	6197	01/20/2017	Unauthorized Access/Disclosure	Electronic Medical Record
	Associated Catholic Charities Incorporated	MD	Healthcare Provider	1143	01/20/2017	Unauthorized Access/Disclosure	Email
	Trihealth, Inc.	OH	Healthcare Provider	1126	01/19/2017	Unauthorized Access/Disclosure	Network Server, Paper/Films

Compliancy Group

AOA excel
Endorsed Business Partner

HHS Wall of Shame



Based on HHS Breach Portal: Breaches Affecting 500 or More Individuals, "Type of Breach" https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Are YOU HIPAA Compliant?

We are HIPAA compliant...

Risk Assessments

- I had an expensive Security Risk Assessment done
- Am I HIPAA compliant?

Payment Summary

Please review the following details for this transaction.

Description	Item Price
Remote Risk Assessment $4000	$4,000.00
Total	$4,000.00

Policies & Procedures

- I have a Manual, I am compliant "right"?

Workforce Training

- I paid for my employees HIPAA training, I am compliant.

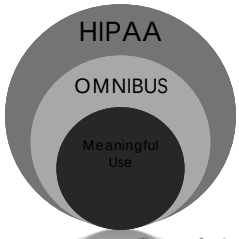
* Cost for 10 employee practice

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 & CAP (Corrective Action Plan)**

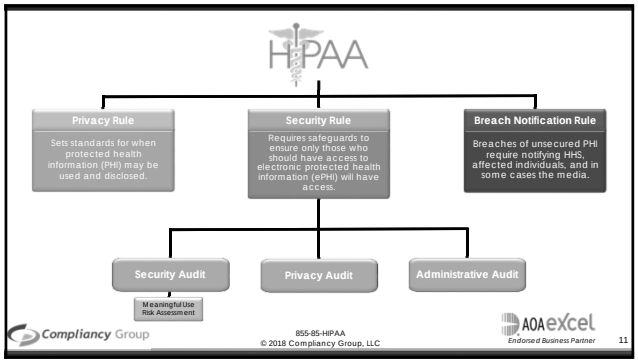
What is HIPAA Compliance and what is NOT

- **HIPAA/HITECH**
  - Protect patient confidentiality while furthering innovation and patient care
  - Privacy Rule and Security Rule
- **Omnibus**
  - Business Associates must be HIPAA compliant
  - Covered Entities must have BAAs
    - Conduct Due Diligence
  - Breach Notification Rule
- **Meaningful Use**
  - Accelerate adoption of EHR (electronic Health records)
- **Compliance vs. Security**
  - Fines vs. Risk



Compliancy Group
855-85-HIPAA

AOA excel Endorsed Business Partner
10



Compliancy Group
855-85-HIPAA

AOA excel Endorsed Business Partner
11

What Information Does HIPAA Protect?

PHI may include any of the following:

- Names
- Addresses
- Dates of Service
- Telephone Numbers
- Fax Numbers
- Email Addresses
- Social Security Numbers
- Medical Record Numbers
- Health Plan Beneficiary Numbers
- Account Numbers
- Certificate/License Numbers
- Vehicle identifiers/Serial Numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers;
- Biometric identifiers
- Full Face Photos or Videos
- Any other unique identifying number, characteristic, or code

Compliancy Group
855-85-HIPAA

AOA excel Endorsed Business Partner
12

Compliance vs. Security

- Audits
  - Security, Privacy, and Administrative
- Gap Identification
- Remediation
- Policies & Procedures
- Employee Training & Attestation
- Business Associate Management
  - BA Agreements & Audit
- Incident Management

- Security Risk Analysis
  - Penetration Testing
  - Vulnerability Scan
- Network Security
- Managed Services
- IT Consulting
- Cloud Services

