Legal Disclaimer

This information does not constitute legal advice and is for educational purposes only. This information is based on current federal law and subject to change based on changes in federal law or subsequent interpretative guidance. Since this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource regarding the matters covered, and may not be tailored to your specific circumstance. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED HEREIN IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.
Your Presenters

Michelle Caswell, Senior Director Legal & Compliance | JD
- More than 15 years healthcare experience
- Extensive experience in HIPAA Privacy, Security and Breach Notification Rules
- Experienced Principal Healthcare Privacy/Security Consultant, conducting compliance audits and risk assessments; drafting policies and procedures; training staff and assisting with remediation efforts
- Former HIPAA Investigator for the U.S. Department of Health and Human Services, Office for Civil Rights
- Licensed attorney in Georgia and Tennessee
- Frequent national speaker on healthcare compliance and security

Bob Chaput, CEO & Founder
MA, CISSP, HCISPP, CRISC, CIPP/US
- 35+ years in Business, Operations and Technology
- 25+ years in Healthcare
- Executive | Educator | Entrepreneur
- MA, BA - Mathematics
- Global Executive: GE, JNJ, HWAY
- Responsible for largest healthcare datasets in world
- Member: IAPP, ISC², CHIME/AEHIS, HIMSS, ISSA, ISACA, HCCA
- Numerous Technical Certifications (MCSE, MCSA, etc.)
- Expertise and Focus: Healthcare, Financial Services, Retail, Legal
Our Passion

We’re excited about what we do because...

...we’re helping organizations improve patient safety and the quality of care by safeguarding the very personal and private healthcare information of millions of fellow Americans...

... And, keeping those same organizations off the Wall of Shame...!
Awards and Recognition

2015 & 2016

Exclusive

Sole Source Provider

#11 – 2015 & 2016

Industry Resource Provider

Software Used by NSA/CAEs
But FIRST!

We are not attorneys! → Engage Competent Counsel!

The Omnibus has arrived! → Welcome Aboard, BAs!

Lots of different interpretations! → Please, Ask Lots of Questions!
Some Ground Rules

1. Slide materials
   A. Check “Download” area on GoToWebinar Control panel to copy/paste link and download materials

2. Questions in “Question Area” on GTW Control Panel

3. In case of technical issues, check “Chat Area”

4. All Attendees are in Listen Only Mode

5. Please complete Exit Survey, when you leave session

6. Recorded version and final slides within 48 hours
Pause and Quick Poll

Poll #1 - How many Clearwater Compliance webinars have you attended?

1st time!  2 - 4  5 - 9  10+
Pause and Quick Poll

Poll #2 - What type of organization do you represent?

- Hospital / Health System
- Other CE
- BA
- Hybrid
- Don’t Know
Pause and Quick Poll

Poll #3 - How would you rate your HIPAA expertise?

What’s HIPAA?
I’m getting there!
Experienced
Let me teach next time!
Pause and Quick Poll

Poll #4 – Are you registered to attend the upcoming Clearwater HIPAA and Cyber Risk Management BootCamp™?
Clearwater HIPAA and Cybersecurity BootCamp™

Designed for busy professionals, the Clearwater HIPAA and Cybersecurity BootCamp™ distills into one action-packed day, the critical information you need to know about the HIPAA Privacy and Security Final Rules and the HITECH Breach Notification Rule.

Take Your HIPAA Privacy and Security Program to a Better Place, Faster ...

Earn up to 10.8 CPE Credits!

