Cyber Security Awareness and the importance of HIPAA/HITECH Compliance in the Healthcare Industry

By: Marco Polizzi, HCISPP, MHA, LHRM, RN.

Delta Cyber Security Systems LLC
Fort Myers, FL
Disclosures

- I have no disclosures
Overview

• Signs of the Times: Adapting to Ever Changing Technology
• HIPAA: In The Beginning...
• Healthcare Industry Data Breaches
• Today’s Cyber Security Threats in Healthcare Industry, The Law & Countermeasures
Signs of the Times: Adapting to Ever Changing Technology

Over the past 10 years...

The internet has grown exponentially

Number of internet users

- 812 million in 2004
- 2.7 billion in 2013

The world's projected population by 2017 will be about 3.6 billion internet users, more than 48% of the world's projected population.
Our Virtual Social Live

AND WE'VE BECOME MORE SOCIAL

NUMBER OF MONTHLY ACTIVE Facebook USERS

2005: 6 million
2013: 1.15 billion

4/10 social network users have fallen victim to cybercrime on social networking platforms

1/6 social network users report that someone has hacked into their profile and pretended to be them

3/4 believe cybercriminals are setting their sights on social networks

1/10 social network users have fallen victim to a scam or fake link on social network platforms
Daily Live = BYOD

WE'RE RELYING MORE ON OUR MOBILE DEVICES

US CELL PHONE SUBSCRIBERS

192.1 MILLION
2004

326.4 MILLION
2012

91% of adults are now using cell phones
51% of high school students carry a smartphone with them to school everyday
28% have used mobile banking in the past 12 months
$1.3 TRILLION of global mobile payments are predicted to exceed by 2017
Virtual Tools: The Apps

AND USING APPS TO SIMPLIFY OUR LIVES

NUMBER OF ANDROID APPS

1 MILLION
2013

58% of all teens have downloaded apps to their cell phone or tablet computer.
Technology’s Affecting our Lives

But the growth of technology comes with **increased risk**

- **556M per year**
- **1.5M per day**
- **18 per sec**
HIPAA: In The Beginning...

Extracts from HIPAA Regulations: Definitions

- Health Insurance Portability and Accountability Act of 1996
- 45 CFR 160.103 Health Insurance Reform: Privacy and Security Standard; Final Rule – General Administrative Requirements; Definitions
- 45 CFR 164.514: HIPAA Privacy Rule

CFR: Code of Federal Regulations
• **HIPAA – 1996 - 2003**
  - Law Enforcement (LE) & Investigative authority for potential violations to the Attorney General of each state; investigated by OIG (Office of the Inspector General) began in 4/2003

• **HITECH/ARRA – 2003 & Modification 2013**
  - The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of The American Recovery and Reinvestment Act in 2009 and included:
    - The final Breach Notification Rule
    - Updates to Business Associate responsibilities
    - Expansion of the penalty consequences & LE
Complaint & LE Process

HIPAA Privacy & Security Rule Complaint Process

Complaint
- Possible Criminal Violation

Intake & Review
- Possible Privacy or Security Rule Violation

DOJ
- Accepted by DOJ
- DOJ declines over & refers back to OCR

Investigation

Resolution
- OCR finds no violation
- OCR obtains voluntary compliance, corrective action, or other agreement
- OCR issues formal finding of violation

Resolution Criteria
- The violation did not occur after April 14, 2003
- Entity is not covered by the Privacy Rule
- Complaint was not filed within 180 days and an extension was not granted
- The incident described in the complaint does not violate the Privacy Rule
1 out 6 Data Breaches that occurred in 2009 was targeted at Healthcare Industry...

Open Security Foundation
http://www.openinfosecfoundation.org/
HIPAA Security Rule (HSR) Overview & NIST Countermeasures Toolkit

- HSR establishes national standards for a covered entity to protect individuals’ electronic personal health information (ephi)
Consequences, and Price Tag...

