Compliancy Group
Achieve.Illustrate.Maintain.
Compliance Simplified

AOA eXcel

Industry leading Education
Today's Webinar

- **Understanding HIPAA Privacy & Security**

Webinars

- Upcoming & past webinars: http://compliancy-group.com/webinar/

Compliancy Group

We simplify compliance so you can confidently focus on your business.

Started in 2005 by HIPAA auditors & Compliance experts

- Market need of a solution - for the client
  - **The Guard**: cloud-based solution
- Proprietary **Achieve**, **Illustrate** and **Maintain** methodology
- Confidently satisfy HIPAA, HITECH and Omnibus regulations

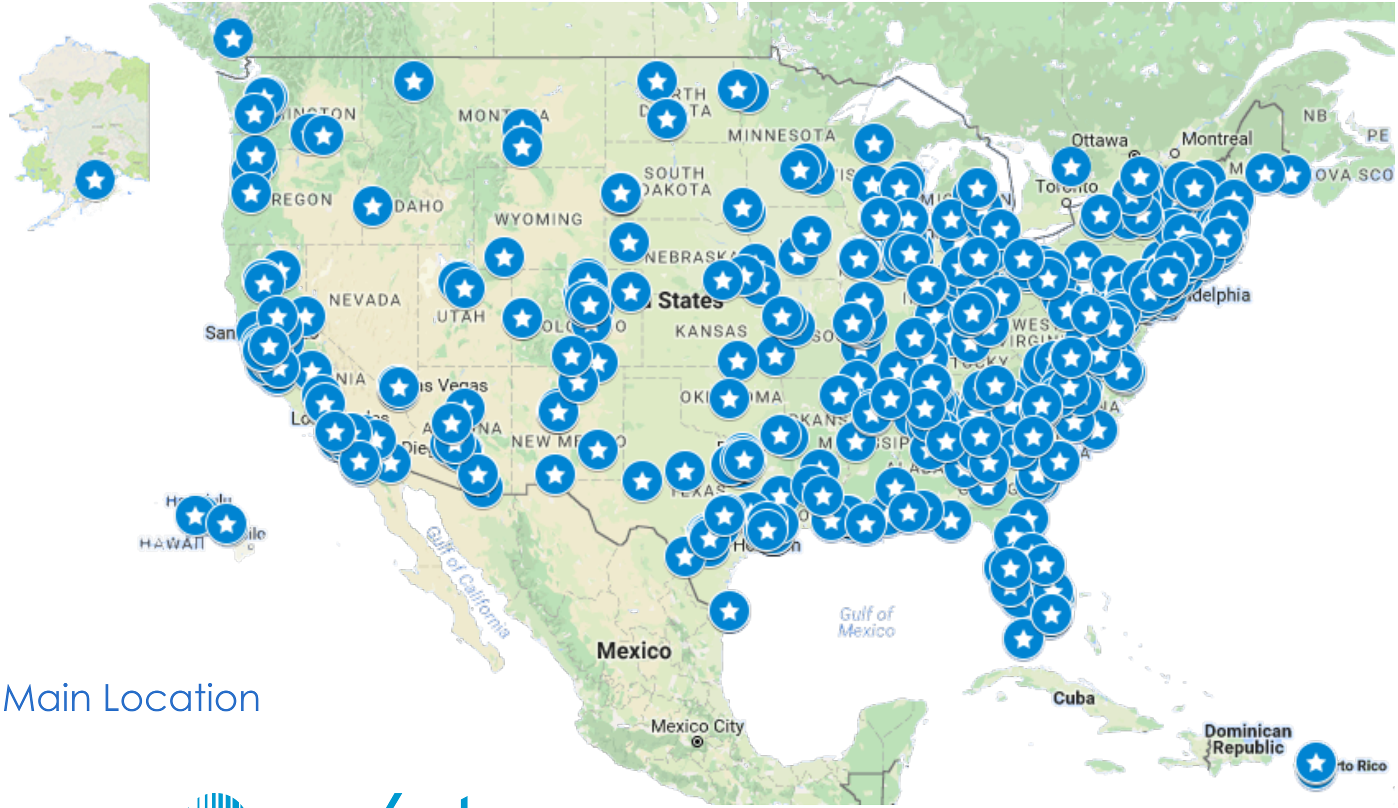
Compliance is our business

- **No client has ever failed an OCR or CMS audit**
- 100% of our clients would refer us to a friend
- **Recognized Leader** of Compliance
  - Top Compliance Tools & Emerging Vendor
  - Subject-Matter Expert referenced in multiple publications
  - **Endorsed by Industry Leaders and Associations**