Join us for our next virtual, web-based events...Three, 3hr sessions:
• November 3rd, 10th, 17th – 2016
• February 9th, 16th, 23rd - 2017
• May 4th, 11th, 18th - 2017
• August 4th, 11th, 18th - 2017

http://clearwatercompliance.com/bootcamps/
Learning Outcomes

- Explain the history of HIPAA and HITECH and what motivated the creation of these regulations
- Identify sources of liability other than HIPAA for CEs and BAs
- Articulate the types of organizations which have experienced breaches and complaints
- Demonstrate a working knowledge of the fundamentals of the HIPAA regulations
- Explain to colleagues and management the recent statistics related to breaches of PHI
- Describe the difference between the Privacy and Security Rules

All registrants will receive a copy of all slide materials & the recorded webinar
Discussion Flow

1. Why Do These Laws & Regulations Exist? - Bob
2. Who Is Covered? - Michelle
3. What Is Covered? - Michelle
5. Who Enforces? - Bob
6. What Happens If I Don't Comply? - Michelle
**Bottom Line Up Front**

*Before HITECH/Omnibus:*
- “Paper Tiger”
- Healthcare industry largely ignored
- Business Associates didn’t know or care or both!
- Information Security was woefully inadequate

*After HITECH/Omnibus:*
- “Game-changer”
- Healthcare industry woefully unprepared
- Largest and most consequential expansion of Federal Privacy rules
- Significant new burden on business associates
- Substantially increases the magnitude of HIPAA risk and liability

Today: Help you mitigate your newly created compliance and cyber risks and liabilities as a CE and BA
"Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart therefrom, which ought not to be noised abroad, I will keep silence thereon, counting such things to be as sacred as secrets."

- Hippocrates, 4th Century, B.C.E.
First Healthcare Risk Manager

“First, Do No Harm.”

- Hippocrates, 4th Century, B.C.E.
  - OR

- Auguste François Chomel (1788–1858)
  Parisian pathologist and clinician
  - OR
  - ???

At the End of the Day, HIPAA Privacy, Security & Breach Notification Rules Are About Preventing Harm from New Threat Sources
Where Privacy and Security Fits In

Health Insurance Portability and Accountability Act Of 1996

Title I
- Insurance Portability

Title II
- Fraud and Abuse
- Medical Liability Reform
- Administrative Simplification

Title III
- Tax Related Health Provision

Title IV
- Group Health Plan Requirements

Title V
- Revenue Off-sets

Privacy

Security

EDI

Identifiers

Transactions

Code Sets
Article from Forbes on the Last Day of 2015

We are in the midst of a large and rapidly growing health information privacy crisis!

- HHS reports that 253 healthcare breaches affected nearly 112 million individuals last year
- The top 10 data breaches accounted for over 111 million
- The top 6 breaches affected at least 1 million individuals – 4 of 6 were BCBS
- Hacking/IT Incident – 21% of all breaches
- Theft – 29% of all breaches

What About Our Patients?

Medical identity theft increased nearly 22 percent in the last year, an increase of nearly half a million victims since 2013.

- 22% increase in medical identity theft
- 65% of victims paid more than $13,000 out-of-pocket costs to resolve the crime
- 90% say they suffered embarrassment stemming from disclosure of sensitive personal health conditions
- 30% do not know when they became a victim

79% expect their healthcare providers to ensure the privacy of their health records.

48% say they would consider changing healthcare providers if their medical records were lost or stolen.

5th Annual Study on Medical Identity Theft, Ponemon Institute
Pause and Quick Poll

Poll #5 – How important is safeguarding PHI to your organization?

Not  Sort of  Pretty  Very
“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.” re: Oregon Health & Science University

“In addition to identifying risks and vulnerabilities to their ePHI, entities must also implement reasonable and appropriate safeguards to address them within an appropriate time frame. We at OCR remain particularly concerned with unaddressed risks that may lead to impermissible access to ePHI.” re: University of Mississippi Medical Center
Discussion Flow

1. Why Do These Laws & Regulations Exist?
2. Who Is Covered?
3. What Is Covered?
4. What Is Required Or Prohibited?
5. Who Enforces?
6. What Happens If I Don't Comply?
7. What Resources Can Help?
HIPAA Entities

Covered Entity
• Health care providers (that conduct e-transactions), health plans, health care clearinghouses

Business Associate
• Entity that uses or discloses PHI on behalf of a CE
• Create, receive, *maintain* or transmit PHI on behalf of a CE

Subcontractor (or Agent?) Sub Business Associate
• A person or entity to whom a BA delegates a function, activity, or service, other than in the capacity of a member of the workforce of such BA.
Know These Brands?

