Healthcare Data in the Cloud – A Gathering Storm of Governance

Erik Pupo
Senior Manager, Deloitte
Objectives for this Webinar

• Explain what the healthcare cloud really means
• Highlight emerging challenges with using cloud computing in the healthcare industry
  – Focus specifically on challenges, best practices, and planning associated with data governance
• Look at the relationship of data governance and cloud computing and how to get it right
WHAT IS THE HEALTHCARE CLOUD?
Types of clouds

- **Cirrocumulus** (mackerel sky) above 18,000 feet
- **Cirrus** above 18,000 feet
- **Altocumulus** 6,000 to 20,000 feet
- **Altostratus** 6,000-20,000 feet
- **Stratocumulus** below 6,000 feet
- **Stratus** below 6,000 feet
- **Cumulus**
- **Cumulonimbus** from near the ground to above 50,000 feet
Types of clouds

- **Software as a Service (SaaS)**
  - "Consume the Cloud"
  - Applications designed for end-users delivered over the web
  - Examples – Salesforce, Workday, Concur

- **Platform as a Service (PaaS)**
  - "Leverage the Cloud"
  - A set of tools and services designed to make coding and deploying those applications quick and efficient
  - Examples – Force.com, Google App Engine

- **Infrastructure as a Service (IaaS)**
  - "Be a Cloud"
  - The hardware and software that powers it all – servers, storage, networks, operating systems
  - Examples – Amazon Web Services, Azure, Rackspace
Enterprise cloud application revenues reached $22.9B in 2011 and are projected to reach $67.3B by 2016.

60% of server workloads will be virtualized by 2014.

Global cloud traffic will account for nearly two-thirds of total data center traffic by 2016.

Today 46% of business data stored outside of internal IT structures.

Over the past three years nearly 74% of data centers increased physical server count.

IaaS cloud management & security and PaaS are growing from $7.6B in 2011 to $35.5B in 2016.

1. Need to avoid or reduce risk
2. Need for cost efficiencies
3. Need for business agility

Projected Market Spend of $241 Billion by 2020

Business Drivers for Healthcare Cloud Computing

Private

Hybrid

Public

39%

37%

24%
Trickiness of Cloud Data

- Balance between user needs and governance
  - Because the cloud can be outside the physical location of the entity, how can governance be applied?
- Determining what data needs to be in the cloud versus what resources should remain in house
What happens when it goes all wrong?

Meenakshi Budhraja
@gastromom

Sobering not to have had access to my practice for the last two days
@PracticeFusion
Thank god for paper charts
WHAT DOES GOVERNANCE HAVE TO DO WITH THE CLOUD?
Good uses of the healthcare cloud

- **Web-based EHR**
  - Providers can save money and not have to worry about consultants or maintenance

- **Cloud Analytics**
  - Providers face increasing pressure to both report and mine clinical data to identify ways to improve patient care, comply with federal regulations and manage costs

- **Cloud Imaging**
  - The explosive growth of digital image usage requires hospitals to invest in infrastructure to store, manage, and share radiology and other images.
Where does the healthcare cloud work well?

- When processes, data and applications are largely independent
- When points of integration are well defined
- When lower levels of security are allowed
- When the web is desired
- When cost is an issue
- When applications are new
- When the core architecture is healthy
Q: Rate the **challenges/issues** of the 'cloud'/on-demand model

(Scale: 1 = Not at all concerned  5 = Very concerned)

- Security: 87.5%
- Availability: 83.3%
- Performance: 82.9%
- On-demand paym’t model may cost more: 81.0%
- Lack of interoperability standards: 80.2%
- Bringing back in-house may be difficult: 79.8%
- Hard to integrate with in-house IT: 76.8%
- Not enough ability to customize: 76.0%

Source: IDC Enterprise Panel, 3Q09, n = 263
Lack of Governance in the Cloud or On-Site

• Who is Data Governance for?
  – Anybody that Defines, Produces and Uses Data
  – Anybody Who Must Support Data Governance in Order for it to be Successful
  – Anybody Who is Supported by or Supports These People
  – Anybody that Sees Room for Improvement Associated with Data
  – Anybody Who is Feeling the Pain of Having Crummy Data
Data Governance Options and Cost

