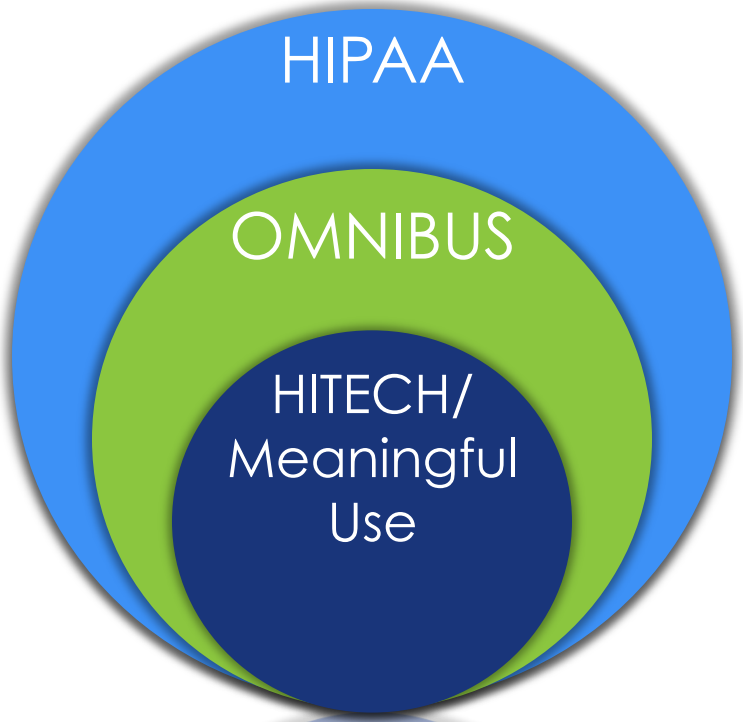
HIPAA Compliance for Business Associates: The Value of compliance, how to acquire and retain clients!

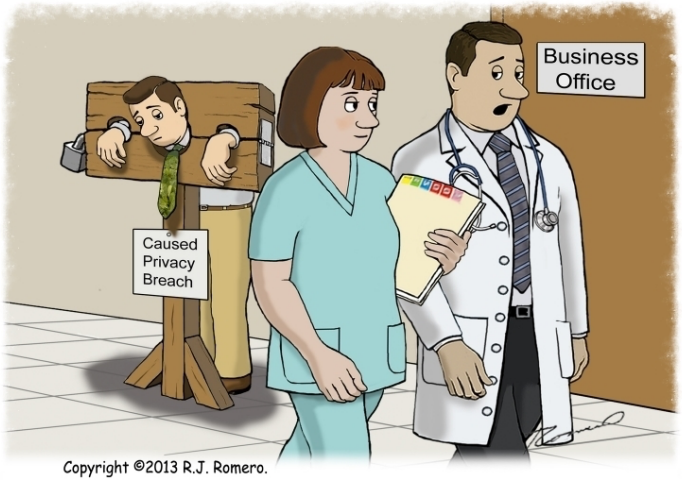
HIPAA & HITECH

- 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).
- Penalties or Incentives for adherence



Before/After Omnibus Rule

- **Before Omnibus**: BAs/Subcontractors regulated through Business Associate Agreements (BAAs)
- **After Omnibus**: BAs/Subcontractors are now regulated directly under HIPAA:
  - Comply with HIPAA Security Rule
  - Comply with a specific section of the HITECH Breach Notification Rule
  - Comply with all applicable provisions of the Privacy Rule
- **Substantially increased the magnitude of HIPAA enforcement risk and liability**



"I heard the new HIPAA Omnibus Rules are a whole lot tougher on business associates."

BAAs

Business Associate Agreements: Agreement between the CE and BA to govern the BA's creation, use, maintenance and disclosure of PHI.