**HIPAA Penalties Based on ARRA, 2009**

<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA</td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to reasonable cause and not due to willful neglect</td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to willful neglect but violation is corrected within the required time period</td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation is due to willful neglect and is not corrected</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>
Resolution Agreements
Resolution Agreements and Civil Money Penalties reported at hhs.gov

- HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software
- $800,000 HIPAA Settlement in Medical Records Dumping Case - June 23, 2014
- Data Breach Results in $4.8 Million HIPAA Settlements - May 7, 2014
- Concentra Settles HIPAA Case for $1,725,220 - April 22, 2014
- QCA Settles HIPAA Case for $250,000 - April 22, 2014
- County Government Settles Potential HIPAA Violations - March 7, 2014
- Resolution Agreement with Adult & Pediatric Dermatology, P.C. of Massachusetts - December 20, 2013
- HHS Settles with Health Plan in Photocopier Breach Case - August 14, 2013
- WellPoint Settles HIPAA Security Case for $1,700,000 - July 11, 2013
- Shasta Regional Medical Center Settles HIPAA Privacy Case for $275,000 - June 13, 2013
- Idaho State University Settles HIPAA Security Case for $400,000 - May 21, 2013
The biggest 2014 health data breaches listed on the federal tally so far demonstrate that security incidents are stemming from a variety of causes, from hacker attacks to missteps by business associates.
Information Compromised:

Names, addresses, birthdates, telephone numbers, in some instances Social Security numbers, health insurer names, radiology procedures, diagnoses

Touchstone
MEDICAL IMAGING

307,000 Patients Affected

The organization became aware in May “that a seldom-used folder containing patient billing information relating to dates prior to August 2012 had inadvertently been left accessible via the Internet.”

Business Associate Involved: No
Information Compromised:
Names, addresses, birthdates,
television numbers,
Social Security numbers

CHS Community Health Systems

4.5 Million Patients Affected

Forensic experts believe an advanced persistent threat group originating from China used highly sophisticated malware and technology to attack the hospital chain's systems.

Business Associate Involved: No

CONFIDENTIAL
Information Compromised:
Names, birthdates, Medicaid numbers, medical and billing records, diagnosis codes, reports, photographs

TEXAS
Health and Human Services Commission

CONFIDENTIAL

2 Million Patients Affected

The breach arose from a legal dispute between the state and its former contractor, Xerox. When the state ended its contract with Xerox, the vendor allegedly failed to turn over to the state computer equipment, as well as paper records.

Business Associate Involved: Yes
Information Compromised:
Names, birthdates, Medicaid numbers, medical and billing records, diagnosis codes, reports, photographs

COUNTY OF LOS ANGELES
Public Health

342,000 Patients Affected
Sutherland Healthcare Services – L.A. County’s vendor – had eight unencrypted desktop computers stolen from its offices.

Business Associate Involved: Yes
The Real Cost of Data Breach
Ponemon Institute Releases 2014 Cost of Data Breach

• Overall the average cost of a data breach across all industries was $194 per record

• The cost of a data breach in healthcare was $240 per record!!

http://www.ponemon.org/
Compromised information presents the following potential risks to patients:

- **IDENTITY THEFT**
- **INSURANCE FRAUD**
- **DANGEROUS HOAXES**
- **STOLEN PRESCRIPTIONS**
- **TAMPERING OF MEDICAL RECORDS**
Solution & Countermeasures

Security Considerations

- Hacker attacks against healthcare likely to increase
- Insiders still pose biggest threat to most entities
- More scrutiny needed on business associate relationships

Sources: HHS Office for Civil Rights, Community Health Systems, Texas Health and Human Services Commission, Los Angeles County Departments of Health Services and Public Health, Touchstone Medical Imaging, Redspin, Experian
Countermeasures to Protect EPHI: Adopting the Basic Principles of Information Security - CIA
Adopting an Ongoing Dynamic Assessment & Implementation: Security Controls

- **Technical Safegards/Controls:**
  - Access/Authentication
  - Audits
  - Encryption
  - BYOD – Cellular/Tablet, etc.

