Health Care Data in the Cloud:
Strategies for Contracting With Cloud Providers

Wednesday, January 16, 2013

FOLEY

FOLEY & LARDNER LLP

12.9135

Housekeeping Tips

- Live questions will be taken at the end of the program and questions can also be asked during the program by clicking on the Q&A tab above.
- Your feedback is greatly appreciated, so we ask that you take a few minutes and complete the survey that will appear on your screen after the Q&A session.
- Foley will apply for 1 general CLE credits for today's program. Please allow up to 14 weeks for processing your credits.
- CLE for New York: If you are seeking CLE Credit for New York, please listen for **one course code** that will be announced during the web conference. Please write down the code and then request an Attorney Affirmation form by contacting zrahim@foley.com. This form will need to be completed with the course code in order to receive your credit for the state of New York.

12.8453

Speakers

Moderator:

Michael Scarano
Partner
Foley & Lardner LLP
mscarano@foley.com

Presenters:

Matthew Karlyn
Partner
Foley & Lardner LLP
mkarlyn@foley.com

Daniel Orenstein
General Counsel
Athenahealth, Inc.
dorenstein@athenahealth.com

Leeann Habte
Associate
Foley & Lardner LLP
lhabte@foley.com

Health Information Technology's Migration to the Cloud

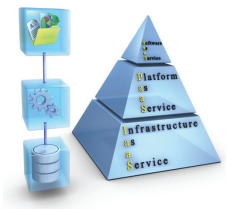
- **Current Use**
  - 30 percent of health care organizations report using cloud technology for clinical and non-clinical applications, according to a CDW tracking poll
    - Electronic Health Records (EHR)
    - Radiology images
    - Telemedicine
    - Patient management
    - Revenue cycle management and/or claims management
- **Projected Use**
  - 71 percent of health care organizations are either deploying or plan to deploy cloud technology, according to a survey by KLAS Research
  - Worldwide cloud services revenue is projected to reach $148.8 billion in 2014, according to a Gartner study

Definitions of Cloud Computing

- **Characteristics**
  - Delivery over the Internet (*i.e.*, the "cloud")
  - Software, platform or infrastructure resources provided as services
  - Scalability on-demand
  - Utility and/or subscription billing (*i.e.*, based on the Customer's actual use and/or a period of time)

Types of Cloud Computing Services

- **Software-as-a-Service (SaaS)** → refers to the Provider's software being delivered over the cloud to the Customer as a service (*e.g.*, electronic health record systems)
- **Platform-as-a-Service (PaaS)** → refers to the Provider's software development platforms being delivered over the cloud to the Customer as a service (*e.g.*, interface development)
- **Infrastructure-as-a-Service (IaaS)** → refers to virtual servers, memory, processors, storage, network bandwidth, and other types of infrastructure resources, delivered over the cloud to the Customer as a service (e.g., data hosting)



Benefits of Cloud Technology

- Reduction in Capital Costs
- Enhanced Computing Power
- Greater Flexibility
- Lower Upfront Risks and Complexity
- Availability of In-house Expertise

Part 2 – Speaking of Contracts…

- Cloud computing agreements have *some* similarity to licensing agreements, but have more in common with hosting or ASP agreements

Licensing vs. the Cloud

- **Traditional Licensing/Hardware Purchase**
  - Vendor installs the software or equipment in the Customer's environment
  - Customer has ability to have the software or hardware configured to meet its needs
  - Customer retains control of the data
- **In the Cloud…**
  - Software, hardware and Customer data are hosted by the Provider typically in a shared environment (e.g., many customers per server)
  - Software and hardware configuration much more homogeneous across all customers

Licensing vs. the Cloud (cont'd)

- **Shift of Top Priorities**
  - From configuration, implementation and acceptance (in the licensing world) to service availability, performance, service levels, data security and control (in the cloud)
- **Focus Should be on:**
  - The criticality of the software, data and services to the enterprise
  - The unique issues presented by a cloud computing environment
  - The service levels and pricing offered by different suppliers and for different services
- **Outsourcing agreements and traditional licensing agreements are a good starting point, but not a good ending point**

The paradigm shift to cloud contracting can be challenging . . .

