Cloud Computing Contracts
Top Issues for Healthcare Providers

North Carolina Bar Association
Health Law Section
Annual Meeting

NC Bar Center
Cary, North Carolina

April 23, 2015

Presenters

Kathryn Brucks, Director, Information Security, Lexington Medical Center, West Columbia, SC

Stephen R. Hunting, Parker Poe Adams & Bernstein LLP, Charlotte, NC

Table of Contents

Page

Attached Example

Service Level Agreement

1. Summary

An increasing number of hospitals and other health care providers are outsourcing the hosting and maintenance of software applications, the storage of data and related support services. Outsourcing can provide cost savings, rapid deployment, system scalability, other efficiencies and appropriate data security. It also introduces additional issues into the provider's risk management analysis, largely based on the fact that a third party rather than the provider has possession and control of vital and sensitive assets and information. This paper identifies top issues for a provider to address in deciding whether to outsource a particular application and on what terms and conditions it will do so.

2. Overview

No business decision or activity is risk free. As a result, this paper addresses risk management, not risk elimination. Risk management is a balancing process based on the particular facts and circumstances. For example, a provider may be less concerned about its inability to access and use productively for a day or two its web-based job application submission portal than its electronic health record application. Not all risks are the same, and a provider will likely devote more attention and resources to managing its greatest risks.

Risk management is a team sport. Effective risk management requires the participation and interaction of representatives of the intended user group, financial analysts, compliance officers, information technology and data security experts, and legal counsel experienced in advising on and negotiating the particular type of contract.

The final form of the contract will not be perfect. Almost always, the parties start the negotiation process with the vendor's "standard" contract. Almost always, it is a one-sided document designed to protect the vendor's interests vigorously. The key is to determine on what issues to focus in light of the particular facts and circumstances, including the reputation and financial strength of the vendor, the results of the provider's inquiries to other users of the software or service and other due diligence, the importance of the application and the impact of its unavailability or failure to perform properly or effectively, and the provider's ability to transition to another vendor or solution quickly if necessary.

Start early. A provider will be in a much better position to manage its risks if it discusses key risk management and contract issues with the potential vendors for a project up front in the RFP stage. This lets each vendor know what is important to its potential customer and that its inability to meet its potential customer's needs may result in its loss of the business. Reviewing the vendor's form contract for the first time when you have completed the selection process and are under pressure to sign and start work on the project unnecessarily reduces the effectiveness of your risk management process and gives additional leverage to the vendor.

Have a plan. Before you start your next outsourcing project, develop a checklist of items that are important to you, including due diligence items you will want to review and provisions you will want any contract to include. Customize your checklist for the particular project. Then include the checklist in your RFP or other early investigation document and ask each potential vendor to respond to it. You will have greater leverage in this early stage of the sales cycle.

3. Cloud

All Clouds Are Not The Same

The following National Institute of Standards and Technology ("**NIST**") publication provides some definitions and an overview of cloud computing models:

NIST Definition of Cloud Computing
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

The most common model healthcare providers use, and the one on which this paper focuses, is the software as a service (SaaS) model. This involves the software the healthcare provider uses, and the provider's data being located on, computer servers owned and operated by one or more third parties.

Other helpful resources include:

NIST Guidelines on Security and Privacy in Public Cloud Computing (800-144)
http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

ISACA, Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives, 2009
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-Governance-and-Assurance-Perspective.aspx

ISACA, Guiding Principles for Cloud Computing Adoption and Use, 2012
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Guiding-Principles-for-Cloud-Computing-Adoption-and-Use.aspx

Private, Community or Public Cloud?

A provider should know how its data will be stored by the cloud service provider. Will the data stored on a separate computer server (an isolated instance) or will it be intermingled with the data of others on the same server (multi-tenancy or resource pooling)? Many cloud databases are created under a single instance, meaning that each provider's data is comingled and is simply tagged with a subscriber identifier. A small error in this tagging could result in your data being exposed to unauthorized persons.

4. Use

Many cloud service agreements will limit those who may access and use the software to employees of the healthcare provider which is a party to the contract. Those agreements typically allow those permitted users to access and use the software solely for the benefit of that contract party. The provider should consider expanding the latter group to include affiliates of the provider and expanding permitted users to include employees and independent contractors and consultants of the provider and its affiliates.