Compliancy Group Endorsed Business Partner of AOA eXcel

855-85-HIPAA

Compliance Across North America



Client's Main Location

HHS Wall of Shame

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Massachusetts Eye and Ear Infirmary	MA	Healthcare Provider	1076	01/08/2010	Theft	Other
Children's Eyewear Sight	CA	Healthcare Provider	1030	01/12/2015	Theft	Desktop Computer
Eye Institute of Corpus Christi	TX	Healthcare Provider	43961	02/26/2016	Theft	Electronic Medical Record
EyeCare of Bartlesville	OK	Healthcare Provider	4000	03/13/2015	Hacking/IT Incident	Desktop Computer, Network Server
Massachusetts Eye and Ear Infirmary	MA	Healthcare Provider	3594	04/20/2010	Theft	Laptop
Oakland Vision Services, PC	MI	Healthcare Provider	3000	05/03/2012	Hacking/IT Incident	Network Server
Southeast Eye Institute, P.A. dba eye Associates of Pinellas	FL	Healthcare Provider	87314	05/05/2016	Hacking/IT Incident	Network Server
University of Houston for UH College of Optometry	TX	Healthcare Provider	7000	05/08/2012	Hacking/IT Incident, Unauthorized Access/Disclosure	Network Server
Silicon Valley Eyecare Optometry and Contact Lenses	CA	Healthcare Provider	40000	05/13/2010	Theft	Network Server
Associates In EyeCare, P.S.C.	KY	Healthcare Provider	971	05/16/2016	Theft	Laptop, Other Portable Electronic Device
Gulf Breeze Family Eyecare, Inc	FL	Healthcare Provider	9626	06/17/2013	Theft, Unauthorized Access/Disclosure	Desktop Computer, Electronic Medical Record, Email, Network Server, Paper/Films
Cefalu Eye-Tech of Green, Inc.	OH	Healthcare Provider	850	07/14/2016	Unauthorized Access/Disclosure	Electronic Medical Record
Ferris State University - MI College of Optometry	MI	Healthcare Provider	3947	10/11/2013	Hacking/IT Incident	Network Server
EnvisionRx	OH	Business Associate	540	10/23/2015	Unauthorized Access/Disclosure	Paper/Films
Indiana University School of Optometry	IN	Healthcare Provider	757	10/25/2011	Theft	Network Server
Visionworks Inc.	TX	Health Plan	74944	11/10/2014	Loss	Network Server
REEVE-WOODS EYE CENTER	CA	Healthcare Provider	30000	11/15/2014	Theft	Network Server
Visionworks Inc.	TX	Health Plan	47683	11/21/2014	Theft	Network Server
True Vision Eyecare	OH	Healthcare Provider	542	11/21/2014	Theft	Laptop
Robbins Eye Center PC	CT	Healthcare Provider	1749	11/28/2012	Theft	Desktop Computer

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

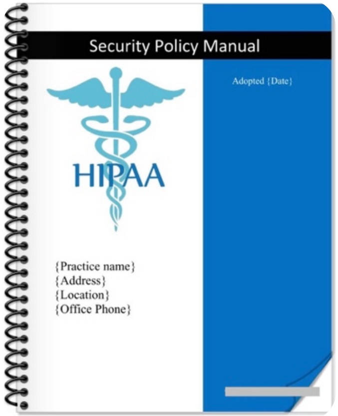
- I had an expensive Security Risk Assessment done
- Am I HIPAA compliant?

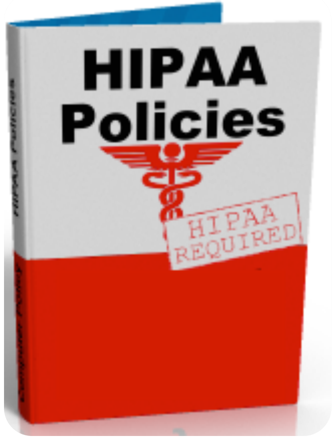
Payment Summary

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.

