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.

For reprint permission and information, please direct your inquiry to bob.chaput@clearwatercompliance.com
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 ADVICE PROVIDED HEREIN IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE. 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.
“I think, one of the key things is that HIPAA compliance needs to be owned by the entire organization. So, it needs to be owned by the leadership of the organization. They need to empower their CIOs, empower their compliance officers, but at the same time, they need to make sure those messages percolate down to all the staff that touches protected health information.”

Leon Rodriquez
Former Director – Office for Civil Rights

http://www.healthcareinfosecurity.com/interviews/hipaa-enforcer-reveals-audit-timeline-i-1736
Bob Chaput

MA, CISSP, HCISPP, CRISC, CIPP/US

- CEO & Founder – Clearwater Compliance LLC
- 35+ years in Business, Operations and Technology
- 25+ years in Healthcare
- Executive | Educator | Entrepreneur
- Global Executive: GE, JNJ, HWAY
- Responsible for largest healthcare datasets in world
- Industry Expertise and Focus: Healthcare Covered Entities and Business Associates, Financial Services, Retail, Legal
- Member: ACAP, AEHIS Foundation, IAPP, ISC², HIMSS, ISSA, ISACA, HCCA, HCAA, ACHE, AHIMA, NTC, ACP, SIM Chambers, Boards

Connect: http://www.linkedin.com/in/BobChaput
About HIPAA-HITECH Compliance

1. We are not practicing law!

2. The Omnibus has arrived at the station!

3. Lots of different interpretations!
Some Ground Rules

1. Slide materials
   A. Check “Chat” or “Question” 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
Poll #1 – How many Clearwater Compliance webinars have you attended?
Poll #2 – What type of organization do you represent?
Poll #3 – How would you rate your HIPAA-HITECH expertise?
Poll #4 – Are you registered to attend an upcoming Clearwater Information Risk Management BootCamp™
Our Passion

We’re excited about what we do because…

…we’re helping organizations provide better care by safeguarding the very personal and intimate healthcare information of millions of fellow Americans…

… And, keeping those same organizations off the Wall of Shame…!
Here’s What We Do For a Living...

• Since 2010
• 400+ Customers
• Compliance Assessments | Risk Analyses | Technical Testing | Policies & Procedures | Training | Remediation | Executive Coaching | BootCamps
• 25 OCR/CMS/OIG Audits & Investigations currently
• Raving Fan customers!

SaaS Platforms for Operationalizing Your Compliance Programs
Clearwater Information Risk Management BootCamp™ Events

Other 2014-15 Plans - Live, In-Person Events (9-hours):
• October 16 - Los Angeles
• December 4 – Tampa
• January 22 – Dallas
• April 23 - Orlando
• April 30 – New Orleans
• July 16 – Denver
• October 29 – Washington, DC

Other 2014-15 Plans – Virtual, Web-Based Events (3, 3-hr sessions):
• November 5-12-19
• February 5-12-19, 2015
• May 7-14-21, 2015
• August 6-13-20, 2015

Take Your HIPAA Privacy and Security Program to a Better Place, Faster ... Earn CPE Credits!

http://ClearwaterCompliance.com/bootcamps/
Upcoming Clearwater Courses

- December 1 - 3, 2014 Nashville, TN
- February 9 – 11, 2014 Miami, FL
- April 6 - 8 – Nashville, TN
- June 1 - 3 – Nashville, TN
- August 10 - 12 – Nashville, TN
- October 5 - 7 – Miami, FL

HCISPP Description

- HCISPP is a foundational credential – confirming a foundational level of performance tasks, knowledge, and abilities relating to the security and privacy of healthcare.
- As a foundational credential, the experience requirement is two years (2), as follows:
  - Minimum two years of experience in one knowledge area of the credential that includes security, compliance & privacy.
  - Legal experience may be substituted for compliance.
  - Information management experience may be substituted for privacy.
  - At least one year of the two-year experience must be in the healthcare industry.
- The HCISPP certification takes a universal approach to how regulations work internationally, so it will be applicable globally.
Before HITECH/Omnibus:  
- “Paper Tiger” 
- Healthcare industry largely ignored 
- Business Associates didn’t know or care or both! 
- Information Security was woefully inadequate 

Think HITECH = Hey It’s Time to End your Compliance Holiday

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 risks and liabilities as a CE and BA (includes Subcontractors)
HIPAA & HITECH 101

1. Why Do These Laws & Regs 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.”
"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, Do No Harm."

