AHLA

Negotiating with Health Care IT Vendors

Member Briefing, March 2016

Sponsored by the Physician In-House Counsel Affinity Group of the In-House Counsel and Physician Organizations Practice Groups. Co-Sponsored by the Academic Medical Centers and Teaching Hospitals; Business Law and Governance; Health Care Liability and Litigation; Health Information and Technology; Hospitals and Health Systems; Payers, Plans, and Managed Care; Post-Acute and Long Term Services; and Regulation, Accreditation, and Payment Practice Groups; and the Behavioral Health Task Force.

AUTHORS

Wade Kerrigan
Kris Kappel
David M. Solberg
Husch Blackwell LLP
Kansas City, MO

The advance of technology provides unique opportunities and challenges for health care entities. Health care providers are developing a variety of new ways to care for patients, ranging from deploying an application for a patient's smartphone to using a complex software program that enhances research for challenging problems.

As health care entities manage their businesses, they enter into various types of agreements with technology vendors to support the provision of care, including: software license, maintenance and support, consulting services, software and application development, hardware, remote server cloud services, and hosting agreements, along with a myriad of related amendments, statements of work, work orders, and settlement agreements. These agreements can involve software enabling your client to use and maintain electronic health records, addressing billing procedures, or enhancing patient care. Each of these agreements presents different challenges, but this Member Briefing focuses on the issues that are the most common for these transactions.

While analyzing both sides of the vendor/licensee relationship on many issues, this Member Briefing primarily approaches these issues from the perspective of a customer of a software and hardware vendor in the health care industry. For purposes of this Member Briefing, we generally presume that you are representing a health care entity to negotiate one of the agreements described above. In most examples, the Member Briefing focuses on software license agreements (including cloud computing services and software-as-a-service or "SAAS" agreements), as those transactions are most common for health care industry clients.

Primary Considerations

Understanding the Business Deal

When your client works with vendors to procure information technology (IT) items or services, you should help your client understand the business deal with the vendor. The first step in any negotiation of a health care IT agreement is to meet with your client to

determine the goals that the client wishes to achieve with the new technology, whether it is software or hardware. You, in turn, should understand the product and the goals that your client expects the product will meet.

Once you understand the client's needs and expectations of the product, you should determine whether the vendor will provide customized developments to the software or hardware. If so, be aware that such customization can lead to many more complications and challenges, including implementation and testing issues, that should be addressed in the contract.

Another important aspect of negotiating a health care software agreement is the contract negotiation process. In the ideal situation, your client will establish a request for proposal (RFP) process that includes multiple software vendors. This strategy can lead to significant financial and legal benefits for your client. Your client should consider its implementation schedule during negotiations, particularly if the negotiations occur near the end of a calendar quarter or the end of a fiscal year. Significant financial benefits may accrue to a customer if a vendor is motivated to close a transaction prior to the end of a quarter or the end of a year. It is critical that you participate in the negotiations, the drafting of these communications, and the discussion leading to the ultimate vendor selection.

As you negotiate the agreement, you should understand the implementation process. When does the product need to "go live?" Is there any transition period from a previous vendor's technology? How long does your client need to test the software (*see Implementation Considerations and Acceptance Testing* below)? In particular, a health care company should determine whether any of its current IT agreements are nearing the end of a term or whether the entity is unhappy with the performance of its current vendor. If either of these is the case, the entity should reserve plenty of time to properly consider a new vendor and negotiate the new agreement. In addition, when reviewing the agreements, a health care company should ensure that the agreements do not contain automatic renewal terms with no guaranteed price caps.

Another important aspect of the business deal is the maintenance and support process and the fees related to those services. Counsel should work with its IT team to include appropriate details as to the level of maintenance and support and address the length of the term of the required maintenance and support for the licensed software. Even if a client acquires a perpetual license for a software program, this may not be sufficient to meet the client's needs if the vendor only provides maintenance and support for two or three years.

