Document Management System
Contract Analysis and Negotiation

March 11, 2012

David Schlossman, M.D.
Northwestern University
Medical Informatics 408
Winter 2012

1. The SaaS (Software as a Service) Model

Right from inception, as specified in the Statement of Work (SOW) and the Request for Proposals (RFP), Community Physician Group (CPG) conceived and designed its Document Management System (DMS) to run under the SaaS model. SaaS is typically defined as a software deployment where a provider licenses an application to customers to use as a service on demand. The application is typically hosted on the vendor's Web servers where subscribing customers can access it using an Internet browser (TRACEONE, 2012). The SaaS model has a number of compelling advantages for CPG (TRACEONE, 2012 and Online-CRM, 2012) including:

- Cost factors. Much lower initial investment in servers, disk space, and personnel costs for additional IT staff members as well as overall lower total cost of ownership over time. Better predictability of future expenses allows easier forecasting and budgeting.
- Time factors. More rapid initial implementation with many of the deployment challenges outsourced to the vendor's expertise as well as access to continuous upgrades with less impact on CPG workflow.
- Flexibility. SaaS is designed and optimized to function over the Internet allowing employees to work from any location with secure Web access and is more easily scalable if the number of users needing access changes.
- Vendor interest. Successful application utilization is necessary to drive agreement renewals and customer references that maintain the vendor's revenue opportunities.

From the physician group viewpoint, the major risks of the SaaS model include:

- Off premises data location with potential access issues.
- Data security and confidentiality issues.
- System usability and level of service issues (latency and availability).

2. Key Components of the Software Contract

The first step in mitigating the risks of cloud computing is due diligence in selecting a vendor with the infrastructure, expertise, and experience to deal with the challenges, so that the benefits of the model outweigh the risks. CPG is confident that this has been accomplished during the RFP process. The second step is negotiating a contract that clearly defines the organization's business needs, the agreed-upon solutions, and the mechanisms to ensure that the vendor will make its best effort and use all its resources to deliver those promised solutions. The key criteria CPG needs from the software contract are those which most effectively manage the risks of cloud computing and support successful adoption of this model. They fall into four main categories (Trapper, 2010): (1) service level agreements (SLA’s), (2) data processing and storage, (3) data security and confidentiality, and (4) vendor relationship management.

2.1 Service Level Agreements

The planned DMS is a critical component of the practice Electronic Medical Record (EMR). As such, documents contained in the DMS may be needed for patient care anytime of the day or night, 365 days a year, and inaccessibility or delay in accessing a documents could impede clinical activities and result in adverse consequences for a patient. The organization is therefore very concerned about the SaaS parameters governed by SLA's including performance and response time, uptime (system availability), support availability, and error and malfunction correction time (Trapper, 2010 and Greenback, 2010). The contract must define objective ways to measure these parameters, target benchmarks to be guaranteed by the vendor, and remedies sufficient to offset potential damages and strongly motivate vendor to meet specified performance targets. This will require a new contract paragraph on SLA's which are not addressed in the model document. It will also require significant revisions to paragraph 3, seven, and eight of the model contract.

2.2 Data Processing and Storage

Because the practice’s valuable data is stored and processed in the vendor's data centers, it is important for the contract to confirm CPG's sole ownership of the data and ownership interest in the results of any processing of that data. If the practice’s data is kept in a multitenant environment in a single server along with the data of other clients, the logical partition architecture protecting its integrity must be verified or consideration should be given to changing to an ASP type model using a dedicated server (Garcia, 2010 and Trapper, 2010). Because circumstances may change requiring the organization to migrate to a different SaaS provider, the contract must specify the method by which the data will be returned to or retrieved by CPG, affirm the practice’s legal right to unfettered access to the data until the transfer is complete, and delineate the vendor’s responsibility and methods for deleting sensitive data after the transition (Trapper, 2010 and Greenback, 2010). Because the data contains Protected Health Information (PHI), the contract must specify a HIPAA compliant Business Associate Agreement and data breach notification processes consistent with state and federal laws. There should also be provisions to indemnify CPG for losses due to data breach that was solely the responsibility of the vendor. Storing protected data outside of the United States may violate export control laws and certainly adds significantly to risk, so this should probably be forbidden in the contract. Finally, the contract should specify the vendor's obligation to CPG should any protected data become the subject of a legal or governmental request for access. The above considerations (summarized from Trapper, 2010) will require the addition of several paragraphs to the model contract and will also require significant revisions of paragraphs nine and ten of the model document.