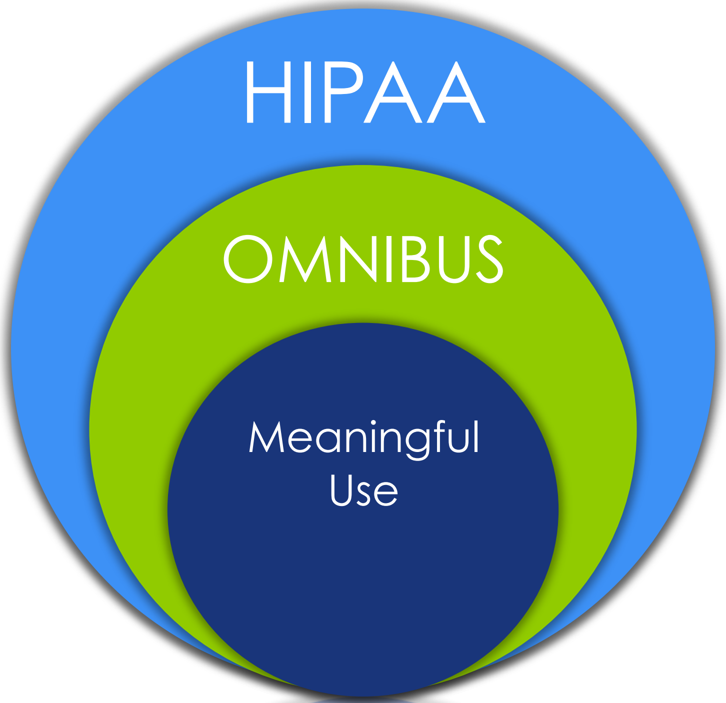
* Cost for 10 employee practice

Avoidable Breach

- Who: Anchorage Community Mental Health Services (ACMHS) - **Nonprofit** org. **(Alaska)**
- 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)** (12/2014)

What is HIPAA Compliance and what is NOT

- **Compliance vs. Security**
  - Fines vs. Risk
- **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

- 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

HIPAA

Privacy Rule

Sets standards for when protected health information (PHI) may be used and disclosed.

Security Rule

Requires safeguards to ensure only those who should have access to electronic protected health information (ePHI) will have access.

- **Security Audit**
  - Meaningful Use Risk Assessment
- **Privacy Audit**
- **Administrative Audit**

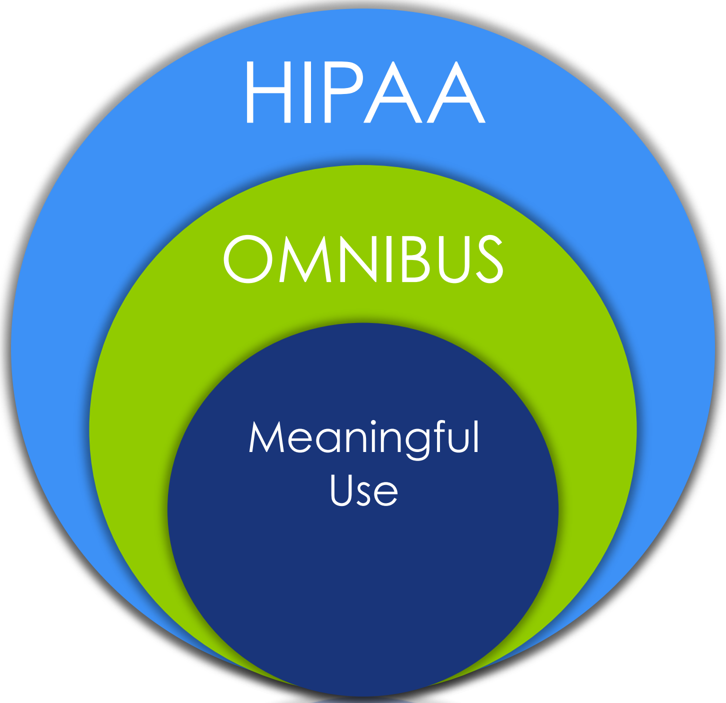
Breach Notification Rule

Breaches of unsecured PHI require notifying HHS, affected individuals, and in some cases the media.

855-85-HIPAA

What is HIPAA Compliance and what is NOT

- **Compliance vs. Security**
  - Fines vs. Risk
- **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)



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)

