Data is Worth More Than Gold
Why Compliance is an Executive Level Problem
Mike Semel

- 35-year IT business owner/manager
- 12 year certified HIPAA Professional
- EMT/ER Tech/FD Rescue Captain/IndyCar Safety Team
- Hospital/Skilled Nursing CIO
- School District CIO
- Cloud Backup Service COO

Mike Semel
President
Chief Compliance Officer
SEMEL Consulting
Speaking, Writing
Amazon Best-Seller

How to Avoid HIPAA Headaches

MIKE SEMEL
A HIPAA HORROR STORY
Patient Data Published to Internet

• Cottage Health’s IT company accidently published it to the Internet

• Patients Googled Themselves & Got their Medical Records

• InSync did not have insurance so Cottage Health filed a claim with its cyber-liability carrier, Columbia Casualty

• Patients sued, lawsuit settled for $ 4.1 million

• Columbia Casualty paid settlement and lawyer’s fees, but said it was still investigating...

• Columbia sued Cottage Health to recover its $ 4.1 million
Will Your Cyber Liability Insurance Pay Off?

Insurer Seeks Breach Settlement Repayment

Alleges Client Failed to Follow 'Minimum Practices'

Columbia Casualty alleges that Cottage Health's application for coverage under the Columbia policy "contained misrepresentations and/or omissions of material fact that were made negligently or with intent to deceive concerning Cottage's data breach risk controls," according to the insurer's lawsuit.
Plus State & Federal Penalties

• Failed to conduct an accurate and thorough assessment of the potential risks
• Failed to implement security measures sufficient to reduce risks
• Failed to perform periodic technical and non-technical evaluations
• Failed to obtain a written business associate agreement with a contractor that maintained ePHI on its behalf.
What is Compliance?

Having to meet requirements set by others

Federal & State Laws
Industry Regulations
Contractual Obligations
Insurance Policy Requirements
Never Compartmentalize Your HIPAA Compliance
HIPAA’s Rules Overlap

**PRIVACY RULE**
Protects all PHI spoken, written, electronic

**SECURITY RULE**
Framework to protect electronic PHI

**BREACH NOTIFICATION RULE**
Breach notification & reporting

Security Risk Analysis
Risk Management Plan
The Phase 2 HIPAA Audit Program reviews the policies and procedures adopted and employed by covered entities and business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These analyses are conducted using a comprehensive audit protocol that has been updated to reflect the Omnibus Final Rule.
All Other Requirements Must be Considered

PRIVATE RULE
PROTECTS ALL PHI SPOKEN, WRITTEN, ELECTRONIC

SECURITY RULE
FRAMEWORK TO PROTECT ELECTRONIC PHI

STATE DATA BREACH LAWS

BREACH NOTIFICATION RULE
BREACH NOTIFICATION & REPORTING

DATA BREACH INSURANCE POLICY

CONTRACTS LICENSES

©2019 Semel Consulting LLC MAY NOT BE SHARED OUTSIDE YOUR ORGANIZATION WITHOUT PERMISSION www.semelconsulting.com
Breach Example - Stolen Laptop
DEPARTMENT OF HEALTH & HUMAN SERVICES
Voice - (212) 264-3313, (800) 368-1019
TDD - (212) 264-2355
(FAX) - (212) 264-3039
http://www.hhs.gov/ocr/

OFFICE OF THE SECRETARY
Office for Civil Rights, Region II
Jacob Javits Federal Building
26 Federal Plaza, Suite 3312
New York, NY 10278

OCR initiated an investigation of the subject incident to determine if there has been a failure to comply with the requirements of the cited regulations and, if necessary, depending on the evidence, other requirements of the Privacy, Security, and Breach Notification Rules.

OCR needs additional information to complete its investigation. Thus, enclosed is a list of needed data and information (Attachment A). Please submit responses thereto within 14 days of the date on this letter. OCR welcomes any additional material you would like OCR to consider in determining its compliance status.

Provide all new or revised policies and procedures issued by you to comply with the Privacy and Security Rules and the Breach Notification Rule since its previous response to OCR, received
The breach notification report indicates that, on January 4, 2016, became aware that on January 1, 2016, a laptop was stolen from their corporate offices. The laptop contained the electronic protected health information (ePHI) of 6,893. The breached ePHI included the names, addresses, dates of births, Medicare and/or Medicaid numbers.