2.3 Data Security and Confidentiality

The safety and integrity of data in the cloud are dependent on functionality of physical data centers. This is especially pertinent in the case of data that represents PHI and components of a legal medical record. It is therefore vital for the contract to codify the specific infrastructure and security obligations and practices the vendor will use to protect the data (Trapper, 2010 and Greenback, 2010). Issues to be addressed include backup procedures, encryption, firewalls and malware protection, physical security of the data center itself, data center security auditing and certification, and rights to data center inspection. The contract should also address the vendor's disaster recovery and business continuity (failover) mechanisms and specify the SaaS provider's obligations to the organization should any of the data become lost or damaged due to vendor’s errors. Again, this will require a substantial new contract language as well as major revision of paragraph 15 in the model document.

2.4 Vendor Relationship Management

Changing to a different service provider can be enormously expensive, and the organization’s negotiating leverage is usually highest before the initial agreement is signed. Therefore CPG wants the initial agreement to specify each organization’s ongoing rights and duties as the product is used over time (Trapper, 2010). Vendors proposing a longer initial term of agreement should be willing to negotiate pricing discounts in return. Even if the initial pricing is favorable, it's vital to protect future interests by also negotiating the maximum cost increase to continue using the service after the initial purchase period. It's also vital to specify the cost structure for expansion or contraction of the organization’s initial volume of usage (Trapper, 2010). One of the great selling points of SaaS is scalability, so the contract should protect the organization from increases in unit price if usage volume decreases or requirements to pay for unused subscriptions until the end of the current term (Greenback, 2010). If there are particular functionalities that are vital to the organization, they should be specified in the contract and conditions under which they may be modified or deleted, even as part of an upgrade, should be defined. The contract should be clearly binding on successor organizations if the vendor is the subject of a merger or acquisition and should keep the primary vendor responsible for complying with all terms of the agreement even if it chooses to outsource some functions to other organizations. Finally the contract should specify the terms and conditions (such as vendor nonperformance or noncompliance) under which your organization can terminate the agreement without penalty (Trapper, 2010).

2.5 A New Paradigm for Software Contracts

Overly and Kalyvas's (2004) model vendor contract was designed to apply to a more traditional software purchasing model where the customer actually takes possession of a copy of the software and manages the technical solution within its own organization. As such, it does not even address the majority of the contracting issues raised in this section. The four broad categories of concern for SaaS contracts encompass a multitude of specific issues all of which are vital in the sense that failure to properly address any one of them could potentially lead to harm to one of the physician group's patients, devastating financial losses, a sudden complete stoppage of the organization's business functions, or other absolutely unacceptable consequences. Therefore, they are all necessary for the contract to be "a successful deal for our organization," and the physician group views them in that light. As cloud computing becomes ever more prevalent, best practices are starting to emerge. Sample contract language applicable to all of the areas mentioned and links to the standard contracts of major cloud computing providers such as Amazon, Microsoft, and Google can be found in Trapper’s (2010) paper on cloud computing contract issues. A sample contract signed by the city of Los Angeles with Google Apps provides good examples of how the best practices can be implemented (City of Los Angeles, 2009). Because the physician group does not actually "own" the software, the structure of the license agreement *per se* is much less important in these types of contracts. The functions of a specific "warranty" largely become subsumed in the service level agreement and contract sections specifying the vendor support obligations, so these are also less important.

3. Vendor Resistance

3.1 HIPAA Compliance Issues

The vendor may object to executing a HIPAA compliant Business Associate Agreement, to the stringent security requirements, and especially to the very expensive indemnities which might be required in the case of a data breach. One approach to managing this would be to reframe the problem by emphasizing that these issues are a fact of life for all organizations in the medical field and asking for their suggestions on a fair way to distribute data breach risks. CPG could also point out that developing expertise in dealing with HIPAA security issues can provide a competitive advantage for the vendor in a market which represents 16% of the total economy and which is rapidly expanding its use of information technology.