- Hippocrates, 4th Century, B.C.E.
Where Privacy and Security Fits In

Health Insurance Portability and Accountability Act Of 1996

Title I
- Insurance Portability

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

Title III
- Tax Related Health Provision

Title IV
- Group Health Plan Requirements

Title V
- Revenue Off-sets

Privacy
- Transactions

Security
- Code Sets

EDI

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

• 60% of consumers ➔ privacy laws don’t adequately protect their privacy

• Over 80% of regulated entities ➔ privacy laws are too complex and difficult to understand

• 50 million health records were reported breached between 2005-2008

• 33.2 million Americans reportedly had their health privacy breached in past 5 years, HHS Wall of Shame
HIPAA & HITECH 101

1. Why Do These Laws & Regs 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-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.

"Ok, so it’s carved in stone, but still open to interpretation, right?"
Know These Brands?

- UnitedHealth Group
- ARAMARK Healthcare
- IBM
- Blue Cross Blue Shield of Rhode Island
- ACCRETIVE HEALTH results providers trust
- McKesson
- Siemens
- SAIC
- KPMG
- Quantum Health Consulting
- Care1st Health Plan
- Aon

20.5M of 38.7M (~53%)
298 BAs in 1129 Breaches (26%)
Hospital

HIPAA-HITECH Covered Entity

Business Associate 1

Billing

Business Associate 2

Outside Law Firm

EHR Contractor

Business Associate n

Data Analytics

Sub-BA 1

Sub-BA 2

Sub-BA n

Portal Provider

Data Analytics firm

Outside IT

Regulations Create Chain of Trust... doesn’t end...
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!
HIPAA SECURITY FINAL 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 Changes 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
1. Why Do These Laws & Regs 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
Is it PHI?

Yes

Is it Health Information?

No ➔ Not PHI

Yes

Is it Individually Identifiable?

No ➔ Not PHI

Yes

Is it Protected?

No ➔ Not PHI

Yes

Meet one of the Exclusions?

No ➔ Not PHI

Yes ➔ Not PHI

NO ➔ PHI
Is it PHI?

3 critical definitions to answer “Is it PHI?”¹

First: Is it Health Information?

• “Health information means any information, whether oral or recorded in any form or medium, that—

  (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

  (B) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.”

¹45 CFR 160.301 Definitions
3 critical definitions to answer “Is it PHI?”

Second, Is it Individually Identifiable Health Information (IIHI)?

• “Individually identifiable health information is information that is a subset of health information (see above), and:
  
  (i) That identifies the individual; or

  (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.”

\(^1\) 45 CFR 160.301 Definitions
3 critical definitions to answer “Is it PHI?”

Third and Finally, is the IIHI being collected is Protected Health Information (PHI)?

• “Protected health information means individually identifiable health information:

  (1) Except as provided in paragraph (2) of this definition, that is:

  i. Transmitted by electronic media;

  ii. Maintained in electronic media; or

  iii. Transmitted or maintained in any other form or medium.

• But there are exclusions...

145 CFR 160.301 Definitions
3 critical definitions to answer “Is it PHI?”

“Heads Up” - there are exclusions

• (2) Protected health information excludes individually identifiable health information in:
  i. Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
  ii. Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
  iii. Employment records held by a covered entity in its role as employer.
  iv. Regarding a person who has been deceased for more than 50 years.”

145 CFR 160.301 Definitions
3 critical definitions to answer “Is it PHI?”

- Also recall that HIPAA lists 18 specific identifiers. Among them are (for brevity) the most likely pertinent identifiers are:
  - Name
  - SSN
  - Medical Record Numbers
  - Health Plan Beneficiary Numbers
  - Account Numbers
  - ...
  - Any other unique identifying number, characteristic, or code.

TIP: Avoid the painful hair-splitting debates! Err on the side of “it” being PHI!

1 45 CFR 160.301 Definitions
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)En++es)

- **Covered(En+ty)**
  - Health'care'providers'(that'
    conduct'e3transac4ons),'health'
    plans,'health'care'clearinghouses'
  - **Business\text{\textregistered}**
    - En4ty'that'uses'or'discloses'PHI'on'
      behalf of'a'CE'
    - Create,'receive,'maintain'or'
      transmit'PHI'on'behalf'of'a'CE'

- **Subcontractor\text{\textregistered}(or\text{Agent?})\text{Sub\text{Business\textregistered}}**
  - A'person'or'en4ty'to'whom'a'BA'delegates'a'func4on,'ac4vity,'or'service,'other'than'in'the'capacity'of'a'member'
of'the'workforce'of'such'BA.'