Business Associates Triggering Major Breaches
HIPAA Chain Of Trust

Hospital

HIPAA-HITECH Covered Entity

Business Associate 1

Business Associate 2

Business Associate 3

Outside IT

Portal Provider

Billing

Outside Law Firm

Data Analytics firm

Sub-BA 1

Sub-BA 2

Sub-BA 3

EHR Contractor

Data Analytics

Regulations Create Chain of Trust... doesn’t end...
Basic HIPAA Requirements On A CE/BA!

45 C.F.R. §164.308 Administrative Safeguards.

(b)(1) *Business associate contracts and other arrangements.* A covered entity may permit a business associate to *create, receive, maintain, or transmit* electronic protected health information on the covered entity's behalf only if ...

(2) *A business associate* may permit a business associate that is a subcontractor to *create, receive, maintain, or transmit* electronic protected health information on its behalf only if ...

(3) *Implementation specifications: Written contract or other arrangement*

Chain of Trust Does Not End!
Basic HIPAA Requirements Of A CE/BA!

HIPAA Security Rule
§164.314 Organizational Requirements
(a)(1) Standard: Business associate contracts or other arrangements. The contract or other arrangement required by §164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

(2) Implementation specifications (Required).
   (i) Business associate contracts. The contract must provide that the business associate will ...
   (ii) Other arrangements. The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of §164.504(e)(3).
   (iii) Business associate contracts with subcontractors. The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section ...
HITECH Changed The Game For BAs

TITLE XIII—HEALTH INFORMATION TECHNOLOGY Subtitle D—Privacy

SEC. 13401. APPLICATION OF SECURITY PROVISIONS AND PENALTIES TO BUSINESS ASSOCIATES OF COVERED ENTITIES; ANNUAL GUIDANCE ON SECURITY PROVISIONS

SEC. 13404. APPLICATION OF PRIVACY PROVISIONS AND PENALTIES TO BUSINESS ASSOCIATES OF COVERED ENTITIES
Discussion Flow

1. Why Do These Laws & Regulations Exist?
2. Who Is Covered?
3. What Is Covered?
4. What Is Required Or Prohibited?
5. Who Enforces?
6. What Happens If I Don't Comply?
7. What Resources Can Help?
Protected Health Information (PHI)

- Protected Health Information (PHI)
  - Past, Present, Future Mental or Physical Health, or billing related thereto
  - Can be connected to individual by one of 18 identifiers
  - All forms: Oral, written, electronic, etc.
  - Excludes employment records and education records

“The doctor is running a bit late. So Mr. Kelly, how’s that rash on your groin coming along?”
The 18 Identifiers

1. Names;
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Phone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and, 18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

145 CFR 160.514
So What?

Must be one of the **Who**...

**HIPAA-HITECH Entities**

**Covered Entity**
- Health care providers (that conduct e-transactions), health plans, health care clearinghouses

**Business Associate**
- Entity that uses or discloses PHI on behalf of a CE
- Create, receive, maintain or transmit PHI on behalf of a CE

**Subcontractor (or Agent?) Sub Business Associate**
- A person or entity to whom a BA delegates a function, activity, or service, other than in the capacity of a member of the workforce of such BA.

+ 

Must be handling the **What**...

