"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."

- Hippocratic Oath, 4th Century, B.C.E.

Welcome to today’s Live Event... we will begin shortly... Please feel free to use “Chat” or “Q&A” to tell us any ‘burning’ questions you may have in advance
...Welcome to ...

How to Avoid The Health & Human Services (HHS) “Wall of Shame”

WEBINAR

Bob Chaput
615-656-4299 or 800-704-3394
bob.chaput@ClearwaterCompliance.com
Clearwater Compliance LLC
Who’s this guy talking?
Bob Chaput, MA, CHP, CHSS, MCSE

- President – Clearwater Compliance LLC
- 30+ years in Business, Operations and Technology
- 20+ years in Healthcare
- Executive | Educator | Entrepreneur
- Global Executive: GE, JNJ, HWAY
- Responsible for largest healthcare datasets in world
- Numerous Technical Certifications (MCSE, MCSA, etc)
- Expertise and Focus: Healthcare, Financial Services, Legal

- Member: HIMSS, HCCA, ACHE, AHIMA, NTC, Chambers, Boards
Our Passion

We’re excited about what we do because…

…we’re helping organizations safeguard the very personal and private healthcare information of millions of fellow Americans…

… And, keeping those same organizations off the Wall of Shame…!
HIPAA HITECH
Blue Ribbon Panel

• Industry Security, Privacy and Regulatory Experts

• Inaugural Event: TODAY, 5pm ET / 4pm CT / 2pm CT

https://www1.gotomeeting.com/register/818154616
1. We are not attorneys!

2. HIPAA and HITECH is dynamic!

3. Lots of different interpretations!

So there!
What’s the Story?

• Health and Human Services (HHS) is starting to *lower the boom*...

• Many Covered Entities and Business Associates are unaware and unprepared for Data Breach Notification!

• There’s “low-hanging fruit” to get started now

• Help you take practical steps avoid the HHS “Wall of Shame” for Data Breachers
Meet the ‘Wall of Shame’

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breach tool.html

Wyoming
District of Columbia
Vermont
North Dakota
Alaska
South Dakota
Delaware
Montana
Rhode Island
Hawaii
Maine
New Hampshire

10.78 MIL

07/14/2011
• 292 CEs
• 58 Named BAs
• 11.4M Individuals
Session Objectives

1. Understand the Requirements

2. Review Recent Cases, Data and Facts

3. Get Started With Practical, Actionable Next Steps
OCR Data Requests...

• **Actual OCR Letter**

• **Word document with Data Request**
Why Should You Care?

1. It’s the law… Breach Notification!

2. Your stakeholders trust you to do this

3. Your reputation depends on it
Session Objectives

1. Understand the Requirements

2. Review Recent Cases, Data and Facts

3. Get Started With Practical, Actionable Next Steps
Three Pillars of HIPAA-HITECH Compliance...

- Privacy
- Security
- Data Breach Notification
Health Information Technology for Economic and Clinical Health Act

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

THREE absolute “game changers”:

1) More Enforcement
2) Bigger fines
3) Wider Net Cast
New Civil Monetary Penalty System

• **Tier 1 (Accidental)**
  – $100 each violation
  – Up to $25,000 for identical violations, per year

• **Tier 2 (Not Willful Neglect, but Not Accidental)**
  – $1000 each violation
  – Up to $100,000 for identical violations, per year

• **Tier 3 (Willful Neglect, but Corrected)**
  – $10,000 each violation
  – Up to $250,000 for identical violations, per year

• **Tier 4 (Willful Neglect, Not Corrected)**
  – $50,000 each violation
  – Up to $1.5 million, per year
PS – Don’t Forget Criminal Penalties

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.
PHI definition

- Protected Health Information (PHI) is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

- PHI is interpreted rather broadly and includes any part of a patient’s medical record or payment history.

- ...and, that is linked to personal (18) identifiers.
Breach definition
(45 C.F.R. § 164.402)

• Acquisition, access, use, or disclosure” of PHI in a manner not permitted by the HIPAA Privacy Rule “which compromises the security or privacy of the protected health information”.

