Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Business Risks To Consider When Outsourcing Health IT

Law360, New York (February 25, 2014, 5:26 PM ET) -- Information technology systems outsourcing is a trend that goes back to the early days of commercial computing. While the name has changed — from "timesharing," "outsourcing" and "offshoring" to the current "cloud" and "as a service" model — and business models have evolved with changing technology, the central driver is the same. Without question, sharing specialty technological resources among multiple customers makes them cheaper and more readily available.

Initially, the burdens of the Health Insurance Portability and Accountability Act's compliance and risks associated with electronic health records kept all but highly specialized technology providers from offering their services in the health care field. However, with the frenetic activity in health care information technology since the American Recovery and Reinvestment Act's meaningful use and electronic health record incentives, health care information technology outsourcing has become a booming business.

The first priority in outsourcing any health care information technology ("HIT") service is, of course, nailing down concerns with the handling and use of individually identifiable patient information. By now most customers and providers of HIT services are aware of the importance of conducting a proper and fulsome risk analysis of the potential risks and vulnerabilities to the confidentiality, availability and integrity of all electronic protected health information ("e-PHI") that it creates, receives, maintains or transmits. Both parties to any HIT outsourcing transaction are likely to have their own forms of business associate agreements and most have a sophisticated understanding of the importance of both putting those agreements in place, and policing their terms.

While the regulatory issues are admittedly key, it is equally important to assess the enterprise risks that arise when negotiating and contracting for any purchase of outsourced services such as systems, storage, software and/or personnel. Below are five other business risk elements to consider.

Establishing and Enforcing Service Level Agreements

According to a recent survey released by the Ponemon Institute and Emerson Network Power, unplanned data center downtime cost health care organizations $689,912 per incident in 2013, and the average cost per minute for data center downtime (across all industries) rose to $7,908.

When you own the data center, and it stops functioning or underperforms, management has direct and meaningful ways to fix the problem. Someone gets fired, new hardware gets purchased and bandwidth is increased. But when a system is outsourced — especially a system related to the provision of direct patient care, which can be difficult to transition to a new provider — resolving performance problems

gets touchier.

Because the customer does not want to have to terminate the agreement or sue the vendor for the damages that come from downtime, it is normal to have quantifiable and easily determinable service levels set out in any outsourcing agreement. However, when assessing the overall risk that outsourcing may present to the business, the details of the service level agreements become critical.

Does the agreement only address "up time?" Or, does the service level agreement include system, disaster recovery and help desk response times? Do the definitions used to calculate any service level credit leave huge loopholes? And, if a service level credit will be the only remedy for a single instance of breach, is there still a methodology for the customer to terminate the arrangement if there are multiple or egregious breaches?

These issues are not unique to HIT. But they are particularly acute when outsourced systems support mission critical or patient care applications, where a single day — or even a single hour — of service interruption can critically impair the delivery of patient care.

Terminating an Outsourced Arrangement

It is relatively painless to get into an outsourced arrangement. Outsourced service providers will often absorb most or all of the cost of getting the customer's data onto the system, formatted in the right way, and the users trained. Early year prices are low.

At the agreement's end, however, motivations change, prices increase and the outsourced provider has no incentive to assist in a transition to a competitor. Therefore, it is important up front to specify obligations and costs upon termination. Will the customer have to pay to get its data back? Will the data be in a proprietary format at that point? Will the vendor provide assistance in transitioning to a new service? Will the customer own (or at least be licensed to use) any customized reports, interfaces or other deliverables the vendor developed during the relationship?

In addition, in the HIT area, health care providers typically have independent regulatory obligations with respect to maintenance and destruction of data. For example, a hospital simply could not agree to allow an EMR vendor to hold the provider's EMR data hostage post-termination. Nor could the health care provider agree to data destruction terms that do not meet HIPAA and state law data security standards.

Pricing Changes During the Relationship

Outsourced service charges typically rise year over year, even though the cost of hardware and bandwidth traditionally declines over time. Many outsourcing business models are predicated on winning the service by bidding at or below cost, and then (because the service is difficult for the customer to transition away from) raising the price over time.

Therefore, even when purchasing a one year contract for HIT services, it is important to try to lock down multiyear pricing, especially if the transition away from the service would be expensive. Although initial pricing may be so low as to not be economically viable for the service provider to offer long term, tying escalation to CPI, or capping escalation with "most favored nation" style pricing provisions can be useful.

Service Changes Over Time

If transition on and off the service is easy, you don't need to worry about holding the service provider's feet to the fire on new functionality. Market forces should keep them updating the functionality in a manner that won't be disruptive to the customer's other systems.

However, when the customer can't quickly or easily change systems, the issue of updates and "technical currency" becomes important. Because most outsourced services are multitenant platforms, the vendor needs to remain compliant with the technical architecture used by most of its customers. Therefore, if an individual customer either wants to upgrade to a new technology, or, conversely, does not want to upgrade its back end systems or retrain its users when the vendor wants to upgrade, there can be problems.

In the HIT context, it is particularly important that the outsourced vendor be required to make changes to its system for regulatory compliance reasons. For example, agreements with respect to billing and claims submission should address transition to ICD-10 coding.

Third-Party License Issues

Although most outsourced HIT systems are advertised as "easy to implement" one-stop services, the reality is that most modern outsourced platforms are complex multilayered ecosystems of interoperable hardware and software.

Many of the big cloud service providers include third party add-on functionality that can be very valuable. However, if you look closely at the terms, frequently the main vendor is disclaiming any and all responsibility for the functionality or actions of the third party. Given that the main system and third-party system are often interwoven — and that the customer seldom has the technical detail to determine which system really is causing an issue — this can be a problem. The customer just wants to know that the (whole) system is up and running. They never want to have to settle a dispute between warring providers about which party is breaking the other's system.

This becomes even more apparent and sensitive when the customer has its own third-party vendors that it wants to integrate with the outsourcer's system. Enterprise software licenses may require special permission (and additional payment) before they allow the customer to permit an outsourcer to do the necessary integration work. If the original enterprise vendor offers its own competitive service, it may just plain refuse that permission.

For example, most hospital billing systems require interoperability between its EMR system, its coding/claims system, its patient accounts system and its collections system. It is rare for all of these functions to be provided by the same vendor — most providers combine several third-party software solutions to deliver this functionality.

It is important early on to assess which third party software will interact with any outsourced system. Then the outsourcer and the customer need to work together to allocate risk, responsibility and cost, for the interoperation and maintenance of the systems.

Conclusion

In sum, outsourcing any system can provide access to better technology at a lower cost. However, it must be handled thoughtfully, and the risks dealt with. Because HIT outsourcing in particular requires extra focus on the handling of confidential personal health information, it is easy to skip over or trade

away points in other areas. While regulations might not require a risk assessment that addresses the points raised above, good business practices suggest you consider them.

—By David G. Rickerby and Julia R. Hesse, Choate Hall & Stewart LLP

David Rickerby and Julia Hesse are partners in Choate Hall & Stewart's Boston office, where they are members of the firm's health information technology group.