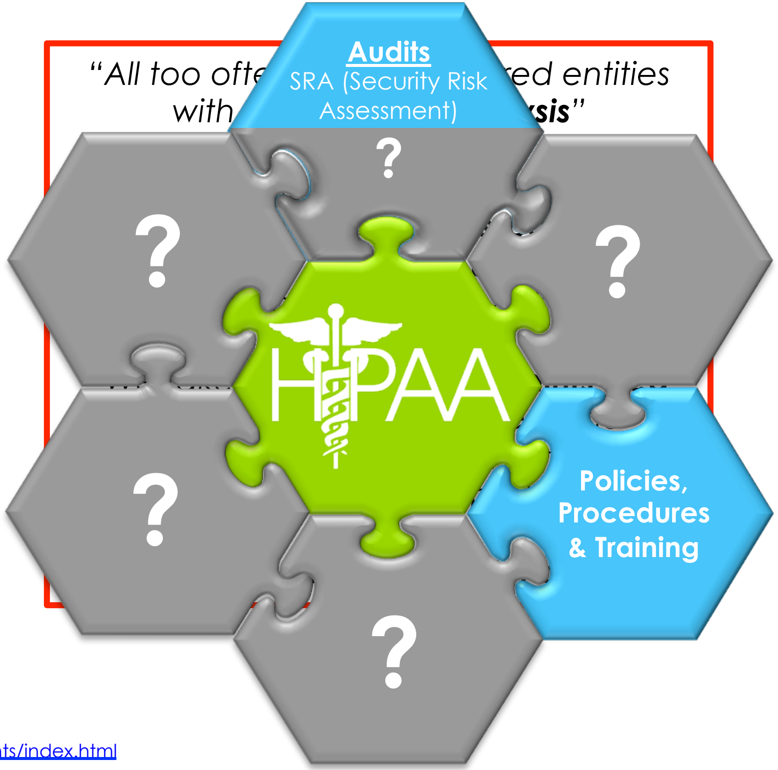
*"This case sends an important message for HIPAA Covered Entities not only about compliance with the requirements of the **Security Rule**, including risk analysis, but compliance with the requirements of the **Privacy Rule**, including those addressing **business associate agreements** and the minimum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

- Jocelyn Samuels, Director of OCR

Why Should I Worry About HIPAA?

HIPAA is the Law

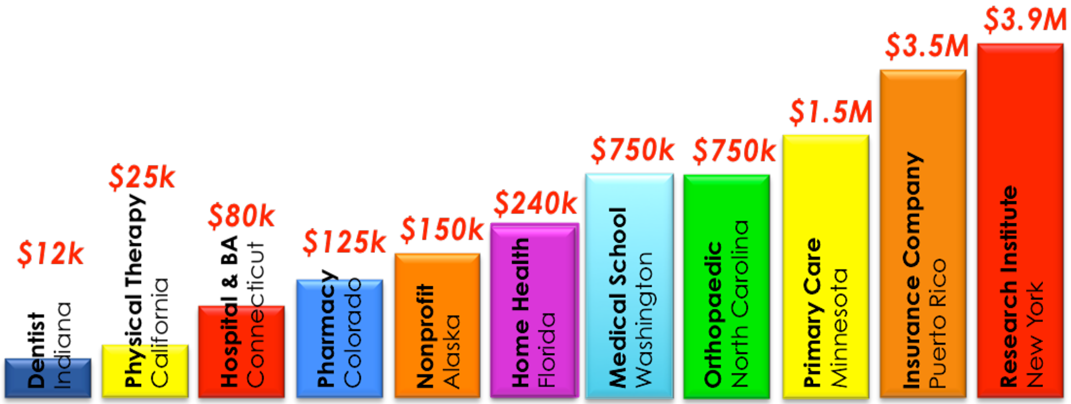
- **Current market solutions often only address *pieces* of compliance**
- **Enforcement is on the rise ↑**
  - Record fines levied: **$20,264,800** this year*
  - Three prison sentences
  - Medical license revoked
  - State Attorney General levying fines



* As of August 2016, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

HIPAA Enforcement

Who is being fined?



- Settlements so far in 2016 have totaled **more than any year prior: $20,264,800**