3.2 Discounts and Length of Term

The term of SaaS contracts can vary from as short as 30 days to as long as five years. Vendors will push for a longer-term in order to enhance the simplicity and accuracy of their revenue forecasts. CPG will seek an initial contract term no longer than one year in order to verify that the product functions well and fits the organization well before making a longer commitment. If the Vendor pushes for a longer term, CPG would consider a two-year contract if it involves negotiated price discounts, scalable pricing for increased or decreased numbers of users, and/or a clause allowing CPG to break the contract within a specified time window if the system is not meeting the defined business needs (Greenback, 2010).

3.3 Support

Because the functionality and availability of the DMS are mission-critical, CPG will be seeking contract language to define 24/7 support availability by Internet, e-mail, or phone and response times of 30 minutes in emergency or two hours in all other cases (Greenback, 2010). Recognizing that these stringent conditions require significant investment in support infrastructure, CPG would be willing to make some price concessions to obtain this level of service. However, CPG will expect the vendor to be able to meet or exceed industry standards for support of mission-critical applications.

4. Best Alternative to a Negotiated Agreement (BATNA)

Community Physician Group's BATNA is to end negotiation with Vendor 1 and initiate contract negotiations with Vendor 2 (see Assignment 4). Although CPG preferred the security and stability of the larger Vendor 1, Vendor 2's proposal did meet all the requirements of the RFP and demonstrated its capability of designing a workable DMS, with the added advantage of being a less expensive solution. Advantages of pursuing the BATNA include:

- Lower initial cost.
- Access to innovative software design with the potential to produce a faster, more responsive DMS, especially in regards to search functions.
- Potential to negotiate a more equitable contract that better meets CPG's key criteria.

Disadvantages of the BATNA include:

- Abandoning the time and effort spent negotiating with Vendor 1
- Failure to obtain the more secure software and comprehensive support infrastructure that CPG really wanted.
- Risk that Vendor 2's product will be less reliable and secure than Vendor 1's.

5. Negotiating a Service Level Agreement

5.1 Key Issues

System performance, latency, and uptime will have a major impact on physician efficiency and significant problems with availability of the DMS might even impact patient safety, so these components of the SLA are of the utmost importance to CPG. Since SLA's are a standard part of SaaS contracts, the vendor will expect to negotiate the goal parameters and minimal acceptable levels for each element of the service provided and the penalties that apply when these targets are not achieved (Trapper, 2010). By far the most common uptime target for SLA's is 99.9%, but the vendor will press for very favorable definitions that only measure down time when their own internal systems report an error and that leave room for dispute about the exact method used to calculate the uptime number. The remedies vendors typically offer consist of small discounts against future service purchases (Greenback, 2010). CPG will need to insist on stringent, precisely defined methods of uptime calculation, on penalties large enough to motivate the vendor to meet or exceed the required level of service, and on the right to independently audit the service quality data to confirm the uptime calculation. The strong difference in viewpoints between the two parties can greatly complicate the process of reaching agreement in this area.

5.2 Going to the Balcony

Going to the balcony is Ury's (1991) metaphor for pausing a negotiation, breaking the cycle of action and reaction, regaining emotional composure, and taking a wider view of the problem in order to develop a solution that can serve both parties' interests. Although there is a small possibility that the other party might feel you are delaying or are too weak to face up to the issue, there really is very little risk to using this technique. Ury himself says "you should go to the balcony at every possible opportunity throughout the negotiation (Ury, 1991, p. 38)." The potential benefits are great. As you control your own emotions, the other party also has time to cool off. You can think through the issues more clearly and comprehensively, better understand the other party's concerns, find areas of agreement on which to build, and find creative ways to craft an agreement that satisfies your interests. After all, the goal of SLA penalties is not to obtain discounts from the vendor. The goal is to incentivize the vendor to provide the level of service that will keep your organization running smoothly and efficiently (Trapper, 2010).

5.3 Other Approaches to SLA Negotiation

Another approach is to "step to their side" (Ury, 1991, p. 52) by discussing the technical challenges of very high availability requirements and carefully revising definitions to properly allow for planned and announced down times (maintenance and upgrades) and for Internet and public network disruptions beyond the vendor's control. Look for vendor concerns that can be addressed to make the agreement more equitable without being permissive. Lowering the uptime requirement to 99.5% and offering an incentive bonus for higher service levels is one such consideration.