Security Risk Assessment

FINES → **REPUTATION** ← RISK

Security AND Privacy Rule

- Who: **Insurance** company, Triple-S (Puerto Rico)
- What/Why: Widespread non-compliance
  - Failure to implement **Administrative**, **Privacy**, and **Technical** safeguards
  - Lack of appropriate **Business Associate Agreements**
  - Failure to conduct **accurate/thorough Risk Analysis**
- Settlement: **$3.5 Million & CAP** (11/30/15)

*"This case sends an important message for HIPAA Covered Entities not only about compliance with the requirements of the **Security Rule**, including risk analysis, but compliance with the requirements of the **Privacy Rule**, including those addressing **business associate agreements** and the minimum necessary use of protected health information."*

- Jocelyn Samuels, Director of OCR

Improper Disclosure Of PHI

- Who: Feinstein Institute for **Medical Research**
- What: **Laptop stolen from car contained** (13,000 PHI) of research participants. **Password-protected but not encrypted**
- Why: Failed to reasonably safeguard PHI;
  - **Lacked policies & procedures** for ePHI access
  - **Failed to implement policies and procedures** to safeguard ePHI
- Ruling: **$3.9 Million & CAP** (3/17/16)

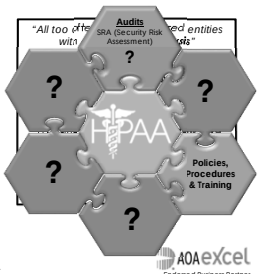
*"**Research institutions** subject to HIPAA must be held to the **same compliance standards as all other HIPAA-covered entities**," said OCR Director Jocelyn Samuels. "For individuals to trust in the research process and for patients to trust in those institutions, they must have some assurance that their information is kept private and secure."*

http://www.crainsnewyork.com/article/20160318/ECONOMY/160319845/the-feinstein-institute-for-medical-research-pays-3-9-million-to-settle-data-breach-one-of-the-largest-sums-ever-paid

Why Should I Worry About HIPAA?

HIPAA is the Law

- **Current market solutions often only address *pieces* of compliance**
- **Enforcement is on the rise ↑**
  - Record fines levied: ***400% increase***
    - **$6.2 Million** in 2015
    - **$24 Million** in 2016
    - **$11.4 Million** so far in 2017*
  - Three prison sentences
  - Medical license revoked
  - State Attorney General levying fines



http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

HIPAA Enforcement

- **$24 Million** in 2016 – 400% increase
- **$11.4 Million** so far in 2017

*"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

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

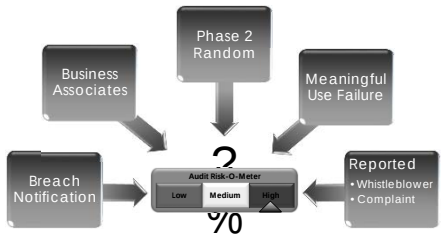
The Seven Fundamental Elements of an Effective Compliance Program

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.*
6. *Enforcing standards through well-publicized disciplinary guidelines.*
7. *Responding promptly to detected offenses and undertaking corrective action.*

*Source HHS & OIG

Causes Of A HIPAA Audit



Compliancy Group
855-85-HIPAA

AOA excel Endorsed Business Partner
19

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

Compliancy Group
855-85-HIPAA

AOA excel Endorsed Business Partner
20

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 & 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.*

http://www.hhs.gov/about/news/2016/03/16/155-million-settlement-underscores-importance-executing-hipaa-business-associate-agreements.html

Compliancy Group
855-85-HIPAA

AOA excel Endorsed Business Partner
21

Risk Analysis is NOT Enough

- Who: OHSU (Oregon Health & Science University)
- What: Reports of **unencrypted laptops, stolen unencrypted thumb drive**, 1,361 patient records
- Why: Conducted **SIX** risk analysis in (2003, 2005, 2006, 2008, 2010, 2013) but did not address the widespread vulnerabilities**.** Also, lacked **policies & procedures.** Lack of **BAA.**
- Settlement: **$2.7 Million & CAP** (7/18/16)