The client also should take particular care to evaluate the necessary functionalities and specifications for the proposed installed software, SAAS application, or cloud computing service. A proper description of these functionalities and specifications can appropriately set the baseline expectations of the vendor and the licensee. The failure to adequately describe the needed functionality and specifications of the software may limit a client's ability to recover later for any potential breaches of a vendor's obligations to provide a software program that meets the needs of your client. The vendor also benefits from a clear description of the program's functionality and specifications, which establishes appropriate expectations. The parties also should address whether updates, upgrades, enhancements, error corrections, and new versions are included within the license scope. For example, in some situations, if a client obtains a perpetual license to a software program, the client should consider requesting a new version of the software at no additional charge if the vendor transfers the program to a new operating environment. A client also should consider whether new software will need to integrate and be compatible with existing client systems.

Finally, as your client considers the general business deal, it must understand its exit strategy from a particular arrangement. No client wants to think about the end of the agreement at the beginning of the relationship, but advance planning in terms of a post-termination or post-expiration transition is essential. In particular, it is essential for the client to determine the procedures for transitioning its data and proprietary information to a new system. In this regard, your client should ensure that the contract does not permit the vendor to hold the client's data hostage (i.e., prevent the client from accessing its own data) due either to late or nonpayment or to termination of the

contract. The client always should have access to its data, especially if that data is used in making patient care decisions. This strategy reduces the number of problems your client may experience when transitioning to a new vendor for the same or similar products.

Agreement Triage—The Negotiation Process

Your client deals with a myriad of legal issues and agreements on a daily basis. Every client needs a solid procedure in place for review of its software and hardware agreements. A health care entity must decide how it will evaluate and negotiate an IT agreement with a vendor. Your client's consideration of the entire negotiation process will lead to a more satisfactory result. For example, if a vendor responds to an RFP, then the client should include all of the terms of the response in the definitive agreement or even consider including the response to the RFP as an exhibit to the agreement. Counsel also should consider the input of its client's board of directors and chief financial officers. Investment in new software and hardware technology can be a material investment for a client and counsel should anticipate these board and chief financial officer considerations as the client enters the negotiation process.

In some situations, the client's IT team may determine that it will simply review the document provided by the vendor. This may be appropriate for a statement of work or amendment that addresses a routine situation based upon an earlier negotiated and executed master license agreement.

In other situations, it may be appropriate for your client to have in-house counsel review and recommend revisions to the agreement. In other situations, it may make sense to include outside counsel to assist with these negotiations. An outside expert can provide a fresh perspective on the negotiation of a particular agreement. In any situation, the legal department and the chief information officer should determine when to introduce counsel into the negotiation process, if at all.

Legal Considerations

When entering the agreement review process, your client should consider many of the following legal provisions that often are included in health care IT agreements.

License Scope and Restrictions

One of the key aspects of a license agreement is determining the scope of the license and the identity of the end users. First, it is important to look at the definition of the "licensee" in the agreement to determine which entities within the corporate structure require access to the software, as well as the actual end users of that software, which can include employees, contractors, agents, or even patients. As counsel analyzes the scope of the agreement, it is important to address the companies that intend to use the software or hardware as well as the ultimate end users. Identifying the companies within the corporate structure that will use the software and hardware, as well as the end users that will use this technology, can have an important effect on the price your client will pay to the vendor for its technology. Your client also should analyze how the number of users will affect pricing methodology implemented by the vendor. The license agreement should address price-adjustment provisions in the event that your client's number of end users trend upwards or downwards during a particular period. Your client should consider this issue during the implementation process or the term of the agreement.

Clients should consider whether joint venture partners, outsourcers, or other third parties will be included within the definition of the licensee. Your client also must determine whether the software will be hosted on its own servers, or whether the vendor will provide the software remotely from its own servers or servers of a third party in a SAAS or cloud computing structure.

