Industry leading Education
Today’s Webinar

- The Age of Ransomware: New threats to the Healthcare industry, Data Security, and HIPAA Compliance

Upcoming Webinars

- How to Pass a HIPAA Audit
  - Tuesday, Oct 25th 2PM ET

Past Webinars

The Age of Ransomware

Ross Gauthier
Mark Haskelson
Patrick Rougeau
What is Ransomware?

“Malware that attempts to extort money from a computer user by infecting and taking control of the victim’s machine, files, or documents”
- **Crypto (64%)**
  - Data Locker
  - Targets Specific Files

- **Locker (36%)**
  - Computer Locker
  - Targets Entire System
How It Works

Infected link received in email

Infected web page

Malware

Internet Explorer

Firefox

Chrome

Flash

Adobe Reader

*Ransomware*

Malware that encrypts data on the PC, blocks user out and asks for a ransom to provide the decryption key.
How Does It Spread?

- Spam Email Messages
- Infected Webpages
- Executable Files
- Downloads and Botnets
- Software Exploits
Attacks on the Rise

- $200 million in first half of 2016
- Different Variants
- 33% of Data Loss Attributed to Cyber Crime
- Healthcare Top Target
Data Breaches and Healthcare

Marc Haskelson
Compliancy Group
# HHS Wall of Shame

<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</th>
<th>Individuals Affected</th>
<th>Breach Submission Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical College of Wisconsin</td>
<td>WI</td>
<td>Healthcare Provider</td>
<td>3179</td>
<td>09/02/2016</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>Center for Neurosurgical &amp; Spine Disorders, LLC</td>
<td>LA</td>
<td>Healthcare Provider</td>
<td>824</td>
<td>08/31/2016</td>
<td>Hacking/IT Incident</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Orleans Medical Clinic</td>
<td>IN</td>
<td>Healthcare Provider</td>
<td>6890</td>
<td>08/19/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>New York State Office of Mental Health</td>
<td>NY</td>
<td>Healthcare Provider</td>
<td>21880</td>
<td>08/15/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Valley Anesthesiology and Pain Consultants</td>
<td>AZ</td>
<td>Healthcare Provider</td>
<td>882590</td>
<td>08/12/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Newkirk Products, Inc.</td>
<td>NY</td>
<td>Business Associate</td>
<td>3466120</td>
<td>08/09/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Professional Dermatology Care, P.C.</td>
<td>VA</td>
<td>Healthcare Provider</td>
<td>13237</td>
<td>08/09/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Prosthetic &amp; Orthotic Care, Inc.</td>
<td>MO</td>
<td>Healthcare Provider</td>
<td>23015</td>
<td>08/07/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Banner Health</td>
<td>AZ</td>
<td>Healthcare Provider</td>
<td>3620000</td>
<td>08/03/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server, Other</td>
</tr>
<tr>
<td>Midwest Orthopedic Pain and Spine</td>
<td>MO</td>
<td>Healthcare Provider</td>
<td>29153</td>
<td>07/26/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Neurology Physicians LLC</td>
<td>MD</td>
<td>Healthcare Provider</td>
<td>4831</td>
<td>07/20/2016</td>
<td>Hacking/IT Incident</td>
<td>Other</td>
</tr>
<tr>
<td>Lee Rice D.O., Medical Corp DBA Lifewellness Institute</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>2473</td>
<td>07/15/2016</td>
<td>Hacking/IT Incident</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>Blaine Chiropractic Center</td>
<td>MN</td>
<td>Healthcare Provider</td>
<td>1945</td>
<td>07/14/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Health Incent, LLC</td>
<td>TN</td>
<td>Healthcare Provider</td>
<td>1100</td>
<td>07/11/2016</td>
<td>Hacking/IT Incident</td>
<td>Other</td>
</tr>
<tr>
<td>Dr. Q Pain and Spine d/b/a Arkansas Spine and Pain</td>
<td>AR</td>
<td>Healthcare Provider</td>
<td>17100</td>
<td>07/11/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Heart Center of Southern Maryland, L.L.P.</td>
<td>MD</td>
<td>Healthcare Provider</td>
<td>1350</td>
<td>07/07/2016</td>
<td>Hacking/IT Incident</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>The Ambulatory Surgery Center at St. Mary</td>
<td>PA</td>
<td>Healthcare Provider</td>
<td>13000</td>
<td>07/07/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Massachusetts General Hospital</td>
<td>MA</td>
<td>Healthcare Provider</td>
<td>4293</td>
<td>06/29/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Uncommon Care, P.A.</td>
<td>NC</td>
<td>Healthcare Provider</td>
<td>13674</td>
<td>06/21/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Allergy, Asthma &amp; Immunology of the Rockies, PC</td>
<td>CO</td>
<td>Healthcare Provider</td>
<td>6851</td>
<td>06/17/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Laser &amp; Dermatologic Surgery Center</td>
<td>MO</td>
<td>Healthcare Provider</td>
<td>31000</td>
<td>06/14/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>EDWARD G. MYERS D.O. INC</td>
<td>OH</td>
<td>Healthcare Provider</td>
<td>6441</td>
<td>06/10/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Grace Primary Care, PC</td>
<td>TN</td>
<td>Healthcare Provider</td>
<td>6853</td>
<td>06/07/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Vincent Vein Center</td>
<td>CO</td>
<td>Healthcare Provider</td>
<td>2250</td>
<td>06/07/2016</td>
<td>Hacking/IT Incident</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>The Vein Doctor</td>
<td>MO</td>
<td>Healthcare Provider</td>
<td>3000</td>
<td>06/03/2016</td>
<td>Hacking/IT Incident</td>
<td>Electronic Medical Record, Network Server</td>
</tr>
<tr>
<td>My Pediatrician, PA</td>
<td>FL</td>
<td>Business Associate</td>
<td>2500</td>
<td>06/01/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
</tbody>
</table>