*"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

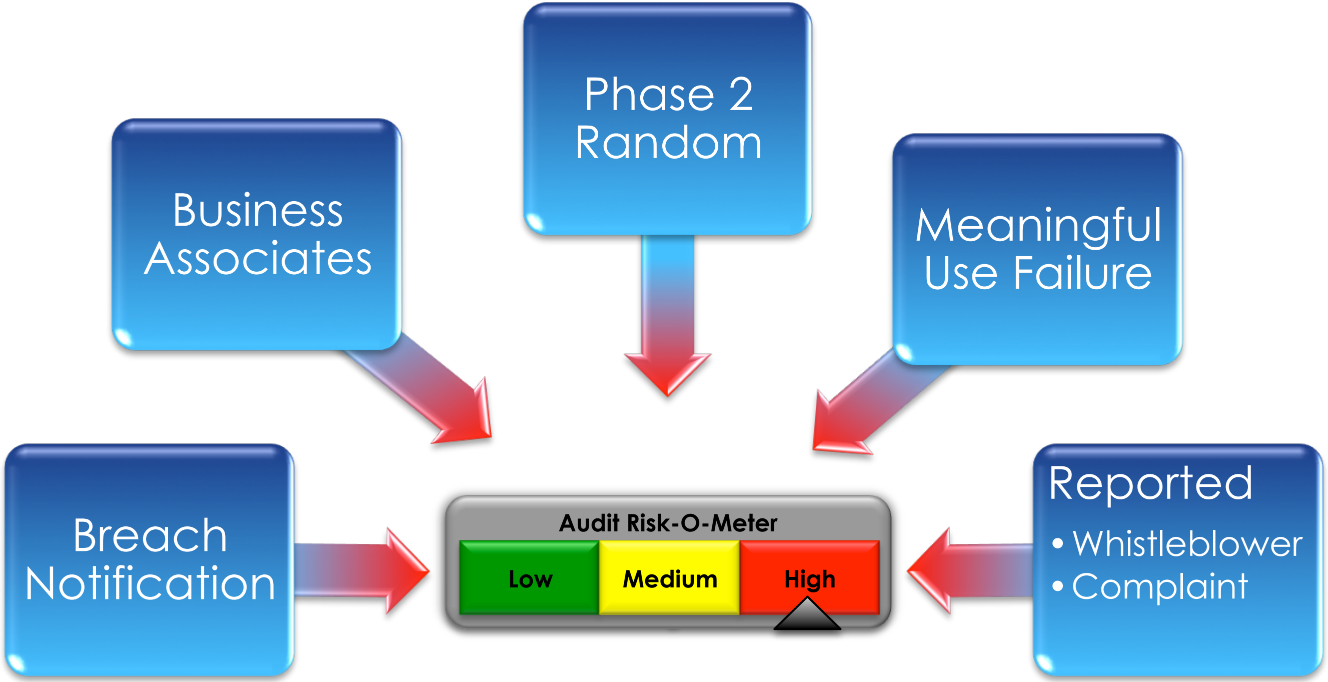
The Seven Fundamental Elements of an Effective Compliance Program

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



The Process Of An Audit

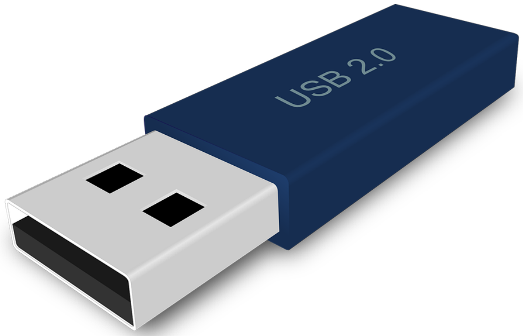
Desk Audit
Request for Gap and Remediation Report

On Site Audit
Review of all 7 Elements of Effective Compliance

Results	
Corrective Action Plan	Fines

Risk Analysis is NOT Enough

- Who: OHSU (Oregon Health & Science University)
- What: **Unencrypted laptops, 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: **$1,550,000 & CAP** (3/19/16)

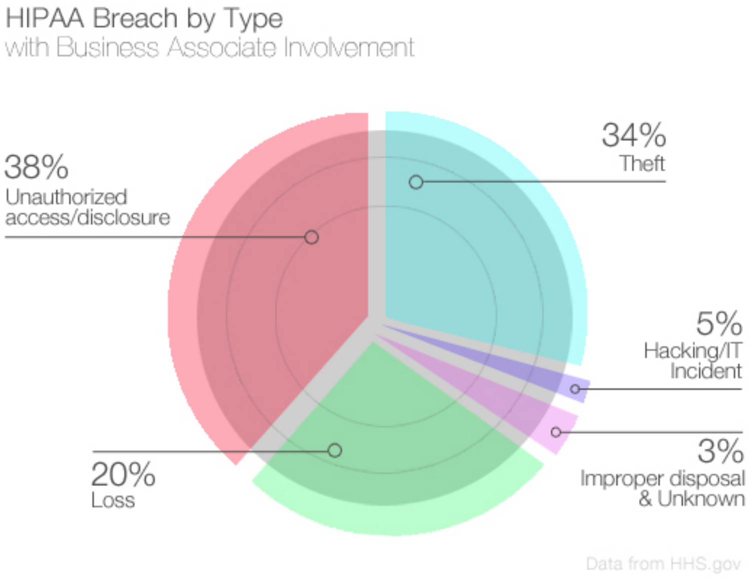


*"From well-publicized large scale breaches and findings in their own risk analyses, OHSU **had every opportunity to address security** management processes that were insufficient. Furthermore, OHSU should have addressed the lack of a business associate agreement before allowing a vendor to store ePHI," 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

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

Solving The HIPAA Compliance Puzzle

Thank You For Your Time!

Questions?

Compliancy Group
855-85-HIPAA
855-854-4722
info@compliancygroup.com
www.CompliancyGroup.com

Marc Haskelson
President & CEO
855-854-4722 Ext 507
Marc@compliancygroup.com