Another important element is the length of the software license's term. Obviously, this will depend primarily on whether your client is installing the software, which will often have a perpetual license, or whether your client is relying on SAAS or cloud services,

which will typically have a distinct term with renewals. As noted earlier, even if a software license is perpetual, the usage likely will be limited by the number of years of maintenance and support available for that software from the vendor. It is important either to secure a minimum number of years of maintenance and support for the installed software or have the ability to obtain a vendor's new software that may have similar levels of functionality to the old product. While it is certainly understandable for a vendor to have an "end-of-life" policy or sunset procedures, you should help your client protect its investment by demanding provisions that provide a sufficient period of use of the product.

In most situations, the software license will be non-exclusive, which is common in the software industry. Unless your client paid for exclusive access to a software application or paid for the development of that application, a software vendor typically wants to license its software to other competitors in the industry. One exception to this rule may be if your client requested custom developments to the software program. In that case, your client should request exclusive use of those customizations and, in some situations, potentially request ownership of the developments.

Your client also should determine the geographic scope and number of users for the software. Although it is less typical for health care entities to have an international presence, your client and you should discuss whether there are any potential international applications for the software. Even if your client only has offices in the United States, in certain circumstances your client may engage in research and development projects in other countries. If your client has international locations, there are many considerations beyond the scope of this Member Briefing that should be addressed, including international data security and privacy issues. If your client only has a presence in the United States, your primary concern is determining the number of users for your client as well as the identity of third-party users, as noted earlier.

While it is critical to properly define the scope of your client's license, it is equally critical to note the restrictions on the license agreement. Again, it is fair and reasonable for a vendor to demand certain restrictions. Your client's license agreement may contain restrictions such as the physical site of the license, the amount and type of end users of

the software, and whether there are any particular limitations on the number of backup copies of the software that may be used. You also should consider the locations from which the end users are accessing the software to ensure that the vendor understands your proposed usage. With respect to software as a service, there may be limitations as to the number of password-protected user accounts that a client may use. You should understand your client's current software and hardware needs and its anticipated future growth when negotiating license restrictions.

Many software vendors preclude licensees from providing third-party access to the software, including so-called "service bureau" access. Understandably, vendors want to preclude their licensees from providing software and hardware services downstream to multiple third parties. While the vendor's position is understandable, this limitation has important implications for health care entities that are contemplating an acquisition or a divestiture of the business. In particular, transition services agreements have become particularly controversial due to the number of mergers and acquisitions in the health care industry. Your client should understand the limitations placed upon the assignment of software, including any limitation on the ability of a health care entity to provide third-party services in a post-closing transition situation.

Although your client may not consider it important at the time of execution of the agreement, you must consider the importance of the transferability of the license to the software. Your client may enter into transactions involving reorganizations, spinouts, consolidations, asset sales, or stock purchases. Your client will want to ensure that it can freely transfer or assign its license rights as a part of such a transaction. In many instances, a vendor may not agree to remove these limitations from its agreement.

Implementation Considerations and Acceptance Testing

While proceeding from agreement execution to the go-live date for a software and hardware solution can be complicated for any company, the issues can be particularly acute for a health care entity. Patient safety is of paramount concern, and software downtime can result in significant care issues. Your client will need the agreement to

provide a clear roadmap for the installation of the software and hardware, including a clear demarcation as to the responsibilities of the parties during the installation. Data conversion from the previous vendor also might be part of that implementation process.

Most agreements include an implementation schedule. This schedule assists the parties in completing the project in a timely manner and helps the vendor understand the client's goals. When possible, the client should consider tying payments to the vendor on the satisfaction of certain thresholds as they are met during the implementation process.

Software agreements in the health care industry often include certain types of provisions that are less common in other industries. If employees and contractors of the vendor are onsite at a care facility during implementation, then the client may consider adding requirements that the vendor's team will comply with your client's internal procedures, including access, privacy, security, and health safety requirements. For example, a client might demand that all implementation team members submit to health tests, including tuberculosis, measles, hepatitis, chicken pox, or the mumps.

Some vendors will provide the software to the client before execution of the agreement to allow the client to evaluate the software in its facilities. In other situations, a client may take a site visit to another customer of the vendor. Most commonly, however, the client gets its first real view of the capabilities of the software once it can test the software in a live production environment.