**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

Must be handling the **What**…

“**I KEEP six honest serving-men**
(They taught me all I knew);
Their names are **What** and **Why** and **When**
And **How** and **Where** and **Who**…”

- Rudyard Kipling
1. Why Do These Laws & Regs 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-HITECH Compliance...

**Privacy**
- Privacy Final Rule
  - 75 pages / 27K words
  - 56 Standards
  - ~54 “dense” Implementation Specs

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

**Breach Notification**
- Breach Notification Rule
  - 6 pages / 2K words
  - 4 Standards
  - 9 Implementation Specs
Summary of Omnibus Content

Includes changes driven by:

1. NPRM – July 14, 2010
2. HIPAA Enforcement IFR - October 30, 2009.

Does Not Include:

NPRM Accounting of Disclosures under HITECH

Recently announced: The Office of the National Coordinator’s Health IT Policy Committee Tiger Team Forming Position on Accounting for Disclosures Rule

Privacy

1. Collection
2. Use & Disclosure
3. Data Quality
4. Data Security
5. Openness
6. Choice
7. Notice
8. Access & Correction
9. Sensitive Information

Security

Confidentiality
Integrity
Availability

Controls
Safeguards

Security Program without Privacy Program; Converse is Not True
Privacy & Security of Your PHI

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

What if my Protected Health Information is shared? With whom? How?

What if my Protected Health Information is not there when it is needed?

Bottom Line: DO NOT COMPROMISE C-I-A of Any PHI!

Your PHI / ePHI

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

© Clearwater Compliance LLC | All Rights Reserved
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.
Phase 2 Audit Focus

2014 – Covered Entities
- Security – Risk analysis and risk management
- Breach — Content and timeliness of notifications
- Privacy — Notice and Access

2015

Round 1 Business Associates
- Security – Risk analysis and risk management
- Breach — Breach reporting to CE

Round 2 Covered Entities (Projected)
- Security — Device and media controls, transmission security
- Privacy — Safeguards, training to policies and procure

2016 (Projected)
- Security: Encryption and decryption), facility access control (physical); other areas of high risk as identified by 2014 audits, breach reports and complaints

Get Risk Analysis Done … and Plan to Keep Doing
Do Risk Analysis and Risk Management!

• "We continue to see a lack of comprehensive and enterprise-wide risk analysis and risk management that leads to major breaches and other compliance problems,"

• “These enforcements send out an important message about compliance issues and the need for covered entities and business associates to take their obligations seriously.”

• “When the OCR investigates a breach, we not only look at what was done to correct and remedy a breach but what led to the incident to determine if noncompliance played a part. Comprehensive enterprise risk analysis followed by ... timely risk management practices is the cornerstone of any good compliance program."

---

Jocelyn Samuels
Director – HHS’ Office for Civil Rights

-- OCR/NIST Conference | September 23, 2014
## 2014-15 OCR Audits Heating Up

### Distribution Projections

<table>
<thead>
<tr>
<th>Entity</th>
<th>Privacy</th>
<th>Breach</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covered entities</td>
<td>100</td>
<td>100</td>
<td>150</td>
</tr>
<tr>
<td>• Health Plans</td>
<td>33</td>
<td>31</td>
<td>45</td>
</tr>
<tr>
<td>• Providers</td>
<td>67</td>
<td>65</td>
<td>100</td>
</tr>
<tr>
<td>• Clearinghouses</td>
<td>--</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Business Associates</td>
<td>0</td>
<td>0</td>
<td>50</td>
</tr>
<tr>
<td>• IT Related</td>
<td>--</td>
<td>--</td>
<td>35</td>
</tr>
<tr>
<td>• Other (e.g., TPAs, claims)</td>
<td>--</td>
<td>--</td>
<td>15</td>
</tr>
</tbody>
</table>
The Breach Notification Rule

Administrative Requirements

Breach Notification

Burden of Proof

All PHI, including ePHI
Regulatory “Field Trip”

Part 160

Part 164

Omnibus Final Rule ➔ Big Changes in 160 & 164
HIPAA v. HITECH v. PPACA

HIPAA ≠ HITECH

HITECH ≠ PPACA

HIPAA ≠ PPACA

Three Distinct Laws ➔ Three Distinct Objectives
**Policy** defines an organization’s values & expected behaviors; establishes “good faith” intent.