*"From well-publicized large scale breaches and findings in their own risk analyses, OHSU **had every opportunity to address security** management processes that were insufficient. Furthermore, OHSU should have addressed the lack of a business associate agreement before allowing a vendor to store ePHI," said OCR Director Jocelyn Samuels. "This settlement underscores the importance of leadership engagement and why it is so critical for the C-suite to **take HIPAA compliance seriously**."*

http://www.hhs.gov/about/news/2016/07/18/widespread-hipaa-vulnerabilities-result-in-settlement-with-oregon-health-science-university.html

Unauthorized Patient Testimonials

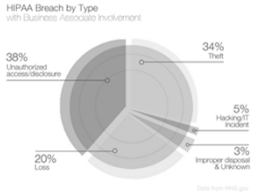
- Who: Complete P.T. Pool & Land **Physical Therapy**
- What: **Posted patient testimonials** (including names/photos) on website without authorization.
- Why: Failed to reasonably safeguard PHI;
  - **Impermissibly disclosed PHI without authorization;**
  - **Failed to implement policies and procedures** to comply with HIPAA regarding authorization
- Ruling: **$25,000 & CAP** (2/16/16)

*"The **HIPAA Privacy Rule gives individuals** important **controls** over whether and how their protected health information is **used and disclosed for marketing** purposes," said OCR Director Jocelyn Samuels. "With limited exceptions, the Rule requires an individual's **written authorization** before a use or disclosure of his or her protected health information can be made for marketing."*

http://www.healthcarepinews.com/news/physical-therapist-pay-25000-over-unauthorized-patient-testimonials

But…It Probably Won't Happen To Me

- In a recent study, **more than half** of business associates (**59%**) reported a data breach in the last two years that involved the loss or theft of patient data. More than a quarter (**29%**) experienced two breaches or more.
- Of the 345 incidents reported by HHS and listed on their site under Breaches Affecting 500 or More Individuals, 74 involved a business associate (**21%**).



Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data conducted by Ponemon Institute
http://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf

The Need For BAAs

- Who: Raleigh Orthopaedic (North Carolina)
- What/Why: 17,300 patients affected
  - Handed over PHI to potential business partner without first executing a **business associate agreement**.
- Settlement: **$750,000 & 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."

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/raleigh-orthopaedic-clinic-bulletin/index.html

Tardy Breach Notification = 1st Fine Of 2017

- Who: Presence Health
- What: **Missing paper schedules** (836 PHI)
- Why: **Failed to notify within 60 days** of discovery:
  - **Media outlets**
  - **OCR**
  - **Individuals affected**
- Settlement: **$475,000 & CAP** (1/9/17)

*"Covered entities need to have a clear policy and procedures in place to respond to the **Breach Notification Rule's timeliness requirements**" said OCR Director Jocelyn Samuels. "**Individuals need prompt notice of a breach** of their unsecured PHI so they can take action that could help mitigate any potential harm caused by the breach."*

https://www.hhs.gov/about/news/2017/01/09/first-hipaa-enforcement-action-lack-timely-breach-notification-settles-475000.html

PHI MUST Be Safeguarded

- Who: MAPFRE (Insurance Company of Puerto Rico)
- What: **USB drive stolen** (2,209 PHI)
- Why: **Failure to conduct Risk Analysis;**
  - Failure **to implement risk management plans**
  - Failure to deploy **encryption** on PHI devices
  - **Failed to implement/delayed implementing corrective measures**
- Settlement: **$2.2 Million & CAP** (1/18/17)

*"Covered entities must not only make assessments to safeguard ePHI, they must act on those assessments as well" said OCR Director Jocelyn Samuels. "OCR works tirelessly and collaboratively with covered entities to **set clear expectations and consequences**."*

https://www.hhs.gov/about/news/2017/01/18/hipaa-settlement-demonstrates-importance-implementing-safeguards-ephi.html

Solving The HIPAA Compliance Puzzle

Compliancy Group

855-85-HIPAA

AOA excel
Endorsed Business Partner

28