Regardless of the situation, the client should request appropriate testing and acceptance procedures. Although each transaction is different, some variation of the following process is reasonable and necessary:

1. Following delivery and/or installation, with the assistance of the vendor, the client will conduct pre-live acceptance testing on the product, which should include a period for live processing.

2. During this process, the parties will work together to achieve go-live status for the product.

3. After the go-live date, the client will then conduct post-live acceptance testing of the product, which should include the use of actual data from the client's business operations in a production mode. This step of the process should prove that the product, together with any related products and interfaces, will operate in accordance with the documentation and specifications for the product. This step highlights the importance of adequately defining the functionalities and specifications for the product, as noted earlier.

4. Upon completion of the post-live acceptance testing, the client should then determine whether the product performed in accordance with the documentation and specifications. If the product passed the test, the client should notify the vendor that it has accepted the product. We typically recommend that the performance warranty period and any maintenance and support payment obligations should not commence until the client has accepted the product.

5. If the product does not pass the test, then the client should provide a written report to the vendor specifying the manner in which the product does not work satisfactorily.

6. The vendor should then have a limited amount of time to correct the issues included in the notice of rejection. If the vendor satisfies the issues such that the product passes the test, then the client should notify the vendor that it has accepted the product.

7. If the vendor fails to correct the issues, then the client can request that the vendor try again with the correction plan or, in certain circumstances, the client should have the right to terminate the agreement and receive a refund for all fees that it has paid to the vendor for the failed implementation.

Representations and Warranties; Disclaimers of Warranties

Although the issue is not peculiar to the health care industry, many health care software and hardware vendors do not provide a broad range of representations and warranties. In some situations, the limited nature of the warranties from a vendor may be appropriate. As a general rule, you should discuss some of the following representations and warranties with your client:

- *Title*—The vendor should represent and warrant that it owns the programs licensed to the client or has a right to sub-license any third-party software. The programs should be free of any liens or other encumbrances.

- *Non-infringement*—This representation and warranty should be included only if the agreement does not include an intellectual property infringement indemnification.

- *Program and hardware performance*—The vendor should represent and warrant that the program and hardware perform in conformance with the documentation and specifications for a period of 180 days after the final acceptance of the product.

- *Compatibility with other applications/systems, including any necessary interfaces*—The client may want the vendor to represent and warrant that the programs, interfaces, operating system, and any related diagnostic equipment will perform together as an integrated system.

- *Regulatory considerations*—While clients in other industries typically will request a representation and warranty that the vendor will comply with all applicable laws, health care entities should consider that general requirement as well as requiring compliance with specific health care regulations. These regulations can include American National Standards Institute standards, Health Level Seven standards (including the Clinical Context Object Workgroup standard for clinical

context management and Joint Commission standards), certification by the National Institute of Standards and Technology, compliance with Continuity of Care Record or Continuity of Care Document standards, standards established by Integrating the Healthcare Enterprise, and regulations of the U.S. Food and Drug Administration (FDA). In addition, even though this Member Briefing was written in 2015, a client should ensure that the software is Y2K compliant.

- *Viruses*—The vendor should represent and warrant that the software and hardware do not contain any lock, clock, timer, Trojan horse, Easter egg, time bomb, counter, copy protection feature, replication devices, defects, or other devices that might lock, disable, or erase a product or prevent the customer from fully utilizing the product.

- *Encryption*—Although this provision may not be required in every agreement, it is crucial that the client consider whether there will be any instances in which the vendor will store, handle, or control any of the client's proprietary information or, just as importantly, any patient information. If the vendor will store the client's data, the client should consider encrypting that stored data. Many recent security breaches and data privacy problems have resulted from stolen laptops, memory sticks, or other vendor equipment. For example, in 2013, Advocate Medical Group suffered a data breach affecting more than four million unencrypted patient records resulting from the theft of four laptops.[1] Cyberattacks also have led to catastrophic security breaches of protected health information (PHI). In January 2015, Anthem Blue Cross and Blue Shield discovered cyberattacks compromising the company's IT system that resulted in the attackers obtaining the personal information of more than 78 million customers.[2]

[1] Patrick Ouellette, *Advocate Medical Group Endures Massive Data Breach*, HEALTHIT SECURITY, (Feb. 26, 2015), http://healthitsecurity.com/2013/08/27/advocate-medical-group-endures-massive-data-breach/.
[2] *How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services*, ANTHEM, (Feb. 26, 2015), www.anthemfacts.com.

