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 – 10 years experience
- Reliant Post-Acute Care Solutions (current)
- Golden Living
- Arkansas Children’s Hospital
- Labor & Employment Counsel

Positions

- Chief Compliance Officer & EVP IT
- Chief Privacy Officer
- Assistant GC, Healthcare & VP Compliance
INTRODUCTIONS

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

<table>
<thead>
<tr>
<th>Background</th>
<th>Positions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Healthcare – Golden Living (15 years experience)</td>
<td>• Chief Information Security Officer</td>
</tr>
<tr>
<td>• Information Systems</td>
<td>• VP Enterprise Project Management &amp; Internal Controls</td>
</tr>
<tr>
<td>• Privacy Implementation</td>
<td>• Director Process Improvement</td>
</tr>
<tr>
<td>• Project Management (PMP)</td>
<td>• Manager IT Systems Audit</td>
</tr>
<tr>
<td>• Information Systems Management (ISSM)</td>
<td></td>
</tr>
<tr>
<td>• IT Audit (CISA)</td>
<td></td>
</tr>
</tbody>
</table>

ASSESSING YOUR ORGANIZATION

PRIORITIZING YOUR REVIEW

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

Large Organizations
- Information Technology
- Organization Privacy Program
- Third Party Vendor/BA
### PONEMON INSTITUTE BENCHMARK

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

### EXTERNAL SECURITY BREACHES: 2016

#### Example 1
- **Cardinal - multi-plan healthcare enterprise.**
  - 200,000 policy holders impacted.
  - 8,931,000 EHRs were stolen.

#### Example 2
- **Centene Corporation.**
  - 3.2 million policy holder records were stolen.

#### Example 3
- **Hackers broke into a company database in Idaho, accessing personal information of patients, including names, Social Security numbers, and other personal information.**

#### Example 4
- **IRS.**
  - Lost 2.2 million employees' information.

### 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 (ePHI).

<table>
<thead>
<tr>
<th>Administrative</th>
<th>Physical</th>
<th>Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Plan</td>
<td>Facility Access Controls</td>
<td>Access Control</td>
</tr>
<tr>
<td>Accountability</td>
<td>Medication Management</td>
<td>Audit Controls</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 Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Training</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Incident Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuity Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intra- and Interorganizational</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interorganizational Business</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizations and Other</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

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

Cybersecurity 101: Threats-Vulnerabilities-Mitigations

Threats
- Socially engineered Trojans
- Software with known exploits not patched
- Exploitable vulnerabilities
- 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
- Current patch management process
- Encryption
- Limiting Local Administrators

Cybersecurity 101: Incident Response

Process
- Incident Detection
- Incident Response
- Post Incidence

People
- Executive Team
- Compliance, Privacy, Security Officers
- IT
- Legal
- Communications
- External Parties
- HR
- Law Enforcement
- Internal Officers
- Internal Analysts
- Senior Executive

Post Incidence
- Incident Response Team
**CYBERSECURITY 101: RISK ASSESSMENT**

1. Conduct Risk Assessment
2. Determine risk tolerance
3. Prioritize
4. Develop action plan
5. Execute action plan

**Example**

**Risk Tolerance – Business Decision**

**COMPLIANCE METRICS: EMAIL**

- **Current Month Email Stats**
- **Weekly Heuristics**
  - Total Submissions for analysis: 1,024
  - Declared High Risk: 9
  - Submitted to Antivirus vendor for analysis: 9
  - No infections encountered

Outbreak of IRS Phishing emails increased the number of emails blocked and number of emails quarantined & subsequently blocked. No infections encountered.