**Protected Health Information (PHI)**

- Protected Health Information (PHI)
  - Past, Present, Future Mental or Physical Health, or billing related thereto
  - Can be connected to individual by one of 18 identifiers
  - All forms: Oral, written, electronic, etc.
  - Excludes employment records and education records

*“Oh, so it’s carved in stone, but still open to interpretation, right?”*

*“The doctor is running a bit late. So Mr. Kelly, how’s that rash on your groin coming along?”*
Discussion Flow

1. Why Do These Laws & Regulations Exist?
2. Who Is Covered?
3. What Is Covered?
4. What Is Required Or Prohibited?
5. Who Enforces?
6. What Happens If I Don't Comply?
7. What Resources Can Help?
Three Pillars Of HIPAA Compliance...

OMNIBUS FINAL RULE

HITECH

HIPAA

Privacy Rule
- 75 pages / 27K words
- 56 Standards
- 54 Implementation Specs

Security Rule
- 18 pages / 4.5K words
- 22 Standards
- 50 Implementation Specs

Breach Notification
- 6 pages / 2K words
- 4 Standards
- 9 Implementation Specs
Balanced Compliance Program

**Policy** defines an organization’s values & expected behaviors; establishes “good faith” intent

**People** must include talented privacy & security & technical staff, engaged and supportive management and trained/aware colleagues following PnPs.

**Procedures** or processes – documented - provide the actions required to deliver on organization’s values.

**Safeguards** includes the various families of administrative, physical or technical security controls (e.g. encryption, firewalls, anti-malware, intrusion detection, incident management tools, etc.)

Clearwater Compliance Compass™
Privacy (GAPP)

1. Management
2. Notice
3. Choice & Consent
4. Collection
5. Use, Retention & Disposal
6. Access
7. Disclosure to 3rd Parties
8. Security for Privacy
9. Quality
10. Monitoring & Enforcement

Security

Confidentiality
Integrity
Availability

Controls
Safeguards

Security Program without Privacy Program; Converse is Not True
At the end of the day...  
...the Privacy and Security Risk Problem We’re Trying to Solve

What if my Sensitive Information is not complete, up-to-date and accurate?

What if my Sensitive Information is shared?

What if my Sensitive Information is not there when it is needed?

ePHI, PII, PCI Data, MNPI, Trade Secrets, Business Plans, Software Code, Etc.

Don’t Compromise C-I-A!
The Breach Notification Rule

- Administrative Requirements
- Breach Notification
- Burden of Proof

All PHI, including ePHI
The Security Rule

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies & Procedures

Only ePHI
The Security Rule

22 Standards and 50+ Implementation Specifications:
Not all requirements are created equal.

Get Risk Analysis Done; then do Risk Management
Do Risk Analysis And Risk Management!

• “All too often we see covered entities with a limited risk analysis that focuses on a specific system such as the electronic medical record or that fails to provide appropriate oversight and accountability for all parts of the enterprise .... An effective risk analysis is one that is comprehensive in scope and is conducted across the organization to sufficiently address the risks and vulnerabilities to patient data.” – Samuels on University of Washington Medicine CAP

• “Two major cornerstones of the HIPAA Rules were overlooked by this entity - 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.” Samuels on North Memorial Health Care of Minnesota CAP
Phase 2 Audit Protocol

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html
Phase 2 Audits: Current Audit Protocol

• As of July 11, 2016, 167 health plans, health care providers and clearinghouses were notified of desk audits

• Chosen organizations received 2 emails
  1. Notification letter, timeline for response and unique link to submit via OCR’s online portal
  2. Additional request to provide a listing of the entity’s BAs, and information re: an upcoming OCR webinar to explain the desk audit process

• All documentation had to be current as of the date of the request

• Entities had 10 business days, until July 22, 2016, to respond to the document requests

• Critical that documentation accurately reflects the program

• Desk audits of business associates will follow this fall

One Shot! ➔ Had to Be Super Ready
## Requirements Selected for Desk Audit Review

<table>
<thead>
<tr>
<th>Rule</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Privacy Rule | Notice of Privacy Practices & Content Requirements  [§164.520(a)(1) & (b)(1)]  
Provision of Notice – Electronic Notice  [§164.520(c)(3)]  
Right to Access  [§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)] |
| Breach Notification Rule | Timeliness of Notification  [§164.404(b)]  
Content of Notification  [§164.404(c)(1)] |

Pause and Quick Poll

Poll #6 – Has your organization conducted a ‘mock audit’ to help you prepare for Phase 2 Audits?

