Toto we are not in Kansas any more: OCR audits, BAs and data breaches oh my!

Presented by:
Marti Arvin
VP, Audit Strategy
CynergisTek, Inc.

CynergisTek, Inc.

Founded in 2004
CynergisTek has been providing services to our clients since 2004, but many of our clients have been with one or both of the founders since well before the company was founded.

Synergistic
The name “CynergisTek” came from the synergy realized by combining the expertise of the two co-founders – building scalable, mature information security programs and architecting enterprise technical solutions.

Consulting Services
CynergisTek provides consulting services and solutions around information security, privacy, IT architecture, and audit with specific focus on regulatory compliance in healthcare.

Securing the Mission of Care
CynergisTek Services are specifically geared to address the needs of the healthcare community including providers, payers, and their business associates who provide services into those entities.
Agenda

- Safeguard PHI by Managing Vendors
- OCR Enforcement Outlook
- OCR Desk Audit Update
- Cybersecurity Updates for Compliance

Vendor Security Must Improve

- Requirements Definition
- Pre-Contract Due Diligence
- Contract Security Specifications
- Performance Monitoring
- Breach Notification
- Contract Termination
- Documentation
Defining Requirements

- Examine Scope of Effort
- Determine What Level of Minimum Necessary
- Identify Security Requirements
- Develop SLAs for Privacy and Security
- Incorporate into RFI, RFP and/or SOW
- Classify Vendor

Due Diligence: Pre-Contract

- Tailor requests to scope of contract
- Security standard followed
- Include privacy and security questionnaire
- Request documentation
- Review third party assessments
- Proof of Training
- Conduct site visit
- Privacy and security incident history
**Contract Security Specifications**

- Define expectations, material changes, subcontractors
- Minimum Necessary
- Transmission, storage & processing
- Incident response
- Audit/monitoring
- Reporting requirements
- Contingency operations

**Maintenance**

- For contracts lasting more than 6 months
- Periodic audits of key processes
- Testing of contingency plans/operations
- Renewal of third party assessments
Breach Notification

- Timeliness of notifications
- Assistance in investigation/risk assessment
- Indemnification for certain costs
- Notifications to public

Additional considerations

- Language of you BAA
  - Definition of a security incident and BA’s obligation to notify you
  - Definition of a breach and BA’s obligation to notify you.
Contract Termination

- Termination for cause vs. end of contract
- Disposition of data if in receipt
- User/system access
- Reminder of Minimum Necessary
- Other continued responsibilities

OCR Enforcement Outlook
OCR Update

Settlements

Memorial Health System settled for $5.5M over inappropriate access by its own employees & employees of affiliated physician offices.
CardioNet settled for $2.5M because of lack of appropriate security program/no device media control measures.
Presence Health Network settled for $400K over failure to timely notify of a breach.

Guidance

OCR guidance that ransomware incidents are breaches. Cloud computing guidance that any vendor handling PHI is a BA. Also guidance on patient access to PHI. Guidance on breach notification, minimum necessary and distribution of penalties still to come.

OCR Enforcement

• Most resolution agreements cite to Security Rule
  – Enterprise wide risk analysis is foundation
  – Expectation that encryption is used on all portable and mobile devices & media
  – Encryption of network servers when reasonable and appropriate
  – Managing/controls of device & media
  – Contingency planning
OCR Enforcement

• Seeing compliance reviews that:
  – Ask for documentation that goes well beyond the issue that originally brought OCR to the door
  – Ask for documentation around multiple reports of small breaches

Key Issues in OCR’s Enforcement Cases

• Business Associate Agreements
• Risk Analysis
• Failure to Manage Identified Risk, e.g. Encrypt
• Lack of Transmission Security
• Lack of Appropriate Auditing
• No Patching of Software
• Lack of appropriate access monitoring
• Improper Disposal
• Insufficient Data Backup and Contingency Planning
OCR Desk Audit Update

OCR’s Audit Findings

• Total covered entities audited 166
  – 103 for Privacy and Breach Rule compliance
  – 63 for Security Rule compliance
  – Break down of covered entities
    • 9% Health Plans
    • 1% Clearinghouses
    • 90% Providers

• Business Associates audited 41
  – All assessed for Breach Notification and Security Rule compliance
OCR Audit Findings

OCR comments about the audit process: Under OCR’s separate, broad authority to open compliance reviews, OCR could decide to open a separate compliance review in circumstances were significant threats to the privacy and security of PHI are revealed through the audit.

Random Audit RoF Scale

The auditor assessed entity efforts to comply with the selected elements using the following guidelines.