Key Contractual Issues

- Service Availability
- Service Levels
- Data Privacy/Security
- Implementation

A Cloud-Based EHR System May Have Some Advantages With Regard to Availability

- **Factors that may lead to enhanced availability:**
  - Platform Strength: A more uniform computing platform structure, which can facilitate better management of security protocols such as configuration control, vulnerability testing, security audits, and patches. Security-protective standards apply to certain entities, such as HIPAA, Payment Card Industries (PCI) standards, SOC1 and SOC2 (SSAE-16), Sarbanes-Oxley
  - Back up and Recovery – Diverse geographies are available. Offsite backup is more readily supported.
  - Data Concentration – Having the data centralized can be an advantage with a distributed workforce, because there is more assurance of data integrity and availability when data is centralized
  - Disaster recovery at scale–Built-in redundancy and disaster recovery when executed on a large scale can enhance availability for a majority of customers

Service Availability

- **What Do You Need?**
  - If Provider is maintaining Protected Health Information (PHI), a disaster recovery plan and an emergency mode operation plan
  - Application of the terms of the agreement to the Provider's disaster recovery site
  - Provider's agreement not to withhold services
  - Protections Against Provider's Financial Instability
    - Quarterly reporting to allow Customer to assess the overall strength and financial viability of Provider
    - Ability to terminate the Agreement if the Customer concludes the Provider does not have the financial wherewithal to fully perform as required
    - In-house software solution: consider requiring the Provider to make available or develop an in-house solution to replacing software services if it stops providing those services

Service Levels

- **Uptime Service Level**
  - Services must be available to Customer at all times to support operations (99% of the time)
    - Outage window
    - Measurement period
    - Remedies
    - Require Provider to monitor servers by automatic pinging
    - "Unavailability" should include severe performance degradation
    - Service Response Time
      - Average download time for each page of the Services
      - Simultaneous visitors
      - Problem response time and resolution time
      - Data return and periodic delivery
      - Remedies for failure to meet service levels

Data Security

- **Business Associate Agreements/Contracts**
  - BAA (or contract) should address the Provider's policies and procedures related to:
    - Location of data
    - Security policies unique to cloud
    - Subcontracting arrangements
    - Breach notification
    - Data ownership and use rights
    - Data conversion/data return

Pre-Agreement Due Diligence

- **Can the Provider Meet your Organization's Expectations?**
  - Require Provider to complete a due diligence questionnaire, with particular attention to:
    - Provider's financial condition and corporate responsibility
    - Location of the data, including disaster recovery facilities
    - Provider's use of subcontractors and contractual relationships
    - Provider's security infrastructure and policies and procedures

Conduct your Security Diligence on a Potential Cloud-Based EHR Vendor for Security Readiness

- **What should you look for in diligence?**
  - Security diligence of a cloud-based vendor is essentially the same as the diligence you would conduct on a standard EHR vendor. The same security requirements apply (including the HIPAA Security Rule)
    - Ask questions such as whether the vendor has conducted a HIPAA Security Risk Assessment
    - Ask if the vendor has a statement of security measures it would be willing to share with you
    - If you have specific concerns, ask to speak to the vendor's Chief Information Security Officer, or other individual with responsibility over security
    - Ask about the vendor's disaster recovery and business continuity programs. Understand the recovery time, and recovery points, as well as how comprehensive the program is

Location of Data

- **Why is it important?**
  - May determine the jurisdiction and the governing law
    - Overseas data may impose additional compliance requirements or may limit ability to enforce data privacy and security compliance
    - State laws may impose compliance requirements in addition to those in the state of origin
    - Contractual agreements or state laws may restrict or prohibit offshore arrangements
  - Should consider inclusion of prohibition on off-shore work, or, at minimum, prohibition on storage of data offshore and restrictions on data transfer without prior written consent of Customer

Offshore Data Processing is Very Common, But Rights and Obligations Could be More Clear

- **What does the health care provider want?**
  - Efficiency and reduction in waste will often ultimately lead to off-shoring
  - Patients' interests can be protected if appropriate diligence is conducted and protections obtained
- **What are the major issues?**
  - It can be harder to hold organizations accountable
  - Data privacy laws might not be as protective abroad
  - It can be more difficult to review the security practices of organizations abroad

Offshore Data Processing is Very Common, But Rights and Obligations Could be More Clear (cont'd)

- **Business process outsourcing (BPO)**
  - Ensure that any BPO partner agrees to a business associate agreement or downstream HIPAA assurances
  - Get comfortable with the security profile of the BPO
    - Certifications and frameworks: e.g., ISO 270001, COSO, NIST
- **Private limitations on off-shoring**
  - Third party data and license sources may restrict use of data or licenses abroad
- **State-imposed limitations on off-shoring**
  - These are very rare
  - May be unconstitutional under US treaties, General Agreement on Trade in Services

Data Security Compliance

- **Security Provisions**
  - Agree to provide third party audit to verify compliance
  - Allow Covered Entity access to facilities to determine HIPAA compliance
  - Define Customer's vs. Provider's responsibilities for security
  - Ensure security policy adequately addresses cloud-specific risks
    - Technical risks
    - Workforce access
    - Review of audit trails

Audit Provisions: Some Practical Considerations

- **Audits: Are they better in theory than in practice?**
  - Lawyers love audit provisions, but will your client organization *really* conduct regular audits?
    - Organizations are typically busy keeping their own houses in order, without the added burden of auditing an external organization
  - Is there a viable substitute available, such as a SOC1 or SOC2 opinion, or the result of a HITRUST audit?
    - These may provide the assurance needed with accompanying evidence of good security practices, without the burden of conducting an audit
  - Is it reasonable to expect that a large service organization will subject itself to multiple additional external audits from customers?
    - The organization is also busy keeping its own house in order, and typically already deals with multiple external audits (SOX or accounting audits, SSAE-16, security audits, tax audits)