Yes  No  I’m Not Worried
Regulatory “Field Trip”

Part 160

Omnibus Final Rule ➔ Big Changes in 160 & 164

Part 164
Pause and Quick Poll

Poll #7 – What do you think is most important in a compliance program?

- Policies and Procedures
- People
- Safeguards
- All equally important
Discussion Flow

1. Why Do These Laws & Regulations Exist?
2. Who Is Covered?
3. What Is Covered?
4. What Is Required Or Prohibited?
5. Who Enforces?
6. What Happens If I Don't Comply?
7. What Resources Can Help?

“No, the 'Meaning of HIPAA' guru is two peaks over that way.”
New “Arrows” In HHS/OCR Enforcement Quiver

• New Civil Monetary Penalty System
• OCR Audits
• Monies Back to OCR Coffers
• State AGs Jurisdiction
• Wider Net
• Breach Notification Rule
• “Wall of Shame”
• Increased Complaints

Help from...

• CMS MU Audits
• Possible FCA Actions
• Possible FTC Actions
• SEC Disclosure Requirements
• Yates Memo

Why is this woman smiling?
1. Update security guidance for covered entities and business associates to ensure that the guidance addresses *implementation of controls described in the NIST Cybersecurity Framework*;

2. Update technical assistance that is provided to covered entities and business associates to address technical security concerns;

3. Revise the current enforcement program to include following up on the implementation of corrective actions;

4. Establish performance measures for the OCR audit program; and

5. Establish and implement policies and procedures for sharing the results of investigations and audits between OCR and CMS to help ensure that covered entities and business associates are in compliance with HIPAA and the HITECH Act.
And, Please Do Not Forget OIG’s “Internal Audit” Role

”Strengthen your Enforcement, OCR!”
-- OIG
Discussion Flow

1. Why Do These Laws & Regulations Exist?
2. Who Is Covered?
3. What Is Covered?
4. What Is Required Or Prohibited?
5. Who Enforces?
6. What Happens If I Don't Comply?
7. What Resources Can Help?

“No, the 'Meaning of HIPAA' guru is two peaks over that way.”
Three Terms To Memorize

1. **Reasonable diligence** means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

2. **Reasonable cause** means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect. **NEW!**

3. **Willful neglect** means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

---

145 CFR 160.401 Definitions

Give Your CEO and Outside Counsel Something to Work With!
<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Penalty Range for Each Violation</th>
<th>All Such Violations of an Identical Provision in a Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A) Reasonable Diligence <em>(Did Not Know)</em></td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(B) Reasonable Cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(C)(i) Willful Neglect – Corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(C)(ii) Willful Neglect – Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

Discretion to Use $50K at Any Level ➔ CEs & BAs ➔ Act Swiftly in Case of Breach
New Math - CMP

Assume: July 2015 event

- Laptop with 1,000 records is stolen from a Covered Entity and ePHI is impermissibly disclosed ... and confidentiality and availability are compromised

OCR investigation found violations:

1. Impermissible disclosure of PHI \((45\text{ CFR }\S 164.502(a))\)
2. Failed to implement safeguards \((45\text{ CFR }\S 164.530(c))\)
3. Did not ever complete a risk analysis \((45\text{ CFR }\S 164.308(a)(1)(ii)(A))\)
4. Did not undertake risk management by implementing reasonable and appropriate controls \((45\text{ CFR }\S 164.308(a)(1)(ii)(B))\)
5. Did not do data backup; failed to create exact retrievable copies of ePHI on laptops \((45\text{ CFR }\S 164.308(a)(7)(ii)(A))\)

