CYBERSECURITY IN THE POST-ACUTE ARENA

AGENDA

1. Introductions
2. Assessing Your Organization
3. Prioritizing Your Review
4. 2016 Benchmarks and Breaches
5. Compliance 101 & Cybersecurity 101
6. Common Threats & Vulnerabilities
7. Compliance Metrics
## INTRODUCTIONS

### Amy Brantley | Chief Compliance Officer, Reliant Post-Acute Care Solutions

**Background**
- Attorney – 25 years experience
- Healthcare – 14 years experience
  - Healthcare Experience
- Reliant Post-Acute Care Solutions (current)
- Golden Living
- Arkansas Children’s Hospital

**Positions**
- Chief Compliance Officer & EVP IT
- Chief Privacy Officer
- Assistant GC Healthcare & VP Compliance
- Labor & Employment Counsel

### Lisa Spears | Privacy and Information Security Officer, Reliant Post-Acute Care Solutions

**Background**
- Healthcare – Golden Living - 23 years experience
  - Roles at Golden Living
- Information Systems Security
- Process Improvement
- Project Management (PMP)
- Information Systems Management (CISM)
- IT Audit (CISA)

**Positions**
- Chief Information Security Officer
- VP Enterprise Project Management & Internal Controls
- Director Process Improvement
- Manager IT Systems Audit
ASSESSING YOUR ORGANIZATION

- Compliance Structure
- Company (large vs small)
- IT Structure
- 3rd Party Vendors
- Size and internal expertise
- Size and internal expertise vs. external
- Degree of reliance upon 3rd party vendors

PRIORITIZING YOUR REVIEW

**Small Organizations**
- Third Party Vendors
- Information Technology
- Internal Resources

**Large Organizations**
- Information Technology
- Organization Privacy Program
- Third Party Vendor/BA
Study Participants: 91 covered entities and 84 business associates

- $6.2B ➔ Cost of breaches to healthcare organizations
- 90% ➔ Healthcare organizations in the study having a data breach in past 2 years
- 45% ➔ Healthcare organizations in the study having a more than 5 data breach in past 2 years
- $2.2M ➔ Average estimated cost of a breach

---

Examples of 2016 Breaches

**Centene**

Announced January – 2016

- Centene - multi-line health-care enterprise
- 950,000 members potentially impacted
- 6 hard drives lost with PHI
- Lab services from 2009 to 2015
- It is not clear if the devices were encrypted

**IRS**

February 2016

- IRS
- Data breach exposing information of more than 700,000 individuals
- Hackers accessed the information, including Social Security numbers and other personal information, through the IRS’ “Get Transcript” program
- The IRS first reported the breach in May 2015, saying it affected 114,000 accounts. That number was expanded in February 2016 to include as many as 724,000 accounts affected.

**21st Century Oncology**

Announced March – 2016

- 21st Century Oncology, a Fort Myers, Fla.-based cancer care provider
- 2.2 million patients based across all 50 states and internationally.
- Hackers broke into a company database in October, accessing personal information of patients, including names, Social Security numbers, physician names, diagnosis, treatment data and insurance information.
- The company said it had “no indication that the information has been misused in any way.”

**FBI**

February 2016

- Nearly 30,000 FBI and Department of Homeland Security workers affected
- Records included personal information on around 9,000 DHS employees and around 20,000 FBI employees, including names, titles and contact information.

---

1 Ponemon Institute LLC, Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, May 2016

2 Sarah Kuranda, “The 10 Biggest Data Breaches Of 2016 (So Far)”, [www.CRN.com](http://www.CRN.com), July 28, 2016
**COMPLIANCE 101: HIPAA SECURITY RULE**

**Rule:** All covered entities and their business associates are required to develop and document a security program to guard against real and potential threats of disclosure or loss, which will include policies, procedures and safeguards to protect Electronic PHI (or ePHI).

<table>
<thead>
<tr>
<th>Administrative</th>
<th>Physical</th>
<th>Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Management Process</td>
<td>• Facility Access Controls</td>
<td>• Access Control</td>
</tr>
<tr>
<td>• Assigned Security Responsibility</td>
<td>• Workstation Use</td>
<td>• Audit Controls</td>
</tr>
<tr>
<td>• Workforce Security</td>
<td>• Workstation Security</td>
<td>• Integrity</td>
</tr>
<tr>
<td>• Information Access Management</td>
<td>• Device and Media Controls</td>
<td>• Person or Entity Authentication</td>
</tr>
<tr>
<td>• Security Awareness and Training</td>
<td></td>
<td>• Transmission Security</td>
</tr>
<tr>
<td>• Security Incident Procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Contingency Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Evaluation Business Associate Contracts and Other Arrangements</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**COMPLIANCE 101: HIPAA PRIVACY RULE**

**Rule:**
Protects all “PHI” (protected health information), which includes just about any piece of information that might possibly identify a person, in any form, including oral information.