5. Security

Control Assurances

Consider requiring the vendor to provide appropriate third party assessments of the design and implementation of the vendor's application and network security protocols. The principal third party assessments are Service Organization Control (SOC) reports pursuant to Statement on Standards for Attestation Engagements 16 published by the Auditing Standards Board of the American Institute of Certified Public Accountants (SSAE 16). *See* http://ssae16.com/SSAE16_reports.html. In general, a Type I report involves a review of the vendor's designs but not its actual systems, and a Type II report includes detailed testing of those systems. Many reputable cloud service providers maintain current independent assessments and will provide a copy on request.

Among the items these assessments should include are confirmation that the vendor is complying with appropriate security requirements. Those include personnel screening for clearances and responsibilities, well documented policies and procedures that are being followed, regular security awareness training for personnel, appropriate physical and logical access controls for all facilities, and best practices for network configuration and software patch management that the vendor follows.

If the initial assessment is satisfactory and you decide to enter into a contract with the vendor, consider having the contract require the vendor to provide a similar assessment annually (or more frequently) during the contract term. The contract should state that if the vendor fails to provide a satisfactory assessment, it will be in breach of the contract, and the provider will be entitled to terminate the contract or to exercise other remedies.

Data Encryption

Encryption is becoming a de facto control in any organization's security program. Organizations need to obtain contract assurances from the cloud services vendor that all data will be encrypted in transit and at rest, including data residing on backup media, and that the vendor will continue to adhere to industry best practices as they evolve. The vendor should also have in place a solid encryption key management program to prevent the compromise of those keys stores and the data the encryption protects. Once you determine with the vendor what the initial and ongoing requirements will be, include them in the contract.

6. Privacy

Confidentiality

The contract should provide that the vendor will keep all of the provider's data strictly confidential and that the vendor may only use that data as necessary to provide the contracted services to the provider.

Big Data

The confidentiality limitations in the contract should expressly apply to de-identified and aggregated data, unless you agree to the contrary in the contract. This is the Big Data era, and every vendor seeks the right to use your data, now and in the future, for some economic gain. While HIPAA may allow the vendor to use certain de-identified and other data, the provider may not want to allow that use or may want to limit it. For more information on de-identification, *see* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html.

If the provider considers allowing the vendor to make independent use of de-identified or other data, possibly for reduced fees or other compensation, the provider should restrict that use in a number of ways. The contract should require (a) that the provider not be identified as one whose data is included in the aggregated database and (b) that the database include data from a minimum number of sources from geographically diverse locations. The provider should also consider the potential for the use by unauthorized persons of data re-identification techniques. For a description of the process of re-identification, *see* https://epic.org/privacy/reidentification/#process.

Transition

The contract should document the cloud service vendor's obligations upon contract termination, such as its obligations to return all data in a mutually agreeable format and to destroy all copies of the provider's data on its systems and those of its subcontractors. There are a number of data destruction standards that the contract could specify. For more information on data destruction standards, *see* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

The healthcare provider should also revoke all physical and electronic access rights it granted the vendor and discontinue all VPN tunnels that may be in place.

Equipment Replacement

The vendor's obligation to destroy data should also apply when the vendor replaces or reassigns equipment on which the provider's data is stored.

7. Functions

Documentation and Specifications

Deciding to access a software application through the internet rather than installing it on a server in your building does not change the need (a) to satisfy yourself that the software has sufficient functions to meet your needs and (b) to make sure the vendor's assurances about the functions the software has are stated in the contract. A typical provision in the cloud services agreement and the associated service level agreement states that the software will perform all of the

functions described in the vendor's user and technical manuals or other publications. It is important to follow through and review the referenced manuals and publications to ensure they contain full and clear descriptions of the functions the software will perform. In some cases, you may want expand that provision to include functions on an additional list you prepare.

E-Discovery and Audit Compliance

The provider should ensure the vendor's software and services support the provider's obligations to answer discovery requests in litigation and to comply with its access control and audit obligations under the HIPAA Security Rule. You should be satisfied you will be able to collect and to preserve the data you need. For more information on the HIPAA Security Rule, *see* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule.