One Laptop Theft = Multiple Violations

**PRIVACY RULE**

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>164.502(a)</td>
<td>Uses and disclosures of protected health information</td>
</tr>
<tr>
<td>164.530 (c)</td>
<td>Administrative Requirements - must reasonably safeguard PHI</td>
</tr>
<tr>
<td>164.530 (f)</td>
<td>Administrative Requirements - must mitigate harmful effect</td>
</tr>
</tbody>
</table>

**SECURITY RULE**

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>164.308(a)(1)(ii)(A)</td>
<td>Risk Analysis</td>
</tr>
<tr>
<td>164.308(a)(1)(ii)(B)</td>
<td>Risk Management</td>
</tr>
<tr>
<td>164.308(a)(1)(ii)(C)</td>
<td>Sanction Policy</td>
</tr>
<tr>
<td>164.308(a)(7)</td>
<td>Contingency Plan</td>
</tr>
<tr>
<td>164.310(a)(1)</td>
<td>Physical Safeguards</td>
</tr>
<tr>
<td>164.310(a)(2)(ii)</td>
<td>Facility Security Plan</td>
</tr>
<tr>
<td>164.310(a)(2)(iii)</td>
<td>(Physical) Access control and validation procedures</td>
</tr>
<tr>
<td>164.310(b)</td>
<td>Workstation Use</td>
</tr>
<tr>
<td>164.310(c)</td>
<td>Workstation Security</td>
</tr>
<tr>
<td>164.310(d)(1)</td>
<td>Device and Media Controls</td>
</tr>
<tr>
<td>164.310(d)(2)(iii)</td>
<td>Accountability - record movements of hardware &amp; media</td>
</tr>
<tr>
<td>164.312 (a)(2)(iv)</td>
<td>Data backup and storage</td>
</tr>
</tbody>
</table>

**BREACH NOTIFICATION RULE**

<table>
<thead>
<tr>
<th>Subsection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>164.404(a)(1)</td>
<td>Notify each individual following discover of a breach</td>
</tr>
<tr>
<td>164.406</td>
<td>Notify the media following a breach of more than 500 records</td>
</tr>
<tr>
<td>164.414</td>
<td>Follow and prove compliance with breach notification rule</td>
</tr>
</tbody>
</table>
Federal HIPAA Penalties

2014 + 2015
$ 14 million

2016 + 2017
$ 42 million

2018
$ 28.7 million
Why are Cybersecurity & Compliance Executive Responsibilities?
Why are Cybersecurity & Compliance Executive Responsibilities?
Increased Litigation

Equifax had patch 2 months before hack and didn’t install it, security group says

"The Equifax data compromise was due to (Equifax's) failure to install the security updates provided in a timely manner," The Apache Foundation, which oversees the widely-used open source software, said in a statement Thursday.
Patient Lawsuits

Then -

• Medical Malpractice
  • Medical Treatment
  • Complaint from 1 patient
  • Insurance coverage
  • Liability Limitations

• Medical Malpractice
• Medical Treatment
• Complaint from ALL patients at same time
• Insurance coverage ???
• Liability Limitations ???
• Breach of Contract
• Negligent Misrepresentation
  • Court considered Notice of Privacy Practices a contract with patients
  • Complaint from ALL patients at same time
  • Insurance ???

Now -

• Medical Malpractice
  • Data Breach
  • Complaint from ALL patients at same time
  • Insurance coverage ???
  • Liability Limitations ???
HIPAA Crime

Suffolk woman sentenced to more than 5 years in identity theft of patients

Healthcare IT News
Six fired for keeping up with Kardashian

EX-UCLA HEALTHCARE EMPLOYEE SENTENCED TO FEDERAL PRISON FOR ILLEGALLY PEEKING AT PATIENT RECORDS

Renal & Urology News
Staff Nurse Faces Jail Time for HIPAA Violations
Medical Record Black Market

• Credit Card Number

• Medical Record

25¢ - $1

$10 - $50
2018 Cost of a Data Breach Report

$ 233  Per Record
Across All Industries

Source: 2018 Ponemon Cost of a Data Breach Report

$ 408  Per Medical Record

10,000 records  --  $ 2- $ 4 million

25,000 records  --  $ 5 - $ 10 million

100,000 records  --  $ 20 – $ 40 million
Data is Worth More Than Gold
Lost Thumb Drives

Thumb Drive Weight – ¾ of one ounce

Gold = $ 1200 per ounce

If Thumb Drive was solid gold it would be worth $ 995

A medical practice paid a $ 150,000 fine when it lost a thumb drive containing patient records

A health plan paid $ 2.2 million when it lost a thumb drive

Data Worth $ 150,000 To $ 2.2 million
How We Approach Security

Security is a BUSINESS problem
With a TECHNICAL solution
HIPAA Timeline

<table>
<thead>
<tr>
<th>HIPAA Act</th>
<th>Privacy Rule</th>
<th>Security Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>1996</td>
<td>2003</td>
<td>2005</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HITECH Act</th>
<th>Data Breach Rule</th>
<th>HIPAA Enforcement</th>
<th>Meaningful Use</th>
<th>Omnibus Final Rule</th>
</tr>
</thead>
</table>

• **Health Insurance Portability & Accountability Act** *(1996)*
  - **HIPAA Privacy Rule** *(2003)* Protects ALL identifiable patient information – written, verbal, electronic (PHI)
  - **Security Rule** *(2005)* protects electronic Protected Health Information (ePHI) – over 50 requirements

• **HITECH Act** *(2009)* funded electronic medical records and changed HIPAA
  - **Breach Reporting Rule** *(2009)* sets reporting requirements & exemptions
  - **HIPAA Omnibus Final Rule** released January, 2013
What is PHI & ePHI?