- *Quality of services*—This provision typically provides that the vendor will perform any professional services in a competent, professional, and workmanlike manner. These services can include development, implementation, maintenance, and support or other professional services.

- *Performance of third-party products*—The vendor should pass through to the client any representations and warranties provided by third-party product vendors. A client should make sure that the client may directly enforce any pass-through warranties.

- *Uptime and response time*—Depending on the circumstances of the transaction, a client might request representations and warranties as to the uptime requirements for the software and/or the time within which the program will receive and respond to a requested transaction.

- *Open-source software*—Due to the potential risks relating to some types of open-source software, the vendor should represent and warrant that the software does not include any open-source software or provide a list of any such software that is included in the licensed product.

- *Medical device*—The vendor should confirm whether any product is a safe medical device and whether the vendor is responsible for any necessary reporting to the FDA.

Your client also should consider the duration of the survival of these representations and warranties and, most importantly, the client's remedies for a vendor's breach of a representation and warranty. Simple re-performance by the vendor may not make your client whole in all situations.

The client also should understand that it is reasonable for a vendor to request a disclaimer for certain warranties. For example, a vendor may include a disclaimer of the implied warranties of non-infringement, merchantability, and fitness for a particular

purpose. Your client should note that it may receive protection for intellectual property infringement in the indemnification provisions. There may be further disclaimers for clients based on unauthorized modifications of the software or hardware by the client or the use of that software or hardware in a non-approved operating environment. Finally, there may be another disclaimer for any warranties in a situation where the client has exceeded the scope of use of the license grant.

Regulatory Compliance; Disaster Recovery; Audits and Certifications

In addition to the representation and warranty regarding general compliance with laws by the vendor, clients should consider including many other health care regulatory covenants in the agreement. It is unlikely that you will need to include every health care regulation in the agreement. That said, while this Member Briefing cannot cover each such regulatory consideration, we typically advise our clients to consider at least the following more common vendor covenants:

- *Standards of Business Conduct*—The vendor should attest to fulfilling its obligations under the agreement in accordance with any established client organizational program or standards of business conduct. Violation of the standards of business conduct (e.g., corporate compliance plan) by an employee or agent of the vendor should serve as cause for termination of the agreement by the client.

- *Participation in Medicare and Medicaid or Other Federal Programs*—The vendor should represent that neither it nor any of its employees, agents, shareholders, officers, or directors have ever been excluded from participation in Medicare, Medicaid, or other federal health programs. In addition, the vendor should state that it is not under any current or pending investigations, and the vendor should agree to notify the client immediately upon the commencement of any such investigations or exclusion proceedings.

- *Debarment*—The vendor should state that it has not been convicted of a criminal offense related to health care and that the vendor is not currently listed as debarred by a federal agency.

- *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*—To demonstrate that it adequately safeguards the privacy and security of all individually identifiable health information obtained from or created for customers, the vendor should represent that it fully complies with HIPAA,[3] as amended by the Health Information Technology for Economic and Clinical Health Act. In this regard, if the vendor either will maintain PHI on behalf of the client or have access to the client's PHI onsite or remotely while performing its support services, the client and the vendor should execute an appropriate business associate agreement.