855-85-HIPAA
© 2016 Compliancy Group, LLC
What is HIPAA?

**HIPAA / HITECH**
Protect patient confidentiality while furthering innovation and patient care

**Omnibus (September 2013)**
Business Associates must protect PHI

**Meaningful Use**
Accelerate adoption of EHR (electronic Health records)

**Compliance vs. Security**
Fines vs. Risk

*2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute© Research Report
855-85-HIPAA
© 2016 Compliancy Group, LLC*
Compliance vs. Security

Compliance:
- Audits
  - Security, Privacy, and Administrative
- Gap Identification
- Remediation
- Policies & Procedures
- Employee Training & Attestation
- Business Associate Management
  - BA Agreements & Audit
  - Incident Management

Security:
- Security Risk Analysis
  - Penetration Testing
  - Vulnerability Scan
- Network Security
- Managed Services
- IT Consulting
- Cloud Services

Security Risk Assessment

FINES

REPUTATION

RISK
Avoidable Breach

- **Who:** Anchorage Community Mental Health Services (ACMHS) - *Nonprofit org. (Alaska)*
- **What:** Malware caused breach of unsecured ePHI
- **Why:** “ACMHS had adopted policies and procedures in 2005, but these *policies and procedures were not followed and/or updated.*” ACMHS could have avoided the breach (and not be subject to the settlement agreement), if it had followed its own policies and procedures
- **Settlement:** $150,000 & CAP (Corrective Action Plan) (12/2014)
Ransomware in Healthcare

- 88% of all ransomware is detected in the healthcare industry
- ~4,000 ransomware attacks average per day in Q1 2016
Cost Per Record

- Health care breaches = #1 in number of records compromised
- $363 = Average cost of healthcare data breach PER record
- 48% of patients would change provider after a data breach
- 50% believe their health care providers can’t adequately protect their PHI.

*2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute® Research Report
855-85-HIPAA
© 2016 Compliancy Group, LLC
Are You Confident Your Healthcare Providers’ Security Measures Protect Your Medical Records

68%  Not confident

Did Your Provider’s Negligence Cause Or Contribute to Identify Theft

53%

HIPAA compliance as a differentiator

Fitbit Inc. – announces its HIPAA compliance, stock price soared (26%)

Causes Of A HIPAA Audit

- Breach Notification
- Business Associates
- Phase 2 Random
- Meaningful Use Failure
- Reported
  - Whistleblower
  - Complaint

Audit Risk-O-Meter
- Low
- Medium
- High

HHS is REQUIRED by law to investigate ALL HIPAA violation complaints
What Are Your Odds?

- Winning Lotto: 1 in a 175 Million
- Attacked by a shark: 1 in a 11.5 Million
- Hit by Lightning: 1 in a 960,000
- Hole in One: 1 in a 12,500
- Random HIPAA Audit: 1 in 10,000
- Meaningful use Audit: 1 in 20
- Breach-Related Audit: 1 in ???
Questions?

Patrick Rougeau
646-747-0556
patrick.rougeau@keepitsafe.com

Marc Haskelson
855-854-4722 Ext 507
Marc@compliancygroup.com