8. Availability

A provider should ensure the contract contains a well written service level agreement ("**SLA**") that addresses, among other things:

- uptime guarantees;
- support services and error escalation; and
- internet bandwidth.

The SLA should establish up-time guarantees with financial consequences for the vendor's failure to comply. An uptime guaranty of 99.999% is industry standard for core and critical systems.

The definitions and other fine print in the SLA matter. For example:

- An uptime of 99% equates to 87.6 hours of downtime in a year. Can your business sustain that many hours of outages, particularly if they occur during peak periods of use?
- What periods of time are excluded from the definition of "available?" If unscheduled maintenance time or unlimited amounts of scheduled maintenance are excluded from the downtime calculation, an uptime guaranty of 99.999% may not be as good as it looks.
- Over what period of time is the uptime percentage calculated? If it is calculated over a particularly long period of time like a calendar quarter or a six-month period, multiple days or weeks in which the vendor fails to meet the uptime guaranty may be averaged out, resulting in no remedy for the provider.
- What constitutes downtime? If nothing but complete system unavailability counts as downtime, the vendor will be entitled to count as uptime periods during which material portions of the system are unavailable or not operating within the specifications.
- Who is responsible for tracking and reporting uptime percentages? Many times the contract states this falls to the provider. Consider making this one of the services the vendor provides.
- Are the vendor's scheduled maintenance windows satisfactory for your peak hours of operation? Double check the time zone the vendor is using.

The healthcare provider should understand the impact of intermediate services like those of an internet service provider ("**ISP**"). If the transmission of your data is dependent upon a specific ISP, you should determine if the ISP has sufficient infrastructure to support your bandwidth requirements.

9. Performance

In addition to availability, you may want the SLA to address performance, the speed with which the system will perform tasks. Work with the vendor to identify toolsets to measure system performance and to specify mutually acceptable minimum performance standards.

Identify all points of potential bottlenecks. For example, does all of the traffic run through a single Internet Service Provider? Or, as is preferable, are there multiple paths?

10. Location

Regulations and other legal requirements vary between countries. If a provider's data is stored on a server in another country, the provider could be subject to additional or different legal requirements and to the jurisdiction of courts in that country. A provider should consider establishing in the contract limitations on where its data may be stored and processed. Also, a provider should determine whether the vendor will use a third party data center to store or process its data. If it will, the provider should seek to obtain similar assurances from the operator of that data center.

11. Services

Help Desk and Error Response

The vendor's SLA should include support services that complement the provider's work environment. The SLA should address the vendor's support processes, toolsets and help desk hours of operation. The vendor's processes should also specify a call escalation process and an error classification scheme.

An SLA typically classifies errors into three categories (critical, causing problems but working around them, and it can wait until you get to it). Each category has a specified time within which the vendor must respond initially. That period of time is shorter for a critical, or level 1, error. Each category also has a standard for the vendor's efforts to fix the error. For example, a vendor might be required to work 24/7/365 to fix a critical error and only during normal business hours to fix an error in the lowest category.

The vendor should not have the sole discretion to classify errors. The SLA should define the categories with sufficient details to make disagreements over classification less likely.

Incident Reporting, Handling, and Response

A Business Associate Agreement (BAA) normally addresses the vendor's obligation to report to the healthcare provider incidents involving data breaches and unauthorized access of the

provider's data. The BAA will also usually state that the healthcare provider will be the one to make any required reports under HIPAA or other laws.

The provisions of the BAA should be coordinated with the cloud services contract, which may go further and require the vendor to report breaches of, and significant attacks on, its network, even if they do not actually result in the provider's data being compromised. These provisions should define clearly the relevant reporting events (data breach versus security alerts, date of discovery, etc.) and should address the vendor's responsibilities in each case, including the period of time after discovery within which the vendor must give the provider written notice.

The cloud services vendor should have an incident response plan that limits resulting damage and reduces its response time and costs. The plan should outline key incident response activities for incident containment, preservation of system logs, remediation, and system restoration. The contract should describe a prearranged communication path between the vendor and the provider for reporting and responding to data breaches.

Set Up

If the contract involves the vendor's providing configuration or other set up assistance, the contract should describe those services in some detail. The contract should also include a schedule of when the vendor will provide those services and what related responsibilities the provider has. Consider tying some compensation to the completion of milestones.