- *Discount Safe Harbor*—Where applicable, in order to comply with the Anti-Kickback Statute, the vendor should warrant that it will comply with the Discount Safe Harbor.[4]

- *Access to Books, Documents, and Records*—Where the client is a hospital or other entity that files a Medicare cost report, the vendor must grant the Comptroller General, the Secretary of the U.S. Department of Health and Human Services, and their duly authorized representatives access to review any and all books, documents, and records as may be necessary to certify the costs of services in excess of $10,000 per year until four years after the agreement has expired.[5]

- *Healthcare Common Procedure Coding System (HCPCS) Codes for Medicare Reporting*—If applicable, a client may request that the vendor provide all HCPCS

[3] Pub. L. No. 104-191, 110 Stat. 1936 (1996).
[4] 42 C.F.R. § 1001.952(h).
[5] 42 U.S.C. § 1395x(v)(1(I); 42 C.F.R. § 420.300-.304.

Codes recognized by Medicare for all vendor products as well as cross-reference each HCPCS Code by the vendor's name, identification number, and product catalog number.

- *Business Continuity/Disaster Recovery Plans*—To account for the possibility of a disaster and ensure that the vendor established a disaster recovery plan, the client should request the vendor's written business continuity and disaster recovery plan. The client should review this plan and require that it be consistent with industry best practices. Due to the experience of many health care entities over the past few years, you also should consider the allocation of expenses between the parties relating to disaster recovery matters or data security breaches. The client also should request that the vendor test all essential components of the plan on a quarterly basis.

- *Statement on Standards for Attestation Engagements (SSAE) 16/Service Organization Control 2 Audits and Reports*—The client may want the vendor to obtain a third-party review of its systems and applications related to the vendor's products and services on an annual basis by independent auditors in accordance with SSAE16 or other accepted accounting standards then in effect. The client either can require the vendor to automatically provide the client with those reports or do so upon the client's request.

Indemnification; Limitation of Liability; Insurance

While provisions regarding limitations of liability, indemnification, and insurance are important, a detailed analysis of these issues merits a separate article.

Various types of indemnification obligations are included in IT agreements, ranging from the parties agreeing to defend, indemnify, and hold each other harmless for losses arising out of the contract to the vendor's replacement of infringing products due to intellectual property infringement. The client should request broad indemnification rights

for intellectual property infringement by the vendor's products. The vendor may provide this type of indemnification, but it also may request exclusions from indemnification if the client: (1) combines the vendor's products with third-party products; (2) modifies the product and that modification makes the product infringing; (3) uses the product outside the scope of the agreement; or (4) continues to use the product after the vendor notifies the client to cease using the product. In addition, the parties should include a process for notification by one party to the other if one party is claiming indemnification from the other party.

There is a wide range of possibilities for the limitation of liability provision. Most agreements do not provide for unlimited liability for either party. Often, a vendor will want to limit the direct damages to the amounts paid by the client under the agreement over the previous 12 months. The client may want to set the limitation of liability at an amount not to exceed the vendor's insurance limits as provided in the insurance section (discussed below). It also is fairly typical to include a mutual limitation of liability for incidental, indirect, consequential, or special damages. Other examples can include a provision that the vendor limits its liability for medical services provided by the client and that nothing in a software program or SAAS application will be deemed to be medical advice to the health care entity.

Your client also should consider exceptions to the limitation of liability provision. For example, the client may want to ask for unlimited liability for: (1) indemnification obligations; (2) breaches of confidentiality; (3) personal injury or property damage caused by the act or failure to act of a party; or (4) the gross negligence, intentional misconduct, or violations of law by a party's employee or agent. It is essential to consider an exception to the limitation of liability provision for breaches of confidentiality, because the liability arising from these incidents can include significant monetary consequences that can substantially exceed typical vendor limits.

The client should require the vendor to maintain appropriate levels of insurance. General requirements for insurance may include having the vendor: (1) name the client as an additional insured; (2) provide notification to the client prior to cancellation of insurance affecting the client; (3) obtain insurance from a carrier with an "A" A.M. Best

rating; or (4) provide an endorsement to include a waiver of subrogation in favor of the client. The types of insurance that a client may request are: (1) commercial general liability insurance to cover bodily injury and property damage to third parties; (2) worker's compensation insurance; (3) commercial automobile liability insurance; (4) umbrella liability insurance; and (5) cyber insurance. If the parties tie the limitation of liability to insurance coverage limits, the agreement should require that the coverage amounts are appropriate.

