PUBLICATION

Cloud Computing For Health Care: Ready Or Not, Here It Comes

July 21, 2010

If you have not already, you will soon need to address the legal (and business) risks of "cloud computing." The cost savings offered by cloud computing are too compelling for a CFO or CTO to ignore. There are many types of cloud services models and, to make matters more confusing, the models keep changing. Cloud services have also created additional legal challenges in highly regulated environments such as health care.

This summary discusses one of the more "standard" cloud offerings known as "software as a service"—the outsourcing of email, applications, software, data processing and data storage from within an organization to a third-party vendor. In this scenario a user would not, for example, have word processing software installed on a computer; rather, the software is accessed and used through the Internet on servers owned or controlled by the vendor. The document is then stored on those servers and not necessarily on the user's computer. The vendor provides the same services to many other parties using "shared" servers, applications, software, and facilities. To clarify, we are not talking about using cloud services for life and death procedures.

Cloud services offered to the health care industry involve more challenges than other unregulated industries. A simple example is that email and documentation may contain Protected Health Information (PHI), invoking the regulatory obligations relating to PHI. This summary is based on recent experiences negotiating with some of the largest cloud computing vendors to the health care industry.

1. Understand the Business Model. We all know that assessing the legal risks of any procurement requires an understanding of the proposed business model. Cloud computing is no exception, with the twist that it is still a *developing* business model that will probably go through many changes over time (and the contract will need to address this reality). For this summary, assume that a health care organization is going to outsource its general email system (health care organizations may still maintain another email system as part of their electronic records suites). In addition, it will be using collaborative tools, such as instant messaging and project management applications, as well as word processing and similar applications offered by the cloud vendor. Finally, all of the data, documents and other "things" used or created in connection with the cloud service will be stored and processed at facilities provided by the vendor or its affiliates or subcontractors.
2. Understand the Vendors. The culture of the cloud vendors will determine the tenor of the negotiations. Vendors for the cloud range from very large vendors of many "free" cloud services for consumers, to well-established and more traditional software licensing companies who are accustomed to doing big "enterprise" deals but are relatively new to the cloud model. It is often challenging to get companies with roots in the "free" consumer world to think in terms of multi-year contracts with businesses. It is equally challenging to get established companies to maintain traditional terms of multi-year contracts in cloud contracts (discussed more below). Another challenge is to convince vendors that, for example, privacy policies, acceptable use policies and security policies provided to individual users for their free services are not appropriate for a health care organization. Also, many cloud vendors work diligently to avoid involving their respective legal teams early in the process, which can substantially increase the contract negotiation time (particularly as they confront the relatively novel issues associated with the health care industry).

Because of the cloud's emerging business model, it is advisable to explore the use of resellers (for potentially better terms) and to consider running multiple negotiations with multiple vendors before down-selecting. As you will see, while most vendors will acknowledge that having your email down, a major loss of data or a security breach of PHI are all "mission critical" situations, translating those and other issues into meaningful legal documentation is an entirely different matter. Keep your options open.

3. Understand the Contract. Cloud computing agreements are often a myriad of documents tied together through many other contracts incorporated by reference through hyperlinks. Before doing your legal analysis, take the time to actually go through each and every link and the related documents. You may be surprised to find just how many agreements actually exist. Many of these are critical agreements, such as service level agreements, privacy policies, security policies, service descriptions, technical support obligations, acceptable use policies, and the like.
4. Pick your team. Cloud computing deals can cross over different disciplines. At least for the near future, your negotiating legal team should most likely include a business technology lawyer, a privacy and security lawyer (often a regulatory lawyer), and an eDiscovery lawyer. The primary negotiator should probably be your technology lawyer, but that lawyer will need help addressing the more complex aspects of privacy, security and eDiscovery in the "cloud."
5. Service Descriptions. Cloud vendors often have a large number of cloud offerings. Before you begin your legal analysis, it is advisable to have a discussion with your internal team and the vendor to specifically point to which services are being provided. You may actually wind up adding or deleting services based on the needs of your company. In addition, great levels of security, privacy, and eDiscovery functionality often require additional and separate services from the vendor.

You may find that it is difficult to obtain sufficient service descriptions. Many vendors have sales documents that describe the services in some detail but are themselves expressly not part of the agreement. Other vendors incorporate descriptions of services through links on sites that most lawyers would not consider pure "service descriptions." These documents can often be user manuals or user guides that, if pieced together and incorporated into the agreement, could be sufficient to be considered service descriptions. In general, however, for health care regulatory compliance as well as eDiscovery purposes, it may be insufficient to defend an inquiry from an administrative agency and show that your company discharged its due diligence on any cloud service without being able to point to a good service description which is actually part of the contract. In addition, in the event of a breach, your company will be severely hampered if there are insufficient service specifications that can form the basis of a claim.

6. Business Associate Agreement. There is currently little consensus from the cloud vendors that they are business associates. Many vendors will readily agree to some form of business associate agreement (BAA) while others will not sign anything containing the word "HIPAA." As you know, covered entities are obligated to ensure that all vendors who are business associates have a BAA. The Office of Civil Rights (OCR) has issued guidance when the vendor would have access to the PHI. The guidance states that if a "software vendor" hosts software that contains PHI on its own server, or has access to the PHI when troubleshooting the software, then the vendor is a "business associate." As discussed earlier, having access to a privacy and security subject matter expert for discussions with the vendors as well as providing contractual language is critical.
7. Security. From a compliance standpoint, a covered entity must be able to prove that it is HIPAA security compliant (including through its vendors) and more significantly, it must have a meaningful contractual clause in a cloud agreement that the vendor will remain HIPAA compliant and assist with the covered entity's on-going efforts. Compliance obligations ultimately flow back to the covered entity, but have contractual assurances that the tools and applications made by the vendor (a) meet HIPAA compliance requirements when implemented and (b) will remain in compliance as the law

changes. Note that, as required by recent OCR guidance, the covered entity will need to be able to have a complete risk analysis performed.