A third approach is to propose using fair objective outside standards as guidelines for resolving the differences between the parties. The National Institute of Standards and Technology (NIST) has issued a set of *Draft Cloud Computing Synopsis and Recommendations* (Badger et al., 2011) which discusses many issues relevant to SLA's, and sources of consensus industry best practices are cited above in Section 2.5. Many large cloud service providers actually publish daily service quality statistics on a web-based dashboard such as Microsoft Windows Azure, Google Apps, and Amazon Web Services. These can also be a source of consensus industry standards. If the vendor is not confident that its product can maintain service levels comparable to industry norms, CPG would take this as a warning that the product's reliability may be less than was indicated in the vendor's proposal.

6. Source Code Escrow

In the SaaS model, the application source code, executable code, and subscriber's data all reside in the *vendor's* servers. Should the vendor go out of business or experience a prolonged service interruption, CPG along with multiple other subscribers could lose access to large stores of valuable historical data and rapidly become unable to continue its business processes. To mitigate this risk, CPG will insist that the contract contain a SaaS escrow protection agreement which goes beyond traditional code escrow. Offered by a number of large organizations such as Iron Mountain (Iron Mountain, 2012), these services combine traditional source code escrow with a separate escrow for executable code and independent automated data backup and recovery services by a separate entity outside of the vendor's company. The separate escrow account for executable code enables more rapid disaster recovery and application continuity in the worst-case scenario. Many escrow agents offer verification services to ensure that the escrow contains complete updated code that will function properly if demand-release conditions are met, and the extra level of *data* backup and recovery can be invaluable in a disaster. The importance of this protection in enhancing customers' trust in vendors and confidence in their data security has led many SaaS providers to execute two-party escrow agreements where a single copy of the source and executable code is held in escrow on behalf of all subscribers, and new subscribers can be added to the agreement by executing a simple 1-2 page document. Again, this is becoming an industry standard best practice in the SaaS model, and CPG would be unwise to omit such protection from the contract.

References

Badger, L., Grance, T., and Patt-Comer, R. (2011). Draft Cloud Computing Synopsis and Recommendations: Recommendations of the National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf.

Brenner, B. (2010). SaaS, Security and the Cloud: It's All about the Contract. CSO Data Protection. Retrieved from http://www.csoonline.com/article/589963/saas-security-and-the-cloud-it-s-all-about-the-contract?page=1.

City of Los Angeles Google Apps Contract (2009). Retrieved from http://clkrep.lacity.org/onlinecontracts/2009/C-116359_c_11-20-09.pdf.

Esperne, E. (2010). Managing Risk in SaaS, Cloud Computing and Other On-Demand and Web 2.0 IT Contracts. IACCM Contracting Excellence. Retrieved from http://www.iaccm.com/news/contractingexcellence/?storyid=903.

Garcia, J. (2010) A Tour of the Clouds. Technology Evaluation Centers research article. Retrieved from http://www.technologyevaluation.com/research/articles/a-tour-of-the-clouds-21076/

Greenback, L. (2010). Nine Key Points to Negotiate in a SaaS Negotiation. SIAA Digital Discourse Blog. Retrieved from http://www.siia.net/blog/index.php/2010/12/9-key-points-to-negotiate-in-a-saas-negotiation/.

Iron Mountain (2012). Software-As-a-Service Escrow. Retrieved from http://www.ironmountain.com/Services/Technology-Escrow-Services/Software-as-a-Service-Escrow.aspx.

Overly,M. and Kalyvas, J. (2004). Software Agreements Line by Line. Thompson/Aspatore: Boston, MA

Online-CRM. (2012). The Realities of CRM SaaS-Advantages and Disadvantages. Retrieved from http://www.online-crm.com/saas_advantages_disadvantages.htm.

TRACEONE (2012). Advantages of SaaS. Retrieved from http://www.traceone.com/services/software-as-a-service/advantages-of-saas.html.

Trapper, T.J. (2010). If It's in the Cloud, Get It on Paper: Cloud Computing Contract Issues. *EDUCAUSE Quarterly 33*(2). Retrieved from http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/IfItsintheCloudGetItonPaperClo/206532.

Ury, W. (1991). Getting Past No. Random House: New York, NY.