Subcontracting Arrangements

- **Subcontracting Arrangements**
  - HIPAA compliance required if PHI is involved (45 C.F.R. § 164.504(e)(ii)(D))
  - Protections if third party is operating data center
    - Ensure third party host complies with key terms of agreement with Provider
    - Advance notice of any change of the host
    - Joint and several liability of the cloud provider with the third party host for any breach of the agreement by the third party host
    - Consider entering a separate confidentiality agreement with the third party host

Breach Notification

- **Breach Notification Provisions**
  - BAA and Contract should establish:
    - The procedures and timeframe for reporting a breach to the Customer
    - The procedures and role of the parties with respect to investigation of the breach and notification of individuals
    - Access to records of investigation
    - Liability of the Provider
    - If subject to HIPAA, must comply with 45 C.F.R. § 164 Subpart D

Breach Notification (cont'd)

- **Breach Notification Provisions**
  - Customer should have sole control over the timing, content, and method of notification (if it is required)
  - If the Provider is responsible for the breach, then the Provider should reimburse the Customer for its reasonable out-of-pocket expenses in providing the notification, mitigating the harm, and otherwise complying with the law
  - Indemnification is key issue, subject to negotiation between the parties

Who Does the Work in the Event of a Data Breach?

- **Whose "system" did the breach occur on anyway?**
  - The health care provider has selected and is using the vendor's electronic data system as their own system
  - But the breach might have literally occurred as a proximate result of the actions of the vendor
- **The party who has more insight into, and control over, the events that led to the breach may want to take a lead role in the response**
  - Define how coordination of efforts will work
  - Address the challenges posed by multiple states', federal requirements
  - When an issue arises, trust and coordination between the provider and vendor are probably as important, or more important, than what the contract says

Data Ownership and Use Rights

- **Agreement should include:**
  - Clear language regarding Customer's ownership of data
  - Specific language (i) regarding the Provider's obligations to maintain the confidentiality of such information and (ii) placing appropriate limitations on the Provider's use of such Customer information
  - Strict limitations on Provider's use of data in aggregated and/or de-identified form
    - Use of aggregate data must be for health care operations purpose permissible under HIPAA
  - May require indemnification in event that PHI is not properly de-identified

Data Conversion/Return

- **Data Conversion/Return of Data**
  - Should ensure that the Customer is not "locked in" to the Provider's solution and Provider can return or destroy data at termination of agreement
  - Establish format for return of data at no cost to Customer
  - Require Provider to completely destroy or erase all other copies of the Customer Information
  - Require certification of destruction of data

Consider Whether Data Usage Rights vs. Data Ownership is More Appropriate

- **Take a hard look at whether anyone truly "owns" the data**
  - Payor-generated content
  - Provider-generated content
  - Patient generated content
  - Medical records laws
    - Ownership vs. Custodianship
  - De-identified information
- **The contract should give the parties the appropriate rights to use and disclose health information to fulfill their obligations, and should address what happens after the contract term**
  - Return of data
  - Time period to maintain data
  - Transfer to subsequent EHR system

Implementations of Cloud-based Systems Often Differ Significantly From Software Implementations

- **There may be fewer differences if it is pure *platform as a service***
  - The customer may be running their enterprise software using a third party platform, with typical software implementation considerations
- **. . . But if it is software as a service, or cloud enabled service:**
  - Authorization may replace acceptance
  - Implementation cycles and upgrade/update cycles should be more rapid and require less customer involvement
- **If it is a standardized service (such as SAAS or cloud-enabled service), not customized development, the focus is more on "results" rather than "functionality"**
  - E.g., how will the provider accomplish MU compliance, maintain EHR certification, achieve ICD-10, ANSI 5010 compliance

Health Care Data in the Cloud: Strategies for Contracting with Cloud Providers

- Contact Information:

Matthew A. Karlyn
Foley & Lardner LLP
111 Huntington Ave., Ste. 2500
Boston, MA 02199
Tel: (617) 342-4000
email: mkarlyn@foley.com

M. Leeann Habte
Foley & Lardner LLP
111 Huntington Ave., Ste. 2500
Boston, MA 02199
Tel: (213) 972-4679
email: lhabte@foley.com

Daniel Orenstein
General Counsel
Athenahealth, Inc.
Watertown, MA
Tel: (617) 402-1397
email: dorsenstein@athenahealthcom

Moderator:
R. Michael Scarano, Jr.
Foley & Lardner LLP
111 Huntington Ave., Ste. 2500
Boston, MA 02199
Tel: (858) 847-6712
email: mscarno@foley.com