• Compromise means: “poses a significant risk of financial, reputational, or other harm to the individual.”
## Your Breach Investigation & Notification Obligations

<table>
<thead>
<tr>
<th>Obligations</th>
<th>Description</th>
<th>Readiness</th>
</tr>
</thead>
<tbody>
<tr>
<td>45 C.F.R. § 164.402</td>
<td>Breach Definition</td>
<td></td>
</tr>
<tr>
<td>45 C.F.R. § 164.404</td>
<td>Individual Notification</td>
<td></td>
</tr>
<tr>
<td>45 C.F.R. § 164.406</td>
<td>Media Notification</td>
<td></td>
</tr>
<tr>
<td>45 C.F.R. § 164.408</td>
<td>Secretary Notification</td>
<td></td>
</tr>
<tr>
<td>45 C.F.R. § 164.410</td>
<td>Notification by a Business Associate</td>
<td></td>
</tr>
<tr>
<td>45 C.F.R. § 164.414</td>
<td>Administrative Burden of Proof</td>
<td></td>
</tr>
<tr>
<td>45 C.F.R. § 164.530</td>
<td>Administrative Requirements</td>
<td></td>
</tr>
<tr>
<td>45 C.F.R. § 160.310(b)</td>
<td>Complaint Investigation &amp; Review (Office for Civil Rights-OCR)</td>
<td></td>
</tr>
</tbody>
</table>

**Title 45: Public Welfare | PART 164—SECURITY AND PRIVACY | Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information**
Presumed Guilty: Administrative Burden Of Proof

1. The CE has the burden of demonstrating (documenting) that all notifications were made as required by new Subpart D;

2. Or demonstrating that the use or disclosure did not constitute a breach, by completing a risk assessment and documenting that the impermissible acquisition, access, use, or disclosure could not pose a “significant risk of financial, reputational, or other harm to the individual”;

3. Or by establishing that the PHI was a limited data set or one of the exclusions were met
# Knowing & Identifying Exclusions

<table>
<thead>
<tr>
<th>Data Breach Exclusions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PHI Encryption per 45 C.F.R. § 164.304</td>
<td>✓</td>
</tr>
<tr>
<td>Disclosure of a “Limited Data Set” (LDS)</td>
<td>✓</td>
</tr>
<tr>
<td>Unintentional acquisition, access, or use by a CE or BA workforce member who was acting in ‘good faith’ and does not further use or disclose the PHI</td>
<td>✓</td>
</tr>
<tr>
<td>Any inadvertent disclosure by an authorized person to another authorized person working within the same CE or BA or within an ‘organized health care arrangement’ which the CE is part of, as long as the PHI inadvertently disclosed is not further used or disclosed</td>
<td>✓</td>
</tr>
<tr>
<td>Disclosure of PHI where the CE or BA has “a good faith belief” that the unauthorized recipient “would not reasonably have been able to retain such information.”</td>
<td>✓</td>
</tr>
</tbody>
</table>
Data Breach Notification Requirements

Individual Notice

Media Notice

Notice to the Secretary
**Individual Notice**

- Notice in written form
- Possibly web site postings or major print or broadcast media
- Possibly phone calls and other means
- Notifications must be provided in no case later than 60 days
- Must include:
  - Description of the breach
  - Description of the types of information
  - Steps affected individuals should
  - Description of what the covered entity is doing
  - Contact information for the covered entity
  - Toll-free number for individuals to contact the covered entity
Data Breach Notification Requirements - 2

**Media Notice**

- For a breach affecting more than 500 residents of a State or jurisdiction, CE or BA must provide notice to prominent media outlets serving the State or jurisdiction

- Media notification must be provided in no case later than 60 days
Notice to the Secretary

• CEs and BAs must notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form.

• If a breach affects 500 or more individuals, CEs and BAs must notify the Secretary in no case later than 60 days following a breach.