- Must comply with HIPAA Security and Privacy Rules
- BAAs have **ALWAYS** been required by HIPAA
- After Omnibus – Require **reciprocal monitoring** by the BA & CE
- Subcontractors of BAs are treated as BAs as well

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

Compliance + Security

- Audits
  - Security/Administrative/Privacy
- Gap identification and Remediation
- Policies & Procedures
- Employee Training & Attestation
- Incident Management
- Business Associate Management

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

Trends in HIPAA Enforcement

HIPAA compliance as a **differentiator**

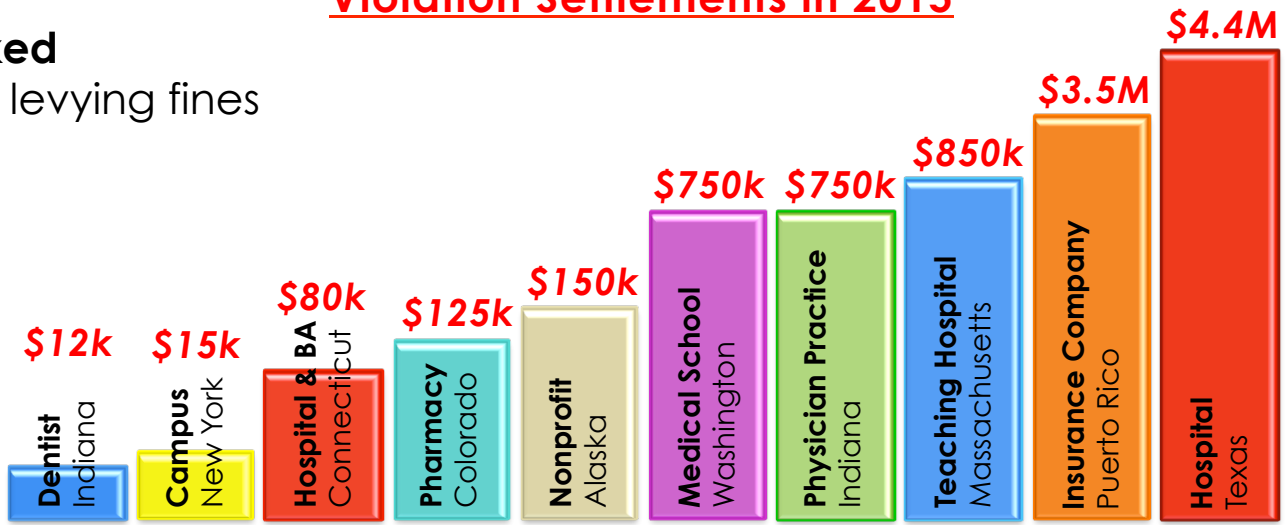
- **Fitbit Inc.** – announces its HIPAA compliance, stock price soared (26%)

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

1 in 4 Americans

Affected by Anthem Breach

Violation Settlements in 2015



Phase 2 Audits - **NOW**

- Began: March 22, 2016
- Covered Entities will receive an email from OCR to verify their contact information; Business Associates as well
- **Failure to respond will not exclude you from potentially being audited, OCR will simply use publicly available information**

"The 2016 Phase 2 HIPAA Audit Program will review 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."

DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF THE SECRETARY

Voice – (202) 619-0403 TDD – (202) 619-2357 FAX – (202) 619-3818
http://www.hhs.gov/ocr

Director
Office for Civil Rights
200 Independence Ave., SW; RM 509F
Washington, DC 20201

DATE

Contact Person's Name
CE/BA Name
Address
City, State ZIP

Dear Contact:

This is an automated communication from the Office for Civil Rights (OCR).

According to our records, you are the primary contact OCR should use to reach Entity Name regarding its potential inclusion in the HIPAA Privacy, Security, and Breach Notification Rules Audit Program. We are attempting to verify this email address.

Please respond within fourteen (14) days as instructed below to either confirm your identity and email address or instead provide updated primary and secondary contact information.

If you ARE the primary contact for this organization, please select the following link YES. Once the link is selected, a browser window will open and your response will be recorded.

If you ARE NOT the primary contact for this organization, please select the following link NO. Once the link is selected, a browser window will open and your response will be recorded.

Thank you for your cooperation. If we do not receive a response from you we will use this email address for future communications with this entity. Failure to respond will not shield your organization from selection.

If you have questions or comments regarding this message, you may contact us at OSOCRAudit@hhs.gov.

Sincerely,

Jocelyn Samuels
Director
Office for Civil Rights
OFFICE OF THE SECRETARY
Department of Health and Human Services
http://www.hhs.gov/ocr

Why Should I Care?

- Your clients are at risk
- You are at risk
- Limit your liabilities
  - Protect PHI, reputation damage, $$$ penalties

This is a Federal Mandate, NOT optional

"Business Associates are on the hook for HIPAA violations."

What Are My Liabilities?