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

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

**Safeguards** includes the various families of administrative, physical or technical security controls (including “guards, guns, and gates”, encryption, firewalls, anti-malware, intrusion detection, incident management tools, etc.)

**Clearwater Compliance Compass™**
HIPAA & HITECH 101

1. Why Do These Laws & Regs 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?
New “Arrows” in HHS/OCR Enforcement Quiver

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

Help from...

- CMS MU Audits
- Possible FCA Actions
- Possible FTC Actions
- SEC Disclosure Requirements
9. Please submit a copy of XYZ Hospital’s most recent risk analysis, as well as a copy of all risk analyses performed for or by copy XYZ Hospital within the past 6 years pursuant to 45 C.F.R. § 164.308(a)(1)(ii)(A). If no risk analysis has been performed, please state so.
1. Why Do These Laws & Regs 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?
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.
## Enforcement: Amount of CMP - 45 CFR § 160.404

<table>
<thead>
<tr>
<th>Violation Category - Section 1176(a)(1)</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
Assume:

- 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:
- Impermissible disclosure of PHI (45 CFR § 164.502(a))
- Failed to implement safeguards (45 CFR § 164.530(c))
- Did not appoint a security official (45 CFR § 164.308(a)(2))
- Did not ever complete a risk analysis (45 CFR § 164.308(a)(1)(ii)(A))
- Did not undertake risk management by implementing reasonable and appropriate controls (45 CFR § 164.308(a)(1)(ii)(B))
- Did not conduct security awareness and training (45 CFR § 164.308(a)(5))
- Failed to implement security incident response and reporting policies and procedures (45 CFR § 164.308(a)(6))
- Did not do data backup; failed to create exact retrievable copies of ePHI on laptops (45 CFR § 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”
New Math

Civil Monetary Penalty calculation might be:

• Two violation Privacy Rule (Impermissible disclosure + Safeguards failure)

• Six 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 ➔ $1,500,000 per

• 8 violations * $1,500,000 = $12,000,000

But wait, there’s more!!

• Impermissible Disclosure – 1 time ➔ $1.5
• Every other violation:
  • 2006 - 2008 ➔ 3 yrs x 7 x $25K = $0.5
  • 2009 – 2014 ➔ 6 x 7 x $1.5 = $63.0

$65.0M
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.

---

1. USCODE-2011-title42-chap7-subchapXI-partC-sec1320d-6_HIPAA Criminal Penalties
| Requirement                                                                 | $800K Parkview | $3.8M NYP/CU | $150K APDERM | $1.2M AHP | $1.7M WLP | $400K ISU | $50K HONI | $1.5M MEEI | $2.3M CVS | $1.0M Rite-Aid | $1.5M BCBS TN | $1.0M MGH | $100K PHX | $865K UCLA | $1.7M AK DHSS |
|---------------------------------------------------------------------------|----------------|--------------|--------------|-----------|----------|----------|----------|-----------|----------|----------------|----------------|-----------|----------|------------|------------|---------|
| Establish a Comprehensive Information Security Program                    |                |              |              |           |          |          |          |           |          |                |                 |           |          |            |            | $17.3+M |
| Designate an accountable Security Owner                                   |                |              |              |           |          |          |          |           |          |                |                 |           |          |            |            |         |
| Develop Privacy and Security policies and procedures                      | X              |              |              |           |          |          |          |           |          |                |                 |           |          |            |            |         |
| Document authorized access to ePHI                                        |                | X            |              |           |          |          |          |           |          |                |                 |           |          |            |            |         |
| Distribute and update policies and procedures                             |                | X            |              |           |          |          |          |           |          |                |                 |           |          |            |            |         |
| Document Process for responding to security incidents                      | X              | X            |              |           |          |          | X        |           |          |                |                 |           |          |            |            |         |
| Implement training and sanctions for non-compliance                       |                | X            |              |           |          |          | X        |           |          |                |                 |           |          |            |            |         |
| Conduct Risk Analysis / Establish Risk Management Process                  | X              | X            | X           |           | X        | X        | X        | X         | X        |                |                 |           |          |            |            |         |
| Implement Reasonable Safeguards to control risks                          | X              | X            | X           |           | X        | X        | X        | X         | X        |                |                 |           |          |            |            |         |
| Regularly review records of information system activity                    |                |              | X           |           | X        | X        | X        | X         | X        |                |                 |           |          |            |            |         |
| Implement reasonable steps to select service providers                    |                |              | X           |           | X        | X        | X        | X         | X        |                |                 |           |          |            |            |         |
| Testing and monitor security controls following changes                    | X              | X            | X           |           | X        | X        | X        | X         | X        |                |                 |           |          |            |            |         |
| Obtain assessments from qualified independent 3rd party                   |                | X            | X           |           | X        | X        | X        | X         | X        |                |                 |           |          |            |            |         |
| Retain required documentation                                             | X              | X            | X           |           | X        | X        | X        | X         | X        |                |                 |           |          |            |            |         |
Learn from OCR Enforcement