Maintenance and Support

This Member Briefing covered several considerations for your client with respect to maintenance and support. Your client also should consider including some of the following provisions in the software and hardware maintenance and support terms:

- No payment of maintenance and support until the client's final acceptance of the product.

- A minimum term of five years of maintenance and support for the purchased product and for such longer term as the vendor is supporting the product for another customer.

- Including source code escrow provisions in the event of cessation of maintenance and support.

- A cap on annual increases of the maintenance and support fees.

- Availability of general support during normal business hours and, due to the nature of business for many health care entities, 24/7/365 emergency support provisions.

- Providing a framework for the deadline for a vendor response based on the severity level of the errors in the program.

- Including credits for the client upon the occurrence of errors that are of a high severity level or chronic problems for the software at lower severity levels.

- The regular provision to the client of all upgrades, updates, enhancements, and error corrections and all necessary installation and training assistance that the client may need. This requirement should include any such revisions that ensure that the program complies at all times with any federal, state, and local health care laws.

- So long as the client is current on its maintenance and support fees, the right to exchange a program for another vendor program that includes similar functionalities, at no cost to the client.

Other Considerations

Software and Mobile Application Development

As noted earlier, a client may require modifications or new interfaces to use a vendor's software in the client's facilities. There may be other situations in which the client wants a third party to develop a completely new software application or mobile health care application to be owned exclusively by the client. In the case of custom software development, it is essential to establish the scope and timing of the deliverables from the developer. For example, will the developer provide the development on a fixed fee or will it charge an hourly rate for development? If the developer charges an hourly rate, the parties should discuss who takes the risk, including the monetary costs of that risk, for any overages on the hourly fee estimate.

As is the case for licensed software, your client must develop a description of the desired specifications for the developed software, the timeline for delivery by the

developer, and acceptance and testing procedures. We recommend that the client structure the procedure for the acceptance of deliverables as noted above and consider tying payments to previously established milestones as they are satisfied by the developer.

Your client should ensure that the parties clearly understand the ownership of the intellectual property underlying the developed software. In particular, there may be situations in which the base software is used by the developer for software development with other parties. If that is the case, the parties should clearly identify the substance of the base software. This will make it easier to identify the new developments provided by the developer. In most situations, your clients will own the intellectual property relating to the developed software.

Your client also should determine whether these new developments will be licensed back to the developer. In most situations, we recommend that clients do not allow such a license back to the developer in order to avoid the potential sub-license of that intellectual property to a third-party competitor.

Use of Mobile Applications and Cloud Computing

Finally, your client should consider the increasing popularity of using mobile applications and cloud computing services in the health care industry. In addition to the privacy and security concerns relating to PHI and HIPAA compliance, your client should also address how these forms of software delivery work with the rest of its IT structure. We highly recommend two recent AHLA articles for your consideration and review: (1) “A Proactive Approach to Cloud Computing in the Healthcare Industry,” which is from the June 2013 issue of *AHLA Connections*; and (2) “There’s an App for That! Should Health Care Organizations Embrace the Mobile Revolution?,” which is from the May 2014 issue of *AHLA Connections*. Each of these articles provides an excellent introduction to the issues surrounding your client’s use of mobile applications and cloud computing technology.

Conclusion

Your client's goal is to have an efficient and integrated IT system that enhances its ability to deliver quality patient care and otherwise run its business. Counsel's primary role is to help its client achieve that goal. Communication between counsel and the client's IT staff will improve the client's results. While this Member Briefing covered many of the essential issues in IT agreements, there is no substitute for counseling your client prior to the execution of the agreement, advising your client during the term of the agreement, and assisting the client as it transitions to a new vendor.

The work required to successfully negotiate IT agreements for your client may seem tedious or even redundant, but the attention you give to the details during negotiations will help avoid unpleasant surprises after the ink is dry on the contract. When your client's chief executive officer calls you at 10:30 P.M. on a Tuesday with a potential problem, you will be glad that you did all you could to put your client in the best possible position to resolve the problem on favorable terms.