Grants individuals broader rights in their PHI:

- Access
- Amendment
- Disclosure Accounting
- Restrictions
- Confidential Communications
COMPLIANCE 101: BUSINESS ASSOCIATE

Business Associate (BA)

Definition
Any entity that “creates, receives, maintains, or transmits” PHI in performing a function, activity, or service on behalf of a covered entity.

- Examples: billing companies, accountants, insurance agents/brokers, payroll vendors, consultants, law firms, data processing firms...
- Any entity that has access to PHI to do something for a Covered Entity.

Requirements
Covered Entity (CE) cannot release or disclose PHI to business associates unless both parties have a Business Associates Agreement (BAA) in place. BAA is not a Non Disclosure Agreement (NDA). BAA should minimally include:

- Confidentiality clause
- Breach disclosure requirements and process
- Disposition requirements and process at BAA termination
- Rights of CE to audit the BA

COMPLIANCE 101: BUSINESS ASSOCIATE

Best Practices for Business Associates Engagement

- Select your vendors carefully as they can be jointly or directly liable for security breaches
- Engage all expertise needed (Legal, Procurement, Operations, Security Officer, Privacy Officer) to create a well rounded and all inclusive agreement
- Ask for and review vendor privacy and security policies to get a sense of controls in place
- Make sure basic technical security controls are in place – encryption, patching, anti-virus, password management, etc.
**CYBERSECURITY 101: BASIC TERMINOLOGY**

**Cybersecurity**

The body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

**LAN – Local Area Network**

**Firewall**

**Zero Day Viruses**

**DMZ**

**Vulnerability**

**Patching**

**Server Patched**

**Demilitarized Zone (DMZ)**

**Threat**

**Threats**

- Socially engineered Trojans
- Software with known exploits not patched
- Ransomware
- Phishing
- Viruses
- Zero Day Viruses
- Advanced Persistent Threats (APT)

**Vulnerabilities**

- Un-educated end user
- Poor password management
- Poor access controls
- No check & balance controls
- Stale virus protection
- Poor patch management processes

**Risk Mitigation**

- User Training and Awareness Program
- Strong password controls
- Minimal access necessary
- Good general controls
- Current virus protection
- Sound patch management process
- Encryption
- Limiting Local Administrators

**Risk**
CYBERSECURITY 101: INCIDENT RESPONSE

**Process**
- Detection
- Assessment
- Containment
- Recovery
- Eradication
- Further Action Required?
- Yes: Closure
- No: Detection

**People**
- Executive Team
- Compliance, Privacy, Security Officers
- HR
- IT
- Event Response Team Lead
- External Parties
- Communications
- Law Enforcement
- Legal

---

CYBERSECURITY 101: RISK ASSESSMENT

1. **Conduct Risk Assessment**
2. **Determine risk tolerance**
3. **Prioritize**
4. **Develop action plan**
5. **Execute action plan**
**CYBERSECURITY 101: RISK ASSESSMENT**

<table>
<thead>
<tr>
<th>Threat Description</th>
<th>Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unintentional disclosure to business partners to unauthorized access for system resources</td>
<td>The inadvertent release of non-essential information (e.g., customer data) in nature.</td>
</tr>
<tr>
<td>Unauthorized access</td>
<td>Unintentional unauthorized access is often prevented in nature.</td>
</tr>
</tbody>
</table>

**Example**

Risk Tolerance – Business Decision

![Risk Tolerance Chart](chart.png)

**COMPLIANCE METRICS: EMAIL**

**Current Month Email Stats**

<table>
<thead>
<tr>
<th>Status</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initially Blocked Emails</td>
<td>200</td>
</tr>
<tr>
<td>Quarantined &amp; Blocked</td>
<td>100</td>
</tr>
<tr>
<td>Virus Detected</td>
<td>250</td>
</tr>
<tr>
<td>Quarantined &amp; Released</td>
<td>240</td>
</tr>
<tr>
<td>Allowed Emails</td>
<td>26</td>
</tr>
</tbody>
</table>

**Weekly Heuristics**

- **Total Submissions for analysis:**
  - **Week 4:** 1,024
- **Deemed High Risk:**
  - **9** Submitted to Antivirus

**Outbreak of IRS Phishing emails increased the number of emails blocked and number of emails quarantined & subsequently blocked. No infections encountered.**
COMPLIANCE METRICS: SOFTWARE UPDATES RECEIVED VS. APPLIED