Compliance Effort Ratings—Legend

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The audit results indicate the entity is in compliance with both goals and objectives of the selected standards and implementation specifications.</td>
</tr>
<tr>
<td>2</td>
<td>The audit results indicate that the entity substantially meets criteria; it maintains appropriate policies and procedures, and documentation and other evidence of implementation meet requirements.</td>
</tr>
<tr>
<td>3</td>
<td>Audit results indicate entity efforts minimally address audited requirements; analysis indicates that entity has made attempts to comply, but implementation is inadequate, or some efforts indicate misunderstanding of requirements.</td>
</tr>
<tr>
<td>4</td>
<td>Audit results indicate the entity made negligible efforts to comply with the audited requirements - e.g., policies and procedures submitted for review are copied directly from an association template; evidence of training is poorly documented and generic.</td>
</tr>
<tr>
<td>5</td>
<td>The entity did not provide OCR with evidence of serious attempt to comply with the Rules and enable individual rights with regard to PHI.</td>
</tr>
</tbody>
</table>
### Privacy and Breach Notification Rules

#### Rating at each end of the rankings for all entities (103)

<table>
<thead>
<tr>
<th>Breach Rule</th>
<th>5 Rating</th>
<th>1 Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeliness of Notification</td>
<td>15</td>
<td>67</td>
</tr>
<tr>
<td>Content of Notification</td>
<td>9</td>
<td>14</td>
</tr>
</tbody>
</table>

#### Privacy Rule

<table>
<thead>
<tr>
<th>Access</th>
<th>11</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPP Content</td>
<td>16</td>
<td>2</td>
</tr>
<tr>
<td>Electronic NPP</td>
<td>15</td>
<td>59</td>
</tr>
</tbody>
</table>

#### Security Rule

<table>
<thead>
<tr>
<th>Risk Analysis</th>
<th>13</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management</td>
<td>17</td>
<td>1</td>
</tr>
</tbody>
</table>

### Privacy and Breach Notification Rules

#### Rankings of the covered entities audited (103)

<table>
<thead>
<tr>
<th>Breach Rule</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeliness of Notification</td>
<td>11%</td>
<td>9%</td>
<td>2%</td>
<td>6%</td>
<td>65%</td>
<td>7%</td>
</tr>
<tr>
<td>Content of Notification</td>
<td>7%</td>
<td>37%</td>
<td>23%</td>
<td>14%</td>
<td>14%</td>
<td>5%</td>
</tr>
</tbody>
</table>

#### Privacy Rule

<table>
<thead>
<tr>
<th>Provision of the NPP</th>
<th>15%</th>
<th>6%</th>
<th>4%</th>
<th>15%</th>
<th>57%</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPP Content</td>
<td>15%</td>
<td>11%</td>
<td>39%</td>
<td>33%</td>
<td>2%</td>
</tr>
<tr>
<td>Access right</td>
<td>11%</td>
<td>54%</td>
<td>27%</td>
<td>10%</td>
<td>1%</td>
</tr>
</tbody>
</table>

#### Security Rule

<table>
<thead>
<tr>
<th>Risk Analysis</th>
<th>13</th>
<th>23</th>
<th>19</th>
<th>8</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management</td>
<td>17</td>
<td>29</td>
<td>13</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>
Cybersecurity