- **Physical Safegards/Controls:**
  - Facility Access
  - Workstations Use/Security

- **Administrative Safeguards/Controls:**
  - Policies & Procedures
  - Awareness & Education
  - Legal/Risk Management
Too Small to Be Safe?

America’s small businesses must take online security more seriously.

Small businesses form backbone of U.S. economy.

1 in 2 American workers are employed in a small business.

65% of small firms

15 million net new jobs created between 1993 and 2009.
Physical Safeguards: Examples of Failed Security

Unauthorized worker!

Server cables going unprotected in main hallway
Physical Safeguards: Examples of Failed Security Continues...
Physical Safeguards:
Examples of Failed Security Continues...
Physical Safeguards: Examples of Failed Security Continues...
Conclusion...
Let’s Keep our Industry Secure!

- RE: CYBER - CEO INITIATIVE
- ASSESS YOUR RISKS
- MONITOR THREATS
- REPORT CYBER ATTACKS
- IMPLEMENT A CYBERSECURITY PLAN
- PROTECT YOUR CUSTOMERS
- TRAIN YOUR EMPLOYEES
References

- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 C.F.R. 160.306
- "University of California settles HIPAA Privacy and Security case involving UCLA Health System facilities".
- CMS Transactions and Code Sets Regulations
- "The Looming Problem in Healthcare EDI: ICD-10 and HIPAA 5010 migration" October 10, 2009 - Shahid N. Shah
- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 CFR Sections 160.102 and 160.103
- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 C.F.R. 160.306
- "University of California settles HIPAA Privacy and Security case involving UCLA Health System facilities".
- CMS Transactions and Code Sets Regulations
- "The Looming Problem in Healthcare EDI: ICD-10 and HIPAA 5010 migration" October 10, 2009 - Shahid N. Shah
- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 CFR Sections 160.102 and 160.103
- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 C.F.R. 160.306
- "University of California settles HIPAA Privacy and Security case involving UCLA Health System facilities".
- CMS Transactions and Code Sets Regulations
- "The Looming Problem in Healthcare EDI: ICD-10 and HIPAA 5010 migration" October 10, 2009 - Shahid N. Shah
- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 CFR Sections 160.102 and 160.103
- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 C.F.R. 160.306
- "University of California settles HIPAA Privacy and Security case involving UCLA Health System facilities".
- CMS Transactions and Code Sets Regulations
- "The Looming Problem in Healthcare EDI: ICD-10 and HIPAA 5010 migration" October 10, 2009 - Shahid N. Shah
- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 CFR Sections 160.102 and 160.103
- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 C.F.R. 160.306
- "University of California settles HIPAA Privacy and Security case involving UCLA Health System facilities".
- CMS Transactions and Code Sets Regulations
- "The Looming Problem in Healthcare EDI: ICD-10 and HIPAA 5010 migration" October 10, 2009 - Shahid N. Shah
- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 CFR Sections 160.102 and 160.103
- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 C.F.R. 160.306
- "University of California settles HIPAA Privacy and Security case involving UCLA Health System facilities".
- CMS Transactions and Code Sets Regulations
- "The Looming Problem in Healthcare EDI: ICD-10 and HIPAA 5010 migration" October 10, 2009 - Shahid N. Shah
- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 CFR Sections 160.102 and 160.103
- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 C.F.R. 160.306
- "University of California settles HIPAA Privacy and Security case involving UCLA Health System facilities".
- CMS Transactions and Code Sets Regulations
- "The Looming Problem in Healthcare EDI: ICD-10 and HIPAA 5010 migration" October 10, 2009 - Shahid N. Shah
- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 CFR Sections 160.102 and 160.103
- "How to File A Health Information Privacy Complaint with the Office for Civil Rights"
- 45 C.F.R. 160.306
- "University of California settles HIPAA Privacy and Security case involving UCLA Health System facilities".
- CMS Transactions and Code Sets Regulations
- "The Looming Problem in Healthcare EDI: ICD-10 and HIPAA 5010 migration" October 10, 2009 - Shahid N. Shah