Business associates are directly liable for:

1. Impermissible uses and disclosures
2. Failure to provide breach notification to the CE
3. Failure to provide access to a copy of ePHI to either the CE the individual, or the individual's designee
4. Failure to disclose PHI where required by the HHS to investigate or determine the BA's HIPAA compliance
5. Failure to follow Minimum Necessary standard when using or disclosing
6. Failure to provide an accounting of disclosures

Insurance Holding Company

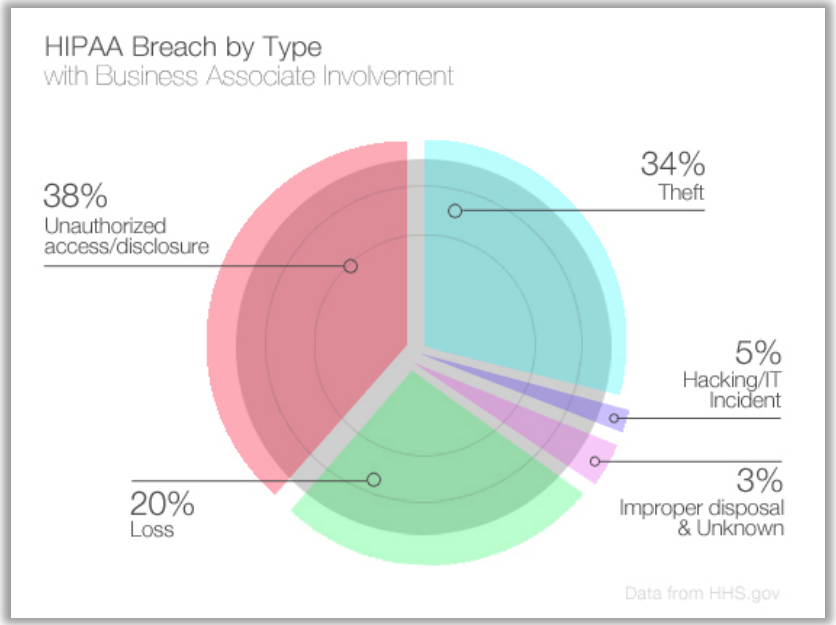
- Insurance company, Triple-S (Puerto Rico)
- Widespread non-compliance
  - Failure to implement Administrative, Privacy, and Technical safeguards
  - Lack of appropriate **Business Associate Agreements**
  - Failure to conduct accurate/thorough Risk Analysis
- Settlement: **$3.5 Million** (11/30/15)

"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." said OCR Director Jocelyn Samuels.

http://www.hhs.gov/about/news/2015/11/30/triple-s-management-corporation-settles-hhs-charges.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

HHS Wall of Shame

Breach Report Results

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Target Corporation Health Plan	MN	Business Associate	719	04/05/2016	Unauthorized Access/Disclosure	Paper/Films
Sisters of Charity of Leavenworth Health System Health Benefits Plan	CO	Business Associate	540	04/05/2016	Unauthorized Access/Disclosure	Paper/Films
Metropolitan Jewish Health System, Inc. d/b/a MJHS	NY	Business Associate	2483	03/22/2016	Hacking/IT Incident	Email
DataStat, Inc.	MI	Business Associate	552	02/12/2016	Unauthorized Access/Disclosure	Paper/Films
BlueCross BlueShield of South Carolina	SC	Business Associate	998	02/12/2016	Unauthorized Access/Disclosure	Paper/Films
SEIM JOHNSON, LLP	NE	Business Associate	30972	02/08/2016	Theft	Laptop
Buchness, Mary Ruth	NY	Healthcare Provider	14910	12/11/2015	Unauthorized Access/Disclosure	Email
Midlands Orthopaedics, P.A.	SC	Healthcare Provider	3902	11/13/2015	Hacking/IT Incident	Network Server
EnvisionRx	OH	Business Associate	540	10/23/2015	Unauthorized Access/Disclosure	Paper/Films
Insurance Data Services	MI	Business Associate	2918	10/08/2015	Theft	Paper/Films
Sunquest Information Systems	AZ	Business Associate	2100	09/24/2015	Theft	Laptop
Melanie Witte (attorney on behalf of EBPMA)	CA	Business Associate	1494	07/29/2015	Unauthorized Access/Disclosure	Laptop
Medical Informatics Engineering	IN	Business Associate	3900000	07/23/2015	Hacking/IT Incident	Electronic Medical Record, Network Server
Heartland Dental, LLC	IL	Business Associate	2860	06/24/2015	Hacking/IT Incident	Network Server