Cost Build Up - Traditional Applications

Cost Buildup - SaaS Applications
WHAT ARE CHALLENGES TO DATA GOVERNANCE IN THE HEALTHCARE CLOUD?
Challenge – Rationalizing Data

Refine
The results are put back into the database to further refine treatments for other patients diagnosed with Neuroblastoma

Diagnose & collect
Tumor sample is taken by the oncologist and added to genome

Cloud technology
Computation & collaboration

Treat
Doctors are able to administer treatment to the patient

Analyze & store
Molecular characterization of the tumor creates a disease signature specific to the patient

Access & compute
The results are saved to the cloud so doctors can quickly access information

Map & match
Tumor is mapped to treatment database to determine targeted drug therapy

8.2 Teraflops
1,200% increase in computing power
Dell Precision workstations
Competent Storage Center Arrays
PowerEdge Blade Servers
PowerVault Storage Arrays
Force10 network infrastructure
Dell technical expertise, knowledge

8.2 Teraflops
1,200% increase in computing power
Dell Precision workstations
Competent Storage Center Arrays
PowerEdge Blade Servers
PowerVault Storage Arrays
Force10 network infrastructure
Dell technical expertise, knowledge
Geographic Governance of Data

• Storing data in cloud infrastructures that are often spread across different locations with different standards for data governance and security
  – Example – Multi-state HIE
  – Example – State with strong privacy controls vs state with weaker privacy controls

• Understanding the patient data that should be stored in the cloud vs. stored locally
Challenge – Location of Cloud Components and Data

• Importance of understanding the number of components, as well as complexity of those components
  – Location
  – Dependency
  – Ability to monitor
  – Ability to secure
The three greatest risks in the cloud:

- Confidentiality
  - Bridging the gap between on-premise security controls and off-premise security controls

- Availability
  - Responsibility ambiguity
  - Isolation failure

- Integrity
  - Some cloud providers may not offer the ability to audit data
Risk - Cloud Security Controls

**Deterrent**
Set in place to prevent any purposeful attack on a cloud system. Much like a warning sign on a fence or property, these controls do not reduce the vulnerability of the system.

**Preventative**
Upgrade the strength of the system by managing and safeguarding vulnerabilities. They cover the attack and reduce the damage and violation when an attack occurs.

**Corrective**
Used to reduce the effect of an attack. Take action as an attack is occurring.

**Detective**
Used to detect any attacks that may be occurring in the system. In the event of an attack, the detective control will signal the preventative or corrective controls.
Challenge – Dealing with Legal Consequences

Due to lack of trust between cloud ecosystems, legal ramifications are enhanced:

- HIPAA
- State Identity Theft
- Destruction of Records
- Cross-Border Data Agreements
- PCI Rules
- Electronic Discovery
CONCLUSIONS AND LESSONS LEARNED
What makes good governance in the cloud?

– Implement policies that calculate and quantify cloud risk
– Quantify and understand your risk tolerance
– Determine your data security fit
– Understand Data Protection and SLA requirements
– Establish Business to Business policies
– Quantify Private Data Exposure
– Assess Data Tampering processes
– Establish a Business Continuity Plan
What might be included in a cloud governance framework?

- **Policy Enforcement**
  - Master Security Policy and Exceptions
  - Risk Impact Criteria
  - Data Class Criteria
  - Hosting Criteria
  - Monitoring Criteria
  - Privacy Criteria
  - Application of Security Standards
- **Certification and Compliance Policy**
Best Practices

• Get everything down on paper
  – Some terms are incorporated by reference
  – Some terms are changeable without notice by vendor

• Understand where data is located and how it is disposed of

• Have a backup governance plan

• Ensure service level agreements are incorporated into governance
  – How is service measured?
  – What are reporting obligations?
Lessons Learned from Data Governance in the Cloud

• Source data rationalization and cleansing
  – Ability to rationalize data and make it presentable to and from the cloud environment

• Encryption of data
  – Encryption of data at rest and among multiple locations in the cloud

• Identity and access management
  – Configuring cloud access
  – Most cloud providers do not have strong auditing features

• Locations of PII
  – Physical location of where PII is stored