Training

If the vendor is required to provide training, the specific training, the number of people from the provider who will be trained, and the location of the training should all be specified in the contract.

Data Migration

Consider whether you will want the proposed vendor to be responsible for migrating your data from a current system to the new one and for verifying that the transfer occurred successfully.

12. Continuity

Data Backup and Disaster Recovery

The cloud services contract should specify how, and how frequently, the vendor will back up the provider's data and test the backups. The backed up data should be stored in a separate but equally secure facility that is required to comply with the same requirements as the primary data center. The vendor's disaster recovery plan should describe how, and how quickly, the vendor will restore full service.

Cloud Services Provider Failure

The healthcare provider should consider how it would respond to a failure of the cloud services vendor. Such an event might be more of a possibility with a startup or small vendor. There are a number of companies that offer business continuity services for subscribers. These arrangements, like the source code escrow arrangements that are sometimes used for licensed software, should be evaluated and consummated in connection with entering into the initial cloud services agreement.

13. Remedies

Damage Limitations

Every cloud services contract a vendor proposes will include broad limitations on the total amount of damages a subscriber can recover and an exclusion of consequential and other categories of damages. These clauses often state that these limitations apply regardless of the theory of recovery.

A provider should consider at least the following carve outs from broad damage limitations. In each case, these damages would be unrelated to, and not fairly limited by, the fees the provider has paid the vendor over any period of time or any other blanket limitation.

- Damages the provider suffers as a result of the vendor's breach of its confidentiality obligations.
- Damages the provider suffers as a result of the fraud or criminal conduct of the vendor, its subcontractors or their respective employees.
- The provider's obligations under any intellectual property infringement indemnity in the contract.

Indemnification

A provider should seek an intellectual property infringement indemnity from the cloud services vendor. The vendor will certainly be a defendant in any suit brought against the healthcare provider. Additionally, the vendor will have an incentive to defend its services and to be able to continue to provide them in an uninterrupted fashion.

SLA

If the vendor does not comply with the availability or performance requirements in the SLA, the provider should ask the vendor to provide credits which the provider can use against future amounts due for the services. If the vendor fails to comply with the requirements too frequently, the subscriber sometimes has a right to terminate the service without penalty.

Example Service Level Agreement

1. **Software Maintenance Services**

   a. Licensor shall maintain the Software and the Documentation in good working order and in compliance with this SLA. Licensor shall correct all errors, problems, interruptions, malfunctions and failures in the Software (collectively, "**Errors**") in compliance with the Agreement and this SLA. Capitalized terms used in this SLA shall have the meanings subscribed to them in the Agreement to which this SLA is an Exhibit.

   b. Licensor shall provide to Licensee and the Affiliates, at the same time it makes them available to other users of the Software, all improvements, enhancements or updates to, and all new releases and new versions of, the Software, including an electronic copy of the accompanying Documentation.

   c. Licensor shall perform all Software scheduled maintenance during the following maintenance windows ("**Maintenance Windows**") and not during other times:

Day of Week	**Start Time (Eastern Time Zone)**	**End Time (Eastern Time Zone)**
Monday	12:01 am	5:00 am
Tuesday	12:01 am	5:00 am
Wednesday	12:01 am	5:00 am
Thursday	12:01 am	5:00 am
Friday	12:01 am	5:00 am
Saturday	12:01 am	5:00 am
Sunday	12:01 pm	8:00 am

2. **Support Services**

   a. **Help Desk**. Licensor shall provide support services in accordance with the Agreement and this SLA through a telephone help desk staffed by trained and qualified natural persons, supported by additional technical support personnel, and not recorded messages ("**Help Desk**"). Authorized Users shall be able (i) to report to the Help Desk problems with the Software and the Documentation and (ii) to receive from the Help Desk prompt assistance in the use of the Software and the Documentation and in the identification, evaluation and resolution of Errors. Licensor will provide Authorized Users access to a toll-free telephone number dedicated to Authorized Users only for all support calls. During the term of this Agreement, the Help Desk normal operating hours shall be at least M-F 8:00 am to 11:00 pm ET, Saturday 8:00 am to 9:00 pm ET, and Sunday noon to 9:00 pm ET. Licensor will use commercially reasonable efforts to have a trained and qualified person answer all calls to the Help Desk by Authorized Users during normal operating hours within 90 seconds.