- April 16, 2014 Concentra Health Services Resolution Agreement & Corrective Action Plan
- April 11, 2014 QCA Health Plan, Inc. Resolution Agreement & Corrective Action Plan
- March 5, 2014 SKAGIT County Resolution Agreement & Corrective Action Plan
- December 20, 2013 Adult & Pediatric Dermatology, P.C. of Massachusetts Resolution Agreement & Corrective Action Plan
- August 14, 2013 Affinity Health Plan Resolution Agreement & Corrective Action Plan
- July 8, 2013 WellPoint Resolution Agreement
- April 5, 2013 Idaho State University Resolution Agreement & Corrective Action Plan
- December 17, 2012 Hospice of North Idaho Resolution Agreement & Corrective Action Plan
- September 17, 2102 Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc. Resolution Agreement & Corrective Action Plan
- July 25, 2102 Accretive Health – State of MN Settlement Agreement embedded in SEC 8-K Filing
- June 2012 Alaska Department of Health & Human Services Resolution Agreement / Corrective Action Plan
- March 2012 Blue Cross Blue Shield TN Resolution Agreement / Corrective Action Plan
- April 2012 Phoenix Cardiac Surgery P.C. Resolution Agreement Corrective Action Plan
- July 2011 University of California Los Angeles Health System Resolution Agreement
- February 2011 Massachusetts General Hospital Resolution Agreement / Corrective Action Plan
- June 2010 RITE-AID HHS Resolution Agreement & Corrective Action Plan
- July 2010 RITE-AID FTC Agreement Containing Consent Order
- January 2009 CVS Resolution Agreement & Corrective Action Plan
- June 2009 CVS FTC Agreement Containing Consent Order
Sources of Risk and Liability
We regret to inform you that, on March 12, Impairment Resources, LLC filed a petition for relief under Chapter 7 of the US Bankruptcy Code in the US Bankruptcy Court for the District of Delaware under case number 12-10850.

Burglary Triggers Medical Records Firm’s Collapse

March 12, 2012, 12:39 PM ET

The New Year’s Eve burglary of a California office building has led to the collapse of a national medical records firm.

Impairment Resources LLC filed for bankruptcy Friday after the break-in at its San Diego headquarters led to the electronic escape of detailed medical information for roughly 14,000 people, according to papers filed in U.S. Bankruptcy Court in Wilmington, Del. That information included patient addresses, social security numbers and medical diagnoses.

Police never caught the criminals, and company executives were required by law to report the breach to state attorneys general and the Department of Labor’s Office of Inspector General. Some of those agencies, including the Department of Labor, are still investigating the matter, the company said in court papers.

“The cost of dealing with the breach was prohibitive” for the company, Impairment Resources said when explaining its decision to file for Chapter 7 bankruptcy protection. That type of bankruptcy is used most often by companies to shut down and sell off what’s left to pay off their debts.
Accretive Health Case Study

Strengthening healthcare providers' financial stability
See how our approach to doing business is rooted in our clients' values.
LEARN MORE >

Higher quality care, greater healthcare access, and improved operational efficiency are possible
Learn how Accretive Health's revenue cycle management, AccretivePAS®, clinical offerings, and population health solutions can help your hospital achieve them.
LEARN MORE >

Being present to the future of healthcare
Visit Accretive Health's blog for the latest news and insights from our thought leaders.
LEARN MORE >
July 2011 - Accretive employee’s laptop computer, containing 20 million pieces of information on 23,000 patients, was stolen from the passenger compartment of the employee’s car.
Another $4 BILLION Lawsuit

Chicago Tribune NEWS

Advocate Medical Group didn't adequately secure data, class-action suit says

September 05, 2013 | By Mitch Smith | Tribune reporter

Advocate Medical Group, already under federal and state investigation after the theft of computers containing personal information on millions of people, is now facing a class-action lawsuit from patients who say the Downers Grove-based physician group didn’t do enough to protect their private data.