• Protected Health Information
  • Identifiable
    (18 different identifiers)
    • Plus treatment and/or diagnostic information

• Electronic Protected Health Information
  • PHI in electronic form
  • Words, images, voice files
  • On any media – devices, portable, cloud
1. **Names**

2. **All geographic subdivisions** smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
   (a) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
   (b) 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 that are directly related to an individual, including birth date, admission date, discharge date, death date, 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. **Telephone numbers**

5. **Fax numbers**

6. **Email 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) addresses**

16. **Biometric identifiers, including finger and voice prints**

17. **Full-face photographs and any comparable images**

18. **Any other unique identifying number, characteristic, or code**, except as permitted by paragraph (c) of this section [Paragraph (c) is presented below in the section “Re-identification”]; and
   (ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.
Business Associates

Covered Entities

Bill electronically
• Doctors
• Dentists
• Hospitals
• Skilled Nursing Facilities
• Pharmacies
• Health Plans

Business Associates

Maintain or Access PHI
• IT Companies
• EHR software
• Data Centers
• Cloud Vendors
• Paper Shredding
• Records Storage
• Copier Repair
• Billing
• Collections
• Healthcare org. lawyers
• Expert Witnesses
• Accountants
• Transcription
TPO

• **Covered Entities may share data** with other CE’s & Business Associates for the purposes of **Treatment**, **Payment**, and health care **Operations**

  - **Treatment** – specialists, pharmacies, labs, patient transfers,
  - **Payment** – bills and correspondence to/from providers and payers
  - **Health Care Operations** – Quality assessment, case management, training, accreditation
HIPAA Outlives You by 50 years

HERE LIES OUR PATIENT
DIED 2015
PROTECTED BY HIPAA
UNTIL 2065
Every business in ALL 50 states is regulated

- ALL states, plus Washington, DC, Guam, Puerto Rico, & USVI
- Protect:
  - Social Security Number
  - Driver’s License Number or state issued ID card
  - Account number, credit or debit card with access info
- 20 states protect Medical Records
  Beyond HIPAA
- States have shorter reporting deadlines
- You must comply with the laws protecting data on customers whose info you have, not just where you are
- **YOU HAVE MORE STAFF DATA THAN CLIENT DATA**

CANADA – PIPEDA
Alberta
British Columbia
Quebec
HIPAA BUSINESS ASSOCIATES
Cloud Services, Data Centers (2016)

• **Cloud Services & Data Centers are Business Associates,** even when:
  - They have no access to their customer’s electronic Protected Health Information (ePHI),
  - Their customer’s ePHI is encrypted and they don’t have the encryption key,
  - They never look at their customer’s ePHI,
  - Their customers manage the access to their own ePHI in the cloud,
  - Their terms and conditions prohibit the storage of ePHI, and
  - They only store ePHI ‘temporarily’ and somehow think they should be exempt
Compliance Responsibility

Patient

Covered Entity

Business Associate

Subcontractor

Business Associate

IT Company

Online Backup

Data Centers
## Relationships & Agreements

<table>
<thead>
<tr>
<th>Patient</th>
<th>Covered Entity</th>
<th>Business Associate</th>
<th>Subcontractor Business Associate</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPP</td>
<td>BAA</td>
<td>Sub-BAA</td>
<td>Cloud Services</td>
</tr>
<tr>
<td>Notice of Privacy Practices</td>
<td>Business Associate Agreement</td>
<td>Subcontractor Business Associate Agreement</td>
<td>Online Backup</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Data Centers</td>
</tr>
</tbody>
</table>
Threats Have Changed

Then

Now
Security Is More Important Now

IBM Security

Ransomware increased 6,000 percent in 2016

The average ransomware attachment rate in spam rose from an average of 0.61% in 2015 to nearly 40% YTD in 2016.

Per the IBM survey, seven in ten of those who have experience with ransomware attacks (70 percent) have paid to get data back. Resolution has come at a hefty price for some, with more than half paying over $10,000.

- 20 percent paid more than $40,000
- 25 percent paid $20,000 – $40,000
- 11 percent paid $10,000 – $20,000
Basics Count

81% of hacking-related breaches leveraged stolen and/or weak passwords
January 14, 2020

• Windows 7 Professional End-of-Life
• Windows Server 2008 R2 End-of-Life

• Budget Now
• New Computers & Servers → New Operating Systems
• Plan Replacement Projects
Security & Compliance

Security Compliance

Policies

Procedures

Evidence
Assess, Correct, & Maintain Total Compliance

- **PRIVACY RULE**: Protects all PHI spoken, written, electronic

- **SECURITY RULE**: Framework to protect electronic PHI

- **STATE DATA BREACH LAWS**: Breach Notification & Reporting

- **BREACH NOTIFICATION RULE**: Breach Notification & Reporting

- **CONTRACTS LICENSES**: Data Breach Insurance Policy

©2019 Semel Consulting LLC      MAY NOT BE SHARED OUTSIDE YOUR ORGANIZATION WITHOUT PERMISSION          www.semelconsulting.com
Questions

mike@semelconsulting.com