Did not address the above violations within 30 days of discovery of the violations

And, assume, organization was found to be in “willful neglect”
Civil Monetary Penalty calculation might be:

- Two Privacy Rule violations (Impermissible disclosure + Safeguards failure)
- Three Security Rule violations listed on previous slide
- 1,000 records * $50,000 per violation = $50,000,000 per violation, capped at $1,500,000 for identical violations during a calendar year \( \Rightarrow \) $1,500,000
- 5 violations * $1,500,000 = $7,500,000

But wait, there’s more!!

- Impermissible Disclosure – 1 time = $1.5
- Every other violation:
  - 2010 – 2015 \( \Rightarrow \) 6 yrs x 4 x $1.5 = $36.0

\[ \text{Total} = $7,500,000 + $36,000 = $7,536,000 \]
Congress also established criminal penalties for certain actions...

- **Up to $50,000 and one year in prison** for certain offenses such as knowingly obtaining PHI
- **Up to $100,000 and up to five years in prison** if the offenses are committed under false pretenses
- **Up to $250,000 and up to 10 years in prison** if the offenses are committed with the intent to sell, transfer, or use protected health information for commercial advantage, personal gain, or malicious harm.

1USCOTE-2011-title42-chap7-subchapXI-partC-sec1320d-6_HIPAA Criminal Penalties
Resolution Agreements

Resolution Agreements and Civil Money Penalties

A resolution agreement is a settlement agreement signed by HHS and a covered entity or business associate in which the covered entity or business associate agrees to perform certain obligations and make reports to HHS, generally for a period of three years. During the period, HHS monitors the covered entity's compliance with its obligations. A resolution agreement may include the payment of a resolution amount. If HHS cannot reach a satisfactory resolution through the covered entity's demonstrated compliance or corrective action through other informal means, including a resolution agreement, civil money penalties (CMPS) may be imposed for noncompliance against a covered entity.

- HIPAA settlement illustrates the importance of reviewing and updating, as necessary, business associate agreements – September 23, 2016

- Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million - August 4, 2016

- Multiple alleged HIPAA violations result in $3.75 million settlement with the University of


- Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University - July 18, 2016

- Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement – June 29, 2016
And, then there were 42...12 so far in 2016

**Summary of HHS-OCR HIPAA Enforcement Actions**

<table>
<thead>
<tr>
<th>Settlement / CMP Amounts</th>
<th>Summary</th>
<th>$22,855,300 in 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settlement / CMP Amounts</td>
<td>$55,130,200</td>
<td>$2,140,500</td>
</tr>
</tbody>
</table>

| Number of Individuals Affected | 6,759,718 | 31,800 | 14,004 | 3,998,439 | 10,000 | 3,044 | 412 | 2 | 17,300 | 13,000 |
| Settlement/Penalty per Individual Affected | $8.16 | $67 | $29 | $1 | $275 | $887 | $1,578 | $1,100,000 | $43.35 | $300.00 |

| Number of Settlement Agreements/CAPs | 42 | CA | RI | IL | MS | OR | PA | NY | NC | NY |
| Media/PHI Home | Publicly accessible web server | Backup Tapes | Desktop/Laptop | Laptop / Network Drive | Laptop / Network and Data Storage | Video Film | x-ray Films | Laptop |
| Announcement Date | Summary | 10/18/16 | 9/23/16 | 8/4/16 |