Current Month Patches

- Vulnerabilities Unable to Eliminate
- Vulnerabilities Not Eliminated in 30 days
- Vulnerabilities Eliminated GT 7 and LT 30 days
- Vulnerabilities Eliminated LT 7 days

Patch Management Trends

- Vulnerabilities Unable to Eliminate
- Vulnerabilities Not Eliminated in 30 days
- Vulnerabilities Eliminated GT 7 and LT 30 days
- Vulnerabilities Eliminated LT 7 days

COMPLIANCE METRICS: SOCIAL ENGINEERING

Social Engineering Attacks

- IRS email
- Wire Transfer Request
- Phone Threats - Arrest Warrant
- Bank of America Profile Issue
- Unpaid Invoices
## Compliance Metrics: Policy Review & Attestations

### Policy Annual Review Status

<table>
<thead>
<tr>
<th>Information Security Policies</th>
<th>Review Date</th>
<th>Review Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Policy</td>
<td>1/31/2017</td>
<td></td>
</tr>
<tr>
<td>Access Control Policy</td>
<td>1/31/2017</td>
<td></td>
</tr>
<tr>
<td>Acceptable Use Policy</td>
<td>1/31/2017</td>
<td></td>
</tr>
<tr>
<td>Business Continuity Policy</td>
<td>1/31/2017</td>
<td></td>
</tr>
<tr>
<td>Data Classification Policy</td>
<td>1/31/2017</td>
<td></td>
</tr>
<tr>
<td>Encryption Policy</td>
<td>1/31/2017</td>
<td></td>
</tr>
<tr>
<td>Mobile Devices Policy</td>
<td>6/30/2017</td>
<td></td>
</tr>
<tr>
<td>Media Handling Policy</td>
<td>6/30/2017</td>
<td></td>
</tr>
<tr>
<td>Network Security Policy</td>
<td>6/30/2017</td>
<td></td>
</tr>
<tr>
<td>Physical and Environmental Security Policy</td>
<td>6/30/2017</td>
<td></td>
</tr>
<tr>
<td>Personnel Security Policy</td>
<td>6/30/2017</td>
<td></td>
</tr>
<tr>
<td>Risk Assessment &amp; Treatment Policy</td>
<td>6/30/2017</td>
<td></td>
</tr>
<tr>
<td>Remote Access Policy</td>
<td>12/31/2017</td>
<td></td>
</tr>
<tr>
<td>Software Development Policy</td>
<td>12/31/2017</td>
<td></td>
</tr>
<tr>
<td>Security Monitoring and System Auditing</td>
<td>12/31/2017</td>
<td></td>
</tr>
<tr>
<td>Security Privacy and Incident Reporting</td>
<td>12/31/2017</td>
<td></td>
</tr>
<tr>
<td>Communications &amp; Operations Security</td>
<td>12/31/2017</td>
<td></td>
</tr>
</tbody>
</table>

- Policy review current
- Policy review past due

### Policy Employee Attestation Status

<table>
<thead>
<tr>
<th>Information Security Policies</th>
<th>Policy Attestation</th>
<th>Goal</th>
<th>Status</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Policy</td>
<td>1000</td>
<td>1000</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Access Control Policy</td>
<td>1000</td>
<td>1000</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Acceptable Use Policy</td>
<td>1000</td>
<td>900</td>
<td></td>
<td>90%</td>
</tr>
<tr>
<td>Business Continuity Policy</td>
<td>250</td>
<td>250</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Data Classification Policy</td>
<td>1000</td>
<td>900</td>
<td></td>
<td>90%</td>
</tr>
<tr>
<td>Encryption Policy</td>
<td>100</td>
<td>85</td>
<td></td>
<td>85%</td>
</tr>
<tr>
<td>Mobile Devices Policy</td>
<td>250</td>
<td>250</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Media Handling Policy</td>
<td>1000</td>
<td>1000</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Network Security Policy</td>
<td>250</td>
<td>225</td>
<td></td>
<td>90%</td>
</tr>
<tr>
<td>Physical and Environmental Security Policy</td>
<td>1000</td>
<td>1000</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Personnel Security Policy</td>
<td>1000</td>
<td>1000</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Risk Assessment &amp; Treatment Policy</td>
<td>100</td>
<td>100</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Remote Access Policy</td>
<td>250</td>
<td>225</td>
<td></td>
<td>90%</td>
</tr>
<tr>
<td>Software Development Policy</td>
<td>100</td>
<td>100</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Security Monitoring and System Auditing</td>
<td>100</td>
<td>100</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Security Privacy and Incident Reporting</td>
<td>1000</td>
<td>1000</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>Communications &amp; Operations Security</td>
<td>100</td>
<td>100</td>
<td></td>
<td>100%</td>
</tr>
</tbody>
</table>

### Questions?

![Q&A Image]