Evolving Healthcare Threat Landscape

Cyber Incidents

<table>
<thead>
<tr>
<th>2009 - 2011</th>
<th>2011 Theft</th>
<th>2015</th>
<th>2016</th>
<th>2017*</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCBS Tenn</td>
<td>1.02M Stolen HD</td>
<td>Advocate Medical 4.05M Computer Theft</td>
<td>CareFirst 1.1M Hacking</td>
<td>Premera BCBS 11M Hacking</td>
</tr>
<tr>
<td>AvMed</td>
<td>1.2M Stolen Laptops</td>
<td>Emory</td>
<td>4.5M Hacking</td>
<td>Healthnet 1.9M Lost HD</td>
</tr>
<tr>
<td>NYC Health &amp; Hospitals</td>
<td>2.1M Stolen Backup Tapes</td>
<td>Boston Children Hacktivism Anonymous</td>
<td>Health Net 1.9M Lost Backup Tapes</td>
<td>Nebraska Health 7M</td>
</tr>
<tr>
<td>UHS (CHC)</td>
<td>750K Hacking</td>
<td>Aetna</td>
<td>1.1M Hacking</td>
<td>Orleans Medical Clinic 7M Hacking</td>
</tr>
<tr>
<td>Penn Health</td>
<td>1.6M Lost Backups</td>
<td>Anthem</td>
<td>BCBS 0DM Hacking</td>
<td>Orleans Medical Clinic 7M Hacking</td>
</tr>
<tr>
<td>Michigan</td>
<td>1.6M Lost Backups</td>
<td>CareFirst</td>
<td>1.1M Hacking</td>
<td>Appalachi*op Regional Hospitals 3 Weeks Hacking</td>
</tr>
<tr>
<td>Hewlett-Packard</td>
<td>10 Days Hacking</td>
<td>Baptist</td>
<td>5 Days Hacking</td>
<td>St. Francis 6K Extortion</td>
</tr>
<tr>
<td>Hartford</td>
<td>5 Days Hacking</td>
<td>Emory</td>
<td>225K Hacking</td>
<td>Orleans Medical Clinic 7M Hacking</td>
</tr>
<tr>
<td>CHS</td>
<td>4.5M Hacking</td>
<td>Silk Road</td>
<td>10 Days Hacking</td>
<td>Oral Health Clinic 7M Hacking</td>
</tr>
<tr>
<td>Nemours</td>
<td>1.6M Lost Backups</td>
<td>Emory</td>
<td>4.5M Hacking</td>
<td>Hacking</td>
</tr>
<tr>
<td>Utah</td>
<td>750K Hacking</td>
<td>Emory</td>
<td>225K Hacking</td>
<td>Haley VI 5 Days Hacking</td>
</tr>
<tr>
<td>BlueCross BlueShield</td>
<td>1.1M Hacking</td>
<td>Emory</td>
<td>4.5M Hacking</td>
<td>Blankenbaker VA 5 Days Hacking</td>
</tr>
<tr>
<td>Aetna</td>
<td>1.1M Hacking</td>
<td>Emory</td>
<td>4.5M Hacking</td>
<td>CareFirst 1.1M Hacking</td>
</tr>
<tr>
<td>Baylor</td>
<td>5 Days Hacking</td>
<td>Emory</td>
<td>4.5M Hacking</td>
<td>CareFirst 1.1M Hacking</td>
</tr>
<tr>
<td>Emory</td>
<td>4.5M Hacking</td>
<td>Emory</td>
<td>4.5M Hacking</td>
<td>CareFirst 1.1M Hacking</td>
</tr>
<tr>
<td>Emory</td>
<td>4.5M Hacking</td>
<td>Emory</td>
<td>4.5M Hacking</td>
<td>CareFirst 1.1M Hacking</td>
</tr>
</tbody>
</table>

Disruption
Cybercrime “IS” a Business

The Justice Department predicted Cybercrime would generate $600B in revenues in 2016

- Cybercrime-as-a-service model* gives less technically-savvy criminals access
- Dark web marketplaces make “monetizing” stolen data as easy as buying on Amazon
- Cybercriminals are adopting tactics previously only used by nation-state attackers

Cyber Extortion is Rampant

- First appeared around 2005
- Two forms: Crypto ransomware (data) and Locker ransomware (system)
- Sophisticated attacks use:
  - New asymmetric keys for each infection
  - Industrial strength & private/public key encryption
  - Privacy enabling services like TOR and Bitcoin for payments
- Indifferent to target, everyone is a target (home/business)
- Malvertising, spam email, downloaders/botnets & social engineering

*The United States is the largest target worldwide by a huge margin. SOCs worldwide report as much as a 10X increase in ransomware attacks from December to January with no abatement.
Percentage of Phishing Emails Delivering Ransomware

![Percentage of Phishing Emails Delivering Ransomware](chart.png)

Source: PhishMe Q1 Malware Review

---

Should You Pay Ransom for Your Data?

- US Dept. of Justice Guidance on Ransomware says “No”
- Paying a ransom does not guarantee an organization will regain access to its data; in fact, some victims were never provided with decryption keys after paying ransom
- Some victims who paid the demand have reported being targeted again by cyber actors
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key
- Report ransomware incidents to the FBI using the checklist of information that is helpful to them
Ubiquitous Is The New Paradigm

- Smart phones
- IOT
- Social media
- POS systems
- Medical devices
- Removable media (USBs)
- SPAM & email
- Applications
- Smart TVs
- CCTV cameras
- Environmental systems
- Downloads
- Attachments
- Browsers
- Wearables
- Telehealth

Threats are introduced from all directions, simple compliance strategies will not suffice, an integrated set of controls is needed.

The Insider Threat

- 93% feel vulnerable to insider threats
- 59% worry about privileged users most
- Contractors/service providers next biggest concern
- 2010-2015 20% increase in ID/Med ID theft
- 37% feel user awareness training is failing
- Traditional audit methods are failing right and left
Responding to Cybersecurity Incidents

- What is the scope of incident: What networks, systems or applications are affected?
- Where was the origin of the incident in your network?
  - Who/what/where/when
- Determine whether incident is finished, ongoing or has propagated additional incidents throughout the environment
- How did the incident occur?
- Contain the impact and propagation of the ransomware
  - Tools and attacks methods used, vulnerabilities exploited
- Eradicate the instance of the ransomware

Questions?

Marti Arvin
Marti.arvin@cynergistek.com
510-402-8550, Ext 7051