• If a breach affects fewer than 500 individuals, the CEs and BAs may notify the Secretary on an annual basis. Reports are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.
Data Breach Notification

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinSTRUCTION.html
Session Objectives

1. Understand the Requirements

2. Review Recent Cases, Data and Facts

3. Get Started With Practical, Actionable Next Steps
Some Recent Legal Actions

- **UCLA Health System Enters into $865K Resolution Agreement & CAP with OCR**
- **Cignet Health Fined for Violation of HIPAA Privacy Rule: $4.3M**
- **MGH entering into a resolution agreement; includes a $1 million settlement**
- **Court Approves VT Attorney General HIPAA Settlement With Health Insurer**
- **AvMed Health sued over 'one of the largest medical breaches in history'**
- **University of Hawaii sued over data breach**
- **Health Net keeps paying for its data breach in 2009... $625K and counting**
- **WellPoint's notification delay following data breach brings action by Attorney General's office**

**Enforcement is on the upswing...**
Theft (49%) and Loss (14%) account for almost 2/3 of all breaches.
What the Initial Postings Tell Us

Computer hard drives (54%) and Network Access (12%) account for almost 2/3 of all breaches.
What the Initial Postings Tell Us

Physical theft (71%) and Loss (16%) account for almost 7 out of 8 Electronic Device breaches.

How Electronic Devices Were Breached

- 71% Physical theft
- 16% Loss
- 4% Combination
- 7% Unauthorized access / disclosure
- 4% Physical loss
- 4% Hacking / IT
- 4% Unknown
Lessons Learned and Solutions

Solutions Available Today:

• Laptop/Desktop Encryption Services
• Laptop/Desktop Lost Data Destruction Services
• Laptop/Desktop Theft Prevention Locks
• Asset Management / Visibility Tools
• Secure Online Backup and Recovery Services
• Policies & Procedures
• Training & Awareness
10-Point Data Protection Checklist

1. Backup Data; be 100% confident you can recover it!
2. Secure Network
3. Block Spam
4. Stop Malware
5. Condition Power
6. Patch Software
7. Encrypt Data
8. Practice Recovery
9. Enforce Policies
10. Insure Technology
“On Demand” HIPAA HITECH RESOURCES, IF NEEDED:

Clearwater Compliance Resources

1. Tools and ToolKits
2. Professional Services & Consulting
3. Risk Management Solutions

Helping you to become and remain HIPAA HITECH compliant
Summary

Don’t let HHS lower the boom on you!
Stay off the ‘Wall of Shame’!

Get started Today... protect your ePHI!
Contact

Bob Chaput

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

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

Clearwater Compliance LLC

© 2010-11 Clearwater Compliance LLC | All Rights Reserved
Why Now? – What We’re Hearing

“Our business partners (health plans) are demanding we become compliant…” – large national care management company (BA)

“We did work on Privacy, but have no idea where to begin with Security” – 6-Physician Pediatric Practice (CE)

“We want to proactively market our services by leveraging our HIPAA compliance status ...” -- large regional fulfillment house (BA)

“With all the recent changes and meaningful use requirements, we need to make sure we meet all The HITECH Act requirements ...” – large family medicine group practice (CE)

“We need to have a way to quickly take stock of where we are and then put in place a dashboard to measure and assure our compliance progress...” – national research consortium (BA)

“We need to complete HIPAA-HITECH due diligence on a potential acquisition and need a gap analysis done quickly and efficiently...” – seniors care management company (BA)
What Our Customers Say...

“The WorkShop™ process made a very complicated process and subject matter simple. The ToolKit™ itself was excellent and precipitated exactly the right discussion we needed to have.” – outside Legal Counsel, national research consortium

“The HIPAA Security Assessment ToolKit™ and WorkShop™ are a comprehensive approach that effectively guided our organization’s performance against HIPAA-HITECH Security requirements.” -- SVP and Chief Compliance, national hospice organization

“... The WorkShop™ process expedited assessment of gaps in our HIPAA Security Compliance program, began to address risk mitigation tasks within a matter of days and... the ‘ToolKit’ was a sound investment for the company, and I can't think of a better framework upon which to launch compliance efforts.” – VP & CIO, national care management organization

“...the process of going through the self-assessment WorkShop™ was a great shared learning experience and teambuilding exercise. In retrospect, I can't think of a better or more efficient way to get started than to use the HIPAA Security Assessment ToolKit.” – CIO, national kidney dialysis center firm

“...this HIPAA Security Assessment Toolkit is worth its weight in gold. If we had to spend our time and resources creating this spreadsheet, we would never complete our compliance program on time...” — Director, Quality Assurance & Regulatory Affairs