SECURING HEALTH INFORMATION IN THE CLOUD

Feisal Nanji, Executive Director, Techumen
feisal@techumen.com
Conflict of Interest Disclosure

Feisal Nanji, MPP, CISSP

Has no real or apparent conflicts of interest to report.
LEARNING OBJECTIVES

• Describe the advantages of Cloud computing for Health Providers
• Identify the major concerns of securing health information in the cloud
• Recognize the key steps to overcoming health information security and privacy issues in the cloud
• Define a suitable audit and compliance process to ensure security and privacy in the cloud
WHAT SHOULD YOU TAKE AWAY?

1. **Level set** – Core technology for cloud computing
2. Cloud computing -- variants
3. What are the key compliance / security concerns of the cloud?
4. How should we manage security in the cloud?
CORE TECHNOLOGY

• Fast networks
• Web enabled eco-system
• The “Virtual Machine”
Virtual Infrastructure

Application
Operating System
Virtual Machine

STORAGE NETWORK SERVERS STORAGE
VIRTUALIZATION CONCERNS...

- Increases complexity
- Strains infrastructure
- Can cause large-scale failure
- Requires special maintenance
THIS ALLOWS......

• Computing capability on demand
• Resource pooling – storage, CPU
• Rapid deployment and scaling of IT services
• Easy measurement of what’s been used
LEADING TO CLOUD VARIANTS....

• Infrastructure as a service (IaaS)
• Platform as a service (PaaS)
• Software as a service (SaaS)
Infrastructure as a Service (IaaS)
Platform as a Service  (PaaS)

- INTEGRATION AND MIDDLEWARE
- APPLICATION PROGRAMMING INTERFACES
- VIRTUALIZATION AND CORE CONNECTIVITY
- HARDWARE AND DATA CENTER FACILITIES
Software as a Service (SaaS)
CLOUD: A SUMMARY

Essential Characteristics

- Broad Network Access
- Rapid Elasticity
- Measured Service
- On-Demand Self-Service

Resource Pooling

Service Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Deployment Models

- Public
- Private
- Hybrid
- Community
CLOUD – HELPING HEALTH CARE....

- Providers, EMR vendors, Health Plans, Government, HIE etc.
- Cheaper and faster
- Better compliance (security)???
TRADITIONAL DATA CENTER SECURITY APPROACHES...

• Physical configuration management governs deployment and control implementation --- standards for specification, configuration, and operation

• Physical control as the ultimate breakwater for logical access control to platforms and applications

• Enterprise policies and organization for separation of duties and control

• Patch testing and patch management ... physical-platform-by-physical-platform

• Data and applications are wherever the machine is and networks are between machines
BUT AS “PHYSICAL” VISIBILITY IS LOST....

• Where is the data?
• Who can see the data?
• Who has seen the data?
• Has data been tampered?
• Where is processing performed?
• How is processing configured?
• Does backup happen? How? Where?
AND COMPLIANCE -- IS NOT JUST SECURITY

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HIPAA Security</td>
</tr>
<tr>
<td>2</td>
<td>Medical Fraud</td>
</tr>
<tr>
<td>3</td>
<td>e-Prescribing</td>
</tr>
<tr>
<td>4</td>
<td>Mental and behavioral health</td>
</tr>
<tr>
<td>5</td>
<td>Health Information Exchange</td>
</tr>
<tr>
<td>6</td>
<td>Health Quality reporting</td>
</tr>
<tr>
<td>7</td>
<td>Policy, Procedure Mgt.</td>
</tr>
<tr>
<td>8</td>
<td>Medical Research</td>
</tr>
<tr>
<td>9</td>
<td>Payment Card Industry (PCI)</td>
</tr>
<tr>
<td>10</td>
<td>FTC Red Flags Rule</td>
</tr>
</tbody>
</table>
# Health Care Compliance and the Cloud

<table>
<thead>
<tr>
<th>Types of Audits</th>
<th>Performed By</th>
<th>Augmented By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems Reviews</td>
<td>Dept of Health and Human Services (CMS)</td>
<td>Audit tools and legal framework</td>
</tr>
<tr>
<td>Transaction Reviews</td>
<td>Independent Review Organizations</td>
<td>Internal audit processes</td>
</tr>
<tr>
<td>Policy and Procedure Reviews</td>
<td>States</td>
<td>Information technology</td>
</tr>
<tr>
<td>Risk Assessments</td>
<td>Federal Trade Commission</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Payment Card Industry (PCI)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Customers / Business Associates</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internal Audit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Food and Drug Administration (FDA)</td>
<td></td>
</tr>
</tbody>
</table>
Requires an interconnected strategy
ARE YOU CLOUD READY?

- Have you standardized most commonly repeated operating procedures?
- Have you fully automated deployment and management?
- Can you provide self-service access for users?
- Are your business units ready to share the same infrastructure?
MAJOR CLOUD COMPLIANCE ISSUES INCLUDE:

• Data ownership and control
  – Trust, consequences and chain of custody
  – Access and authentication

• Facilities and service provision
  – e.g. shared data centers / resources

• Administration
  – Policies, transparency, auditing
KEY CLOUD SECURITY CONCERNS

• Virtualization software (e.g., hypervisor) risk exposure

• Inability to determine location of data or processing

• Mobility among VM’s **contradicts** control principles; boundaries become unreliable and blurred

• Limited visibility into host O/S’s and virtual network (to find vulnerabilities and assess/report configuration, patching)
LEAD TO VERY GRANULAR ISSUES:

• Security policies need to shift "up the stack" to match logical attributes

• Network Access control and Intrusion Prevention

• Root kit Detection

• Inter VM traffic analysis
KEY CONSIDERATIONS

• Move away from physical attributes for meeting compliance

• Application, Identity and Content awareness
CORE RECOMMENDATIONS

• Think of information security as a set of adaptive services integrated with **compliance** requirements and **Information Architecture/Design**

• Get security vendors to deliver their security controls in a virtualized form

• Express security policy across physical, virtualized and private cloud-computing environments

• Maintain separation of duties between security policy enforcement and IT operations
Feisal Nanji, Executive Director
feisal@techumen.com