<table>
<thead>
<tr>
<th>Key Finding and/or Corrective Action Plan</th>
<th>RA Failures %</th>
<th>71%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop / Revise Privacy, Breach Notification &amp; Security PnPs</td>
<td>38</td>
<td>X</td>
</tr>
<tr>
<td>Implement (security awareness) training and sanctions for non-compliance</td>
<td>35</td>
<td>X</td>
</tr>
<tr>
<td>Conduct Risk Analysis Periodically</td>
<td>30</td>
<td>X</td>
</tr>
<tr>
<td>Establish Comprehensive Risk Management Plan and Process</td>
<td>27</td>
<td>X</td>
</tr>
<tr>
<td>Distribute and update policies and procedures</td>
<td>25</td>
<td>X</td>
</tr>
<tr>
<td>Document Process for responding to security / privacy incidents</td>
<td>22</td>
<td>X</td>
</tr>
<tr>
<td>Implement Reasonable Safeguards to control risks</td>
<td>25</td>
<td>X (facility access)</td>
</tr>
</tbody>
</table>

**Organizations Struggling with Basic Risk Analysis**
Accretive Health Case Study

How bad things can happen to good companies
Accretive employee’s laptop computer, containing 20 million pieces of information on 23,000 patients, was stolen from the employee’s car in July 2011.

- **MN SAG Suit**: $2.5M settlement in July 2012
- **Compromise**
- **1/19/2012**: MN SAG Suit
- **7/31/2012**: $2.5M MN SAG Settlement
- **4/13/2013**: CEO Replaced
- **4/2/2013**: CFO Replaced
- **8/26/2013**: COO Replaced
- **9/27/2013**: $14M Class Settlement
- **12/21/2013**: FTC Settle
- **3/14/2014**: De-Listed NYSE

Other significant events:
- **$14M Class Settlement**: September 27, 2013
- **170 Jobs Cut**: January 2014
- **De-Listed NYSE**: March 14, 2014

Accretive Share Price & Story
St. Joseph Health System Settles Class Action Lawsuit over Data Breach

St. Joseph Health System settled with a cash payment of $7.5 million to participating settlement class members. The court documents also indicate that St. Joseph spent an additional $4.5 million on identity theft protection, $13.5 million to institute policies to comply with federal & state, and $7.5 million in attorney’s fees.
Discussion Flow

1. Why Do These Laws & Regulations Exist?
2. Who Is Covered?
3. What Is Covered?
4. What Is Required Or Prohibited?
5. Who Enforces?
6. What Happens If I Don't Comply?
7. What Resources Can Help?
Now What?

1. Don’t Panic
2. Continue Education
3. Leverage Resources
4. Think Peer Working Group
5. Think Executive Sponsor
6. Assess Current Situation
7. Think Program, Not Project
One Key Strategic Action To Take Now: Start The Conversation!

- Marketing, Customer Service & Patient Safety Strategy
- Regulatory Compliance Project
- Patient/Member Privacy & Security Program
- Competitive Advantage
- Operational Baseline
- Necessary Evil

BCEM:
- Prepare
- Detect
- Contain & MITigate
- Analyze
- Remediate & Measure
10-Point HIPAA Compliance & Cyber Risk Mitigation Program

1. Set privacy and security risk management program in place
   (45 CFR § 164.308(a)(1))

2. Develop & implement HIPAA privacy, security, and breach notification policies & procedures
   (45 CFR §164.530 and 45 CFR §164.316)

3. Train all members of your workforce
   (45 CFR §164.530(b) and 45 CFR §164.308(a)(5))

4. Complete a HIPAA security risk analysis
   (45 CFR §164.308(a)(1)(ii)(A))

5. Complete a HIPAA security evaluation (e.g. “compliance assessment”)
   (45 CFR § 164.308(a)(8))

6. Complete technical testing of your environment
   (45 CFR §164.308(a)(8))

7. Implement a strong, proactive Business Associate management program
   (45 CFR §164.502(e) and 45 CFR §164.308(b))

8. Complete Privacy Rule and Breach Rule compliance assessments
   (45 CFR §164.530 and 45 CFR §164.400)

9. Assess your current insurance coverage (e.g. cyber liability, D&O, P&C)
   (45 CFR §164.530(c) and 45 CFR §164.306(a))

