IT Audit Process

Prof. Mike Romeu

September 30, 2015
Agenda

• Quiz and AWA Case Review
• Laws and Regulations (continued)
  • HIPAA/HITECH, PCI DSS, SOX
• Standards and Guidelines
Health Information Portability and Accountability Act (HIPAA)

• Covered Entity – 1) Health Plans; 2) Healthcare Clearinghouses; 3) Health Care Providers who electronically transmit any health information in connection with transactions for which the Department of Health and Human Services (HHS) has adopted standards.

• HIPAA Establishes a national standard for electronic patient health information and reasonable security and privacy of patient data.

• HIPAA became effective in 2003 with enforcement effective beginning in 2006.

• Department of Health and Human Services (HHS) must provide for periodic audits to ensure covered entities are in compliance with HIPAA Standards.

• HHS Audit Program Protocol = Standard for HIPAA auditing

• Business Associate provision - a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or as a service to, a covered entity. The BA provision does not transfer compliance responsibility to the service provider. It extends the regulation to the SO.
HIPAA – Security Standards

• **Administrative Safeguards** - these are the administrative functions that should be implemented to meet the security standards. These include assignment or delegation of security responsibility to an individual (HIPAA Security Officer) and security training requirements.

• **Physical Safeguards** - these are the mechanisms required to protect electronic systems, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion. They include restricting access to EPHI and retaining off site computer backups.

• **Technical Safeguards** - these are primarily the automated processes used to protect data and control access to data. They include using authentication controls to verify that the person signing onto a computer is authorized to access that EPHI, or encrypting and decrypting data as it is being stored and/or transmitted.
HIPAA – Administrative Safeguards

- Security Management Process
- Assigned Security Responsibility (HIPAA Security Officer)
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedure
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements
HIPAA – Physical and Technical Safeguards

<table>
<thead>
<tr>
<th>Physical Safeguards</th>
<th>Technical Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Facility Access Control</td>
<td>• Access Controls</td>
</tr>
<tr>
<td>• Workstation Use</td>
<td>• Audit Controls</td>
</tr>
<tr>
<td>• Workstation Security</td>
<td>• Integrity</td>
</tr>
<tr>
<td>• Device and Media Control</td>
<td>• Person or Entity Authentication</td>
</tr>
<tr>
<td></td>
<td>• Transmission Security</td>
</tr>
</tbody>
</table>
Payment Card Industry Data Security Standard (PCI DSS)
<table>
<thead>
<tr>
<th>Goal</th>
<th>PCI DSS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Build and Maintain a Secure Network</strong></td>
<td>1. Install and maintain a firewall configuration to protect cardholder data.</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters.</td>
</tr>
<tr>
<td><strong>Protect Cardholder Data</strong></td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td><strong>Maintain a Vulnerability Management Program</strong></td>
<td>5. Use and regularly update anti-virus software or programs.</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td><strong>Implement Strong Access Control Measures</strong></td>
<td>7. Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access.</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td><strong>Regularly Monitor and Test Networks</strong></td>
<td>10. Track and monitor all Access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes.</td>
</tr>
<tr>
<td><strong>Maintain an Information Security Policy</strong></td>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
</tbody>
</table>
PCI DSS

- Level 1 – Over 6 million transactions processed per year
- Level 2 – 1 million to 6 million transactions processed per year
- Level 3 – 20,000 to 1 million transactions processed per year
- Level 4 – Up to 20,000 transactions processed per year

- Only Level 1 has a requirement for regular compliance audits
Sarbanes-Oxley Act of 2002 (SOX)

• Section 302 – Disclosure of Internal Controls

• Section 404 – Assessment of Internal Controls
  • Financial
  • IT General Controls with direct and indirect impact on financial reporting
  • Requires Annual Assessment by management and Independent Auditors
Figure 3—Common Elements of Enterprises

**Entity-level Controls**
Entity-level controls set the tone and culture of the enterprise. IT entity-level controls are part of a company’s overall control environment.

Controls include:
- Strategies and plans
- Policies and procedures
- Risk assessment activities
- Training and education
- Quality assurance
- Internal audit

**Application Controls**
Controls embedded within business process applications directly support financial control objectives. Such controls can be found in most financial applications including large systems such as SAP® and Oracle® as well as smaller systems such as Sage 300 ERP.

Control objectives/assertions include:
- Completeness
- Accuracy
- Existence/authorization
- Presentation/disclosure

**IT General Controls**
Controls embedded within IT processes that provide a reliable operating environment and support the effective operation of application controls.

Controls include:
- Program development
- Program changes
- Access to programs and data
- Computer operations