By Bob Doe

Negotiating Application Service Provider Agreements

Understanding the Upsides and Downsides of ASPs

Software vendors are increasingly providing access to their software programs by acting as an application service provider (ASP) to healthcare IT users. Under an ASP agreement, the vendor provides the user with remote access to its software application from a centralized site and maintains the environment for the application.

Sometimes access to the application is referred to as a "service" and the agreement is called a "services agreement" (as opposed to a license agreement). From the user's perspective, this should not change the approach to negotiating the agreement. Updates and upgrades are performed on the software vendor's site with minimal impact to the user's system. The main benefit of using this model is low upfront costs. The risks of using this model are that the license is usually term-based and the user's ability to customize the application for its own particular use may be limited.

This column addresses significant issues that must be addressed in ASP agreements. General software license agreement issues must also be addressed in addition to those raised in this article.

DATA

In most ASP arrangements, the software vendor will maintain the user's data on hardware physically located at the software vendor's site. In some instances, the user may not even be capable of retaining a copy of the data that will be provided to the software vendor. For this reason, it is essential to address several issues relating to the user's data in an ASP agreement.

Data ownership. It is important to make clear that all data provided to the software vendor will remain the property of the user and cannot be used for any purpose other than those specified in the agreement.

Data security and access. Data security and access must be addressed in all ASP agreements, especially if the software vendor will be storing the user's data at the software vendor's site. These issues are even more significant if the user will not retain a copy of the data being stored by the vendor.

The user should ensure that its data will be maintained securely while in the possession of the software vendor. Depending on the importance and sensitivity of the data the user can include specific language regarding the particular obligations of the software vendor with regard to keeping the data secure. For example, the user can specify in the agreement which individuals will have access to the user's data, where it will be stored and how it can be accessed.

The security provisions of the user's business associate agreement may cover this issue with regard to patient-related information, but the business associate agreement will likely not be sufficient to protect all of the user's data security interests.

DISASTER RECOVERY

As the user is dependent on the software vendor's hardware and environment to provide access to the software application, the user should include a provision in the agreement requiring the software vendor to follow a disaster recovery plan that will ensure limited downtime and data loss. The disaster recovery plan should include provisions for backup storage of data at an off-site location and user access to the software application and data from a backup site. As each situation is unique, the user should request to review the software vendor's disaster recovery plan. If the plan the software vendor has in place is acceptable to the user, the user can then attach the plan to the ASP agreement as an exhibit, and reference the exhibit in the body of the contract.

TRANSITION SERVICES

Upon termination of the ASP agreement the user will likely need to transition to another third-party solution or one hosted by the user itself. As circumstances surrounding termination of an agreement can vary, it can be very advantageous to include language in an ASP agreement obligating the software vendor, after termination of the agreement, to continue to provide services and access to the software application until the user has transitioned to the new system. This may include assisting with the migration of data to the new system. Absent a vendor breach, the user will likely be required to pay for such services.

RENEWAL ISSUES

As with any agreement that provides services or products on a renewable term

basis, the user should include language that gives the user control over whether the agreement will continue to renew after the initial term. If such language is not included, the user may encounter several problems at the end of the initial term. First, due to the fact that the user has likely made an institutional commitment the hosted software application, the software vendor will have significantly greater bargaining power regarding the pricing and terms governing the renewal term. Second, the software vendor may choose not to renew the agreement, in which case the user may have limited time to find a replacement application. At a minimum, the agreement should require the software vendor to commit to an agreed upon number of renewal terms. In addition, the user should limit increases to the fees charged by the software vendor which are paid on a recurring basis for each renewal term.

SERVICE LEVELS

Uptime and response time. Of particular importance in an ASP agreement is the uptime and system response time representations. The software vendor should represent that the application will be available to the user a certain percentage of the time during a designated period. The software vendor also should represent that the application will respond within a certain amount of time to the user's commands. Any failure to achieve the agreed upon uptime and response service levels should result in a credit of some percentage of the hosting and/or license fee. This response time guarantee should not be confused with support response time representations regarding the software vendor's time limitations to respond to support requests. The uptime and response time service level provision in an agreement should address the following questions:

- Over what period of time will the uptime and response time calculation be made (weekly, monthly, quarterly, annually)?
- What hours should the application be available or meet the response time representations (e.g., 24 hours per day, seven days per week; 8 a.m. to 5 p.m., Monday through Friday).
- What constitutes downtime and response time?

Credits. The service level provision should set forth the consequences of not meeting the service level representations, which is typically a credit to the user. Credits should increase as the level of failure increases. The credits are usually expressed as a percentage of the periodic license or hosting fee. The user should also include the additional protection of the right to terminate the agreement for significant or chronic failures to meet the uptime and response time guarantees.

The user should keep in mind that a credit is only helpful if the agreement continues. Therefore, the agreement should make clear that the user should be given a refund in lieu of a credit if there are no more invoices to be issued under the agreement. The user should strongly resist any attempt by the software vendor to make these credits sole and exclusive remedies.

Scheduled maintenance. As scheduled maintenance time is not included as downtime or poor response time, the user should specify when scheduled maintenance should occur, the maximum number of hours per month scheduled maintenance will be performed, and that the software vendor will notify the user in advance of any scheduled maintenance to be performed.

Reporting. The user and software vendor should agree how the service level guarantees will be monitored. If the software vendor will be providing the data, the data should be sufficient for the user to make the applicable calculations regarding the service level performance. If the user has access to the relevant information regarding the performance of the application, the service level provision should state that the user's data regarding performance will be used to calculate the service level performance.

HOSTING ENVIRONMENT

The user should consider including a provision clearly specifying the parties' obligations with regard to the hosting environment that the software vendor will utilize to provide the hosting services. For the most part, this provision must make clear that the software vendor is responsible for the acquisition and maintenance of all hardware and software required for the hosting environment. If additional hardware and/or software is necessary for the software vendor to meet its contractual obligations, the software vendor must provide such hardware and software at no charge to user. The user may also want to consider including a specific listing or diagram of the hardware and software the software vendor will be utilizing, but allowing for upgrades, updates, enhancements and expansion as required.

Healthcare IT users that have made the decision to contract with a vendor that provides access to its software remotely should consider the following questions: What data will the user send to the vendor? Will the vendor have the only copy of the data? How sensitive is the data? What procedures does the vendor have in place to securely store the user's data? What are the vendor's disaster recovery procedures? What rights does the vendor have to terminate the agreement? What will the user do when the agreement expires or is terminated? How will the user transition to a replacement system? What contractual representations does the user have that the system will perform as anticipated? Does the user want to require the vendor to use certain equipment and software in its hosting environment?

Negotiating ASP agreements is similar in many respects to negotiating a standard software license agreement, but the user must be aware of the additional issues discussed above to protect its business and legal interests. **JHIM**

Bob Doe is a founding member of the law firm of Bonnabeau, Salyers, Stites, Doe & Andresen (www.bssda.com) located in Minneapolis, MN. Mr. Doe has extensive experience preparing, reviewing and negotiating information technology contracts. He can be reached at rdoe@bssda.com or 952-548-6064.