Importance of BAA & Complete Risk Analysis

- North Memorial Health Care of Minnesota
- Laptop theft, 6,497 patient records
- No **BAA** with Billing firm
- Failed to complete a risk analysis to address all potential risks and vulnerabilities to ePHI
- Settlement: **$1,550,000** (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

The NEED for BAAs

- Raleigh Orthopaedic (North Carolina)
- 17,300 patient records
- Handed over x-rays and associated PHI to potential business partner without first executing a business associate agreement.
- Settlement: **$750,000** (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

What's The Big Deal About HIPAA?

- **Federal Mandate "LAW"**
  - Heavy Enforcement
- In the News
- Reputation & Fines
- CRN 2015 Fastest growing sector

Benefits Of Being Compliant

- Differentiate yourself: You become more credible than your competitors
  - Announce your compliance
- Retain current clients
- New revenue streams

Differentiate Your Company

Dropbox now supports HIPAA and HITECH Act compliance

Tolga Erbay | November 6, 2015 | 0 comments 49 114 2

Cirracore Announces **HIPAA** / HITECH **Compliance**
PR Web (press release) - Apr 4, 2016
An **independent auditing** firm Tuttle Consulting performed the **audits** and confirmed Cirracore's **compliance** with the **HIPAA** HITECH standards.

Fitbit is now **HIPAA** compliant—is your business?
CIO - Oct 2, 2015
Fitbit's announcement of its **HIPAA compliance** underscores the need for companies to **comply** with **HIPAA** when they use protected data, even ...

Commonwealth Computer Recycling Offers Free, **HIPAA-Compliant ...**
Digital Journal - 3 hours ago
Greensburg, PA -- (ReleaseWire) -- 04/20/2016 -- As part of its celebration of Earth Day, Commonwealth Computer Recycling is offering free mail-in e-waste ...

Mimecast Completes **HIPAA** Security **Compliance** Assessment and **...**
Business Wire (press release) - Apr 12, 2016
... Act (**HIPAA**) Security **Compliance** Assessment and Service Organization Control 2 Type 1 (SOC 2 Type 1) **Independent** Service **Audit**.

FormAssembly **Announces HIPAA Compliant** Enterprise Form **...**
SYS-CON Media (press release) - Apr 12, 2016
BLOOMINGTON, Ind., April 12, 2016 /PRNewswire-iReach/ -- Veer West LLC **announced** today the availability of a new **HIPAA compliant** ...

Aternity® **Announces HIPAA-Compliant** End User Experience **...**
Business Wire (press release) - Mar 1, 2016
Healthcare organizations looking for a **HIPAA-compliant** End User Experience Monitoring solution can turn to Aternity to ensure that they ...

HIPAA compliance as a **differentiator**

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

MSP/ Service Provider

- Beat the competition
- New Market Opportunities
- Recurring Revenue
- Scalable offering
- Higher Margins

Apex Technology Management, Inc.

BUSINESS CONTINUITY SERVICES OF TEXAS, INC.

Building resilient communities one business at a time.

"We see The Guard as a solution that remedied our concerns about providing compliance support for our clients that also suited their needs to a tee. Liability has never been an issue, and Compliancy Group's proven track record of not having a single client ever fail an OCR audit has proven true with our clients as well. They cared about fitting The Guard into our pre-existing business, and with the marketing and sales support they've even held private webinars just for the benefit of our clients. Compliancy Group and their team of Compliance Coaches has let us focus on the security work we've always provided while enhancing our offerings with a powerful total compliance solution that we know will work for our clients."– George Passidakis, Director of Sales and Market

Adding Compliance To Your Offerings

- Increase stickiness of clients
- Added value to your offerings
- Your clients are compliant and so are you!
  - Limit liability for all parties
- New revenue stream

How Do I Become Compliant?

Business Associate Compliance Requirements:

- Audits
  - Security Risk Assessment and Administrative Assessment
- Identify deficiencies
- Create remediation plans
  - Security and Administrative
- Policies and Procedures
- Employee Training
- Identify CEs and BAs (BAAs)
- Incident Management
- Review of compliance – Annual/periodic

Solving The HIPAA Compliance Puzzle

Compliance Questions?

For more information, contact:

Marc Haskelson
855.854.4722 ext 507
marc@compliancygroup.com