The suit, filed in Cook County Circuit Court, says the health care nonprofit violated privacy regulations by failing to use encryption and other security measures on the four computers that were stolen from its Park Ridge offices in July. The computers contained information on more than 4 million patients.
Class Action Lawsuits $1,000 / record

- Horizon Blue Cross Blue Shield of New Jersey – 840K records
- Advocate Medical Group – Chicago – 4MM Records
- State of Texas – 3.5 MM state employees
- Stanford Hospital & Clinic - 20,000 patients
- Sutter Health Hit With $1B Class-Action Lawsuit
- Patient files $20M lawsuit against Stanford Hospital
- TRICARE Health Management Sued for $4.9B
- AvMed Health sued over 'one of the largest medical breaches in history'
- Emory Healthcare Faces Class-Action Suit Over Data Breach
HIPAA & HITECH 101

1. Why Do These Laws & Regs 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
1 Strategic Action to Take Now: Start the Conversation!

Necessary Evil

Regulatory Compliance Project

Patient/Member Privacy & Security Program

Operational Baseline

Prepare

Remediate & Measure

Detect

Contain & Mitigate

Detect

BCEM

Marketing, Customer Service & Patient Safety Strategy

Competitive Advantage
10 Tactical Actions to Take Now

1. Set Privacy and Security Risk Management & Governance Program in place (45 CFR § 164.308(a)(1))

2. Develop & Implement comprehensive HIPAA Privacy and Security and Breach Notification Policies & Procedures (45 CFR § 164.308(a)(8))

3. Train all Members of Your Workforce (45 CFR § 164.530(b) and 45 CFR § 164.308(a)(5))


5. Complete a HIPAA Security Evaluation (= 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)

10. Document and act upon a remediation plan

Demonstrate Good Faith Effort
"As with any new program or regulation, there may be misinformation making the rounds. The following table distinguishes fact from fiction..."
Two Helpful Resources

Risk Analysis Buyer’s Guide

Risk Analysis Resources:
http://clearwatercompliance.com/hipaa-hitech-resources/
Risky Business: How to Conduct a Bona Fide HIPAA Security Risk Analysis

Get more info...

Register For Upcoming Live HIPAA-HITECH Webinars at:
http://clearwatercompliance.com/live-educational-webinars/

View pre-recorded Webinars like this one at:
http://clearwatercompliance.com/on-demand-webinars/
Two Specific “Tests”

**Clearwater CE Omnibus ReadinessCheck™:**
http://clearwatercompliance.com/covered-entity-omnibus-readinesscheck/

**Clearwater BA Omnibus ReadinessCheck™:**
http://clearwatercompliance.com/business-associate-omnibus-readinesscheck/
In Summary - You Should Care

1. It’s the Law and Regs (many laws and Regs) … HIPAA & HITECH!

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!
Contact

Bob Chaput, CISSP, HCISPP, CRISC, CIPP/US

http://www.ClearwaterCompliance.com
bob.chaput@ClearwaterCompliance.com

Phone: 800-704-3394 or 615-656-4299

Clearwater Compliance LLC

Exit Survey, Please
LEADERS WE SUPPORT
An Expert Staff with Deep Experience Serving Various Compliance Roles

• Compliance Officers
• Privacy Officials
• Security Officials
• General Counsel
• Chief Privacy Officers
• Chief Information Officers
• Chief Information Security Officers
• Chief Operating Officers
• Chief Financial Officers
• Chief Executive Officers

CLARIFY YOUR COMPLIANCE
Three Industry Leading Web-Based Software Solutions to Address All Three HIPAA Rules

Clearwater HIPAA Security Assessment™
Clearwater HIPAA Risk Analysis™
Clearwater HIPAA Privacy and Breach Notification Assessment™

You Choose Your Solution
○ Software
○ Software & Remote Assistance
○ Delivered Professional Work

ORGANIZATIONS WE ASSIST
An Expansive Client Base of 100s of Covered Entities And Business Associates

• Providers
  (Hospitals, Medical Practices, Clinics, Pharmacies, Hospice, Therapists)

• Payers
  (Managed Care, Safety Net Plans, PPOs, ACAs, Group Health Plans)

• Clearinghouses

• Business Associates
  (TPAs, Technology Services, Billing/Collections, Cloud Providers, Labs, Transcription Services, Call Centers, Disease Management)

• Hybrid Organizations
  (County Social Services, Retail, Medical Device)

[Operationalize Your HIPAA-HITECH Compliance]
clearwatercompliance.com

Call 800-704-3394 Today