Cloud Computing in a HIPAA-Compliant World

NRTRC Telemedicine Conference
Dean Oswald
March 25, 2014
Agenda

- Cloud overview
- Infrastructure-as-Service overview
  - HIPAA-compliant IaaS
- Risk – cost – speed tradeoffs
- Responsibility matrix for HIPAA requirements
- New technologies
- Customer Examples
- Recap
Why is it called “the cloud”?

Originally network shorthand for: “Magic happens in here and we don’t know/care how it works.”
Evolution toward the cloud

- **Applications run on-premises**: You own the hardware and perform maintenance and operation of the data center.
- **Applications run in the IaaS Cloud**: You pay someone to run your applications on hardware to your specification.
- **Applications run in the Cloud**: You pay for computing capacity that can be used for your applications.
IT decisions balance conflicting goals

- Risk
  - Reliability
  - DR
  - Compliance
  - Security

- Cost
  - CapEx
  - OpEx
  - Staff

- Speed
  - Deployment
  - Upgrades
  - Scalability

- Features
  - Must Have
  - Nice to Have
  - Ease of Use
Cloud computing is like a miracle drug

- Faster deployment
- Automatic upgrades
- Huge scalability
- Reduces CapEx
- Lower & usage based OpEx
- Reduces staff
- Adequate features, growing
- Applications delivered via web browser
- Higher overall reliability
- Lower overall risk
- Faster deployment
- Automatic upgrades
- Huge scalability
- Higher overall reliability
- Lower overall risk

Risk

Features

Cost

Speed

easy-street
where business lives
Cloud computing service models

Traditional IT
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Infrastructure: IaaS
- Existing Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Platform: PaaS
- Develop New Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Software: SaaS
- Includes the Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking
What is Infrastructure-as-a-Service (IaaS)?
Infrastructure-as-a-Service benefits

An excellent option for healthcare organizations that are:

- Facing the expense of a technology or hardware refresh
- Ready to implement EMR and EHR solutions that require complex environments
- Short-staffed due to changing needs or loss of experienced IT professionals
- Desiring a Disaster Recovery environment outside their own region
- Concerned about ePHI security or other compliance issues (HIPAA-compliant providers)
- Seeking a more predictable cost structure
HIPAA-compliant IaaS

- Added requirements based on HIPAA and/or HITECH-Act regulations
- External auditor assesses organizational, administrative, physical and technical controls
- Validation of compliance with policies and procedures by review of logs, configuration, records and interview of personnel
- Evaluation and validation of architecture, including interviews of personnel responsible for design and implementation, for Technical Safeguards
- Validation of physical controls deployed in the environment
- Privacy Rule requires Business Associate agreement
A common control design assessment model

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Strong</td>
<td>Exhibits strong design in every respect. Control design weaknesses are minor.</td>
</tr>
<tr>
<td>2. Satisfactory</td>
<td>Exhibits safe and sound design but may demonstrate modest weaknesses, which can be corrected without major remediation.</td>
</tr>
<tr>
<td>3. Less than Satisfactory</td>
<td>Exhibits some degree of concern due to a combination of weaknesses that may range from moderate to severe</td>
</tr>
<tr>
<td>4. Deficient</td>
<td>Exhibits control design that would create an unsafe and unsound environment that may impair future viability of the entity.</td>
</tr>
<tr>
<td>5. Critically Deficient</td>
<td>Exhibit critically deficient control design and in need of immediate remedial action.</td>
</tr>
</tbody>
</table>
# Example requirements: Administrative Safeguards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Requirement</th>
<th>ES</th>
<th>Client</th>
<th>Both</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sanction Policy</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information System Activity Review</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workforce Security HIPAA 164.308(a)(3)(i)</td>
<td>Authorization and/or Supervision</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Workforce Clearance Procedures</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Termination Procedures</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Access Management HIPAA 164.308(a)(4)(i)</td>
<td>Isolating Healthcare Clearinghouse Function</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Access Authorization</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access Establishment and Modification</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Awareness and Training HIPAA 164.308(a)(5)(i)</td>
<td>Security Reminders</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protection from Malicious Software</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Log-in Monitoring</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Password Management</td>
<td>■</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Example requirements: Physical Security

<table>
<thead>
<tr>
<th>Standard</th>
<th>Requirement</th>
<th>ES</th>
<th>Client</th>
<th>Both</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility Access Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA 164.310(a)(1)</td>
<td>Contingency Operations</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Facility Security Plans</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access Control and Validation Procedures</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maintenance Records</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device and Media Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA 164.310(d)(1)</td>
<td>Disposal</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Media Re-use</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Accountability</td>
<td>■</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Backup and Storage</td>
<td>■</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Example requirements: Technical Safeguards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Requirement</th>
<th>ES</th>
<th>Client</th>
<th>Both</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Unique User Identification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA 164.312(a)(1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Emergency Access Procedure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automatic Logoff</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Encryption and Decryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td>Mechanism to Authenticate Electronic Protected Health Information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA 164.312(c)(1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmission Security</td>
<td>Integrity Controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA 164.312(e)(1)</td>
<td>Encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
RTO decision drives your options

- **COLD**: Days – Weeks
  - Backups
  - Management/Storage

- **WARM**: Hours – Days
  - Replication
  - Sync/Log Shipping
  - Backups

- **HOT**: Minutes
  - Everything Up/Sync
  - Professional Services
New technologies ease compliance

- SSD with flash storage
- Always on encryption
  - Meets data-at-rest requirement
  - Protects against drive theft or loss in transit or maintenance
  - A combination of software-based and ASIC-accelerated encryption for no performance loss
Customer example #1

- Oregon-based Hospital
  - Large skilled internal IT staff
  - Significant assets already in place
  - Hardware refresh provided opportunity to improve DR

- Solution
  - Primary infrastructure in EasyStreet colocation
  - 9-cabinet cage
  - Redundant/diverse connectivity
  - DR infrastructure located at hospital site
  - Data replication/DR playbook managed by hospital IT
Customer example #2

Arizona-based healthcare provider

- New “green-field” clinical information system
- Complicated modern application
- Extremely high availability/performance required

Solution

- HOT/HOT Disaster Recovery Solution (RPO 1 hour, RTO 4 hours)
- Identical dedicated private clouds in Beaverton and Phoenix
- Multiple replication techniques used
  - Database / storage / hypervisor based
- DR playbook jointly developed by customer and EasyStreet
Recap

— “The cloud” delivered as Infrastructure-as-a-Service is an excellent option for healthcare organizations

— Ensure you’re in compliance with your IaaS provider
  - Have them sign a Business Associate agreement
  - Request a Responsibility Matrix

— Your IaaS provider can help balance the risk/cost/speed or hot/warm/cold requirements that are right for your organization

— New technologies overcome risk/cost/speed limitations
  - Inline encrypted storage
Thank you!

- Call 503-671-1884
- Email gdoswald@easystreet.com