8. Data Breach. Address the possibility of a data or security breach. This includes understanding the investigation and notification requirements of the HIPAA breach notification rule as well as those of the majority of states that have data breach rules. Many vendors will orally state that they will assist, but you will most likely need to incorporate negotiated language into the actual agreement.
9. eDiscovery. eDiscovery can be a particular challenge when using the cloud because data, documents, email and other intangible information can be stored on shared servers in distributed locations within or outside the United States. An eDiscovery legal team member should review the eDiscovery service offerings of the cloud vendor and contractual language in the agreement (or, in some cases, the lack of appropriate language). Of course, your company must comply with the Federal Rules of Civil Procedure and the various states' rules of civil procedure. The vendor's product should be tested and provide the appropriate functionality to allow your company to remain compliant. Contractual language should ensure that such functionality both exists and will not be reduced. Also, remember that eDiscovery means more than just archiving of emails; it also includes instant messaging and other data from other collaborative services provided in the cloud. In addition, you will need to address in the agreement how the vendor will respond to third- party subpoenas or other attestation requests as well as witness availability.
10. Service Level Agreements. Service level agreements (SLAs) are provided by most vendors in connection with specific services, such as "up time" or "availability." Most SLAs provide credits for the failure of the vendor to maintain certain metrics. Most vendors, however, start with the proposition that such credits are the sole and exclusive remedies for such failure. So, while SLAs are good in concept, be aware that they can also severely limit contractual remedies you may have against the vendor unless otherwise negotiated. Also, note that many vendors rely on providing SLAs for uptime instead of giving good service descriptions on disaster recovery and business continuity. The challenge with that (as discussed in the disaster recovery summary below) is that "uptime" commitments do not mean that you understand and agree with the vendor's recovery plan, especially if the sole remedy for the failure to provide the "uptime" is the credits.
11. Modifications to the Service. Most vendors will insist upon retaining the right to modify the services at any time. This can be a point of negotiation. This concept seems to be a holdover from business-to-consumer arrangements and does not translate well into multi-year business agreements in a highly regulated industry. While updates, error corrections, and modifications to a cloud environment as well as additional functionality are inevitable, there need to be restrictions on any *reduction* in the functionality that a covered entity is relying on, especially as it relates to privacy and security and eDiscovery.
12. Modifications to the Terms and Conditions. More onerous than changes to the services, most vendors maintain the ability to change the terms and conditions of the underlying agreement (and any others incorporated by reference) at any time. Some seek an unqualified right, while others create a system where the buyer needs to notify the vendor if such proposed changes materially affect the buyer's business, in which case they would not apply except for a renewal term. The same challenges apply here as with modifications to the services; the covered entity must be able to rely on contract terms as written (including those linked, such as the privacy and security policies). Many of the terms and conditions from an eDiscovery and health care perspective simply cannot be subject to change, especially if such change results in less protection or expanded use. Address this issue in the agreement.
13. Suspension of the Services. Some vendors reserve the right to suspend the service for "any reason," while others want to suspend when the vendor believes that the buyer is in breach of the agreement. As discussed, the use of the services (especially email) is mission-critical for business continuity as well as compliance with health care and other obligations. In short, suspension of the entire service

(versus suspension of an end-user account) should only be allowed in very limited circumstances, such as when many customers are shut down because of a network emergency.

14. Termination and Assistance Services. Most vendors do not provide termination assistance other than providing the buyer some time to download data. In reality, however, consider having continued access to the services as a whole in time to transition to another email vendor or to take it back in-house. This also relates to knowing (and negotiating) the type of format the data can be provided and potential remedies for failure to provide access to the service.
15. Disaster Recovery/Business Continuity. You will most likely need to incorporate some language regarding disaster recovery or business continuity. Many vendors state that they have recovery and continuity policies and that the SLAs for uptime are evidence of the same; however, a covered entity must have a disaster recovery program that must include the vendor's services. For example, consider reviewing the vendor's policy for disaster recovery and business continuity and compare the policy against the HIPAA requirement found at 45 C.F.R. §164.308(a)(7)(ii) as well as from an eDiscovery standpoint.
16. Privacy Policies. All vendors have links to various privacy policies and most are incorporated into the agreement. Review and discuss which privacy policies are applicable to the actual services provided. Depending on the outcome of that discussion, certain restrictive language may be required for inclusion in the agreement.
17. Data Transfer/Offshoring. As a covered entity, understand the current practice of the vendor and possibly prohibit any PHI from leaving the United States. While HIPAA does not currently explicitly prevent PHI from residing outside the U.S., there are significant legal issues which occur as a result (including implicating data privacy and security regimes of other countries or regions, such as the European Union). Additionally, there are concerns with different and/or greater privacy protections of other jurisdictions where data could reside, even if only for a short time. Such privacy concerns could arguably impact and constrict disclosures or eDiscovery requirements related to the production of such data.
18. Liability. Consider remedies for lost or damaged data as well as for breaches surrounding privacy, security, or compliance with regulatory or other laws. There are other issues to consider here, such as the failure to provide transition assistance that results in material business interruption.

These are just some of the issues that need to be addressed. One thing appears to be certain—cloud technologies are currently way ahead of the lawyers in terms of contractual requirements. Over time, negotiations and contracts should become more standardized. For now, however, do your best to help weigh the cost savings against potential legal risks. Part of this analysis will also include determining whether the vendor provides greater protection that you already have, regardless of legal risk!