10. Document and act upon a remediation plan
    (45 CFR §164.530(c) and 45 CFR §164.306(a))

Derived from OCR Enforcement Actions | Demonstrate “Reasonable Diligence”

© Clearwater Compliance | All Rights Reserved
Industry-leading HIPAA compliance software: IRM Pro™ Suite

**IRM | Analysis™**
- **Insight**
  - Understand significant threats and vulnerabilities
- **Controls**
  - Determine if you have the right controls in place
- **Risk Rating**
  - View critical risks on intuitive dashboards and reports
- **Plan and Evaluate**
  - Plan a course of action to reduce critical risks
- **Manage Complexity**
  - Automate the management of risk information across complex enterprises

**IRM | Security™**
- **Gap Assessment**
  - Against all HIPAA Security Standards
- **Audit Simulation**
  - Against HHS Audit protocols
- **Recommendations**
  - Automated expert remediation plan
- **Assign Work**
  - Managed accountability and due dates
- **Dashboards & Reports**
  - Display period-to-period compliance progress

**IRM | Privacy™**
- **Gap Assessment**
  - Against all HIPAA Privacy standards
- **Breach Preparation**
  - Compliance w/Breach Notification under HITECH
- **Audit Simulation**
  - Against HHS Audit protocols
- **Recommendations**
  - Automated expert remediation plan
- **Dashboards & Reports**
  - Display period-to-period compliance progress

**All Exclusively Endorsed by AHA**

© Clearwater Compliance | All Rights Reserved
## Other Upcoming Clearwater Events

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 2, 2016</td>
<td>Complimentary Webinar OCR Phase 2 Audits and How Best to Prepare</td>
</tr>
<tr>
<td>November 9, 2016</td>
<td>Complimentary Webinar How to Implement a Strong, Proactive Business Associate Risk Management Plan</td>
</tr>
<tr>
<td>November 16, 2016</td>
<td>Complimentary Webinar How to Conduct a NIST-based Risk Response to Comply with HIPAA &amp; Other Regulations</td>
</tr>
<tr>
<td>December 1, 2016</td>
<td>Complimentary Webinar How to Conduct a HIPAA Security Compliance Self Audit</td>
</tr>
</tbody>
</table>

Visit [ClearwaterCompliance.com](http://ClearwaterCompliance.com) for more info!
CHIME proudly presents the AEHIX16 Fall Forum for members of AEHIS, AEHIT and AEHIA. The second annual event provides a unique opportunity to network and collaborate with industry colleagues from the rapidly growing security, technology and applications sectors of healthcare.
The premier event for healthcare CIOs!

Keynote Speakers

Amy Cuddy, PhD
Social Psychologist; Associate Profession at Harvard Business School of Public Health; Best-Selling Author, Presence

Robert Herjavec
Entrepreneur, Technology Leader, Motivator

John Jacobs
Co-Founder & Chief Creative Optimist – Life is Good
30-Minute Guide to Hiring The Best Risk Analysis Company | What to Look for in a HIPAA Risk Analysis Company & Solution

https://clearwatercompliance.com/industry-insights/white-papers/
Harnessing the Power of NIST
Your Practical Guide to Effective Information Risk Management

In Summary - You Should Care

1. It’s the Law and Regs (*many laws and Regs*)

2. Your stakeholders trust and expect you to do this... and, *may* be liable, if you don’t!

3. Your revenues, assets and reputation depends on it!
Supplemental Materials

- OCR Phase 2 Protocol
- Clearwater CE Omnibus ReadinessCheck™
- Clearwater BA Omnibus ReadinessCheck™
- HIPAA Resources
- 30-Minute Guide to Hiring The Best Risk Analysis Company
Thank You | How May We Best Assist You?

https://www.clearwatercompliance.com

bob.chaput@ClearwaterCompliance.com

michelle.caswell@ClearwaterCompliance.com

Exit Survey, Please