   b. **Errors**. If Licensor is not able to resolve a Authorized User's question or problem within four hours after that Authorized User's first call to the Help Desk, then:

i. Licensor shall use commercially reasonable efforts to respond to Errors within the applicable time period based on the Severity Level as reasonably determined by the Authorized User.

ii. For purposes of this SLA, the Severity Levels are as follows:

Severity Level	**Definition**
Level 1	**High Priority**. Software (a) not operating at all, (b) having material functions or functionality not operating or operating improperly, or (c) operating in a manner that is corrupting, or is likely to corrupt, any data of Licensee or an Affiliate.
Level 2	**Intermediate Priority**. Software operating properly only with a work around.
Level 3	**Low Priority**. Software has problems with operations that do not reduce functions or performance in a material way.

iii. **Severity Level Response Times**.

(1) Level 1 = Response time is 1 hour or less
(2) Level 2 = Response time is 8 hours or less
(3) Level 3 = Response time is 5 business days or less

iv. **Continuous Efforts**. Licensor shall use reasonable efforts, 24x7x365, to resolve all Level 1 Errors as quickly as possible. Licensor shall use reasonable efforts, during the normal operating hours of the Help Desk, to resolve all Level 2 Errors as quickly as possible. Licensor shall use reasonable efforts to resolve all Level 3 Errors within 10 days after License first reports the Error.

3. **Availability of Software**. Licensor will use reasonable efforts to ensure that the Software is available to all Authorized Users and operable 100% of the time 24x7x365, subject to scheduled maintenance during the Maintenance Windows.

4. **Data Backup**. Licensor will perform a daily backup of all of Licensee's Data during the Maintenance Windows, will ensure all backed up data is encrypted, and will store all backup media at a secure off-site storage facility that complies with the Security Requirements. Licensor will retain all daily backup media for at least 30 days.

5. Service Level Guarantee. At the end of each month during the Term, Licensor shall calculate and report to Licensee the Availability (defined below) of the Software during the preceding immediately `month. If Availability falls below 99.99% in any month during the Term, then Licensee shall automatically receive a credit against all fees and charges due the next or a subsequent month under the Agreement equal to the amount specified in the chart below; **provided** that in no event will the total credits in any month under this guarantee exceed 100%

of the total monthly fees and charges due in such month. Unused portions of credits may be carried forward to future months.

a. **Credits Chart**

Availability Percentage	**Associated Credit**
99.99% to 99.5%	5% of all fees and charges for such month
99.49% to 99.0%	10% of all fees and charges for such month
98.99% to 98.5%	15% of all fees and charges for such month
98.49% to 98.0%	20% of all fees and charges for such month

b. **Definitions**. The Software shall be considered "**Available**" unless (i) Licensee or any Affiliate is unable to access and to use the Software with all functionality and performance described in the Agreement (the "**Non-Compliance**"), and (ii) such Non-Compliance is caused by the Software, Licensor's servers, network, other equipment, or application programs or facilities or issues for which Licensor is responsible under the Agreement. "**Availability**" shall be expressed as a percentage and shall be calculated by dividing the total number of minutes the Software is Available each month (excluding such minutes occurring during the Maintenance Windows that month) by the total number of minutes in that month (excluding the number of minutes in the Maintenance Windows that month).

c. **Termination**. If the Availability Percentage falls below 98.0% three months in a row or three months in any six-month period, then, in addition to its other rights and remedies under the Agreement and this SLA, Licensee shall have the right to terminate the Agreement without penalty by giving Licensor written notice of termination.

6. **Reports**. On or before the 5th day of each month during the Term, Licensor shall deliver to Licensee a written report detailing, with respect to the prior month, the Availability of the Software during the prior month, a detailed calculation of any credits due to Licensee, and other information about the service level guarantees or the Availability of the Software that Licensee reasonably requests. Licensor shall give Licensee immediately a report of any outage with respect to the Software.

7. **Help Desk Reports.** On or before the 5th day of each month, Licensor shall deliver to Licensee all call logs for the Help Desk with service event information as well as such summary reports as Licensee may reasonably request.