Gaining Contract Advantage with EHR Vendors

Using Contract Provisions to Protect Your Organization and Create Successful Vendor Partnerships

BY STEVEN J. FOX AND VADIM SCHICK

With the American Reinvestment and Recovery Act/Health Information Technology for Economic and Clinical Health (ARRA-HITECH) Act incentives expiring in just a few years, healthcare providers will likely get only one chance to qualify for the full amount of incentive payments. Thus, successful installation and operation of an electronic health record (EHR) system by the vendor becomes critical to each healthcare organization trying to achieve meaningful use. Therefore, EHR contracts must include adequate protections, safeguards, and other rights reserved for the customer, in the event that the vendor defaults or otherwise fails to perform to the provider's satisfaction. This article provides a sampling of, though by no measure all, such protections and safeguards, along with some valuable suggestions for negotiating a fair deal for both parties.
GETTING STARTED

Prior to even looking at the vendor's contract, it is important to remember that everything is negotiable, and that includes price, payment terms, limitations of liability, and warranties. This fact is too often ignored. Also, some providers make the mistake of advising a vendor that it has either been selected as the winner of the request for proposal (RFP) process or that it is the "vendor of choice," and all that remains is to enter into a contract. That is a sure-fire method to undermine one's bargaining position.

It is much more effective to select the top two vendors, then advise the preferred vendor that if negotiations break down or do not go as expected, the second choice is waiting in the wings. In some cases, a dual-track negotiation process may even be worthwhile. These methods tend to keep the pressure on the preferred vendor and generate additional concessions. Nevertheless, both parties should aim for a win-win deal and keep in mind that the purchaser and vendor will have to work together in the future for an extended period of time.

IT IS ESSENTIAL TO DETERMINE THE CORRECT TYPE OF LICENSE FOR THE ORGANIZATION'S PARTICULAR NEEDS AND PROPOSED USE, THERE IS NO SUCH THING AS A 'STANDARD' LICENSE.

LICENSE

It is essential to determine the correct type of license for the organization's particular needs and proposed use. There is no such thing as a "standard" license. For example, there are shrink-wrap licenses, typically used for off-the-shelf software; site licenses, covering a specific geographical location; enterprise-wide licenses, encompassing an entire business or institution; named user or concurrent user licenses; and application service provider (ASP) or software as a service (SaaS) licenses (also known as "cloud" licenses), governing the right to use software on a subscription-type basis. Each of these and concurrent users instead of name users? If so, negotiate additional license fees up front, rather than agreeing to pay "then current" fees in the future. Is any third-party software included in the system that may necessitate a sub-license? If all of these issues are not addressed properly, this could lead to significant problems during the term of the agreement.

CONFIDENTIALITY, PRIVACY, AND SECURITY

Another set of hidden dangers relates to confidentiality and proprietary rights. Most of the boilerplate contract terms protect the vendor's trade secrets and restrict access to the software. However, it is less common to find similar protections for the purchaser's confidential and proprietary information. Insist on mutual confidentiality obligations with strict limitations on the vendor's use of the organization's patient information.

This is especially important in light of the substantial changes to the existing Health Insurance Portability and Accountability Act (HIPAA) regime, as mandated by the HITECH Act and the accompanying regulations. Privacy and security issues are directly related to a provider's ability to amend and/or terminate the contract for a vendor's failure to comply with applicable laws; fair allocation of compliance costs and requirements for vendors to enter into business associate agreements, where applicable.

WARRANTIES

Most vendors provide minimal to nonexistent warranties in their form contracts. It is crucial for providers to include these kinds of warranties: system compliance with functional and performance specifications; compatibility of components; viruses and disabling devices; prevention of unauthorized access or usage of system; sunset protection; availability of support/maintenance; vendor replacement of third party software; regulatory compliance; interoperability; service levels; personnel qualifications; transition, along with many other important issues.

If the vendor's product is essential to achieving meaningful use, then it should also warrant to fully cooperate with the provider to enable it to achieve meaningful use. The vendor should warrant that its product is and will remain certified by one of the Office of the National Coordinator for Health Information Technology (ONC) Authorized Testing and Certification Bodies.

Considering the compressed timelines for qualifying for the maximum incentive payments, a vendor's breach of these warranties would have a significant negative finan-
cial impact on the customer. Therefore, if a healthcare provider fails to qualify for the HITECH incentive payments because of its vendor's failure to obtain certification, inability to deliver products that enable the provider to achieve the necessary measures and objectives, remain certified or cooperate fully with its customer, the provider should be entitled to a refund of all fees paid to the vendor under the agreement and possibly additional damages as well. This will represent one of the most difficult areas to negotiate.

**LIMITATION OF LIABILITY AND INDEMNIFICATION**

The limitation of liability (LoL) clause is often the most contentious areas of negotiation. However, failure to adequately address this may result in the inability to recover or even claim damages for actual losses suffered as a result of breach of contract or negligence by the vendor. It is essential to "carve out" a number of areas from the LoL's operation, including breach of confidentiality and privacy (including breach notification expenses under HIPAA); personal injury, death and property damage; intellectual property infringement; and, if possible, the vendor’s breach resulting in the provider’s failure to achieve meaningful use in a timely manner.

A good contract should also contain strong indemnification provisions and warranties. The indemnification should protect the purchaser from HIPAA and privacy/confidentiality viola-

**THE LIMITATION OF LIABILITY CLAUSE IS OFTEN THE MOST CONTENTIOUS AREAS OF NEGOTIATION. HOWEVER, FAILURE TO ADEQUATELY ADDRESS THIS MAY RESULT IN THE INABILITY TO RECOVER OR EVEN CLAIM DAMAGES FOR ACTUAL LOSSES SUFFERED AS A RESULT OF BREACH OF CONTRACT OR NEGLIGENCE BY THE VENDOR.**

...tions by the vendor; third party claims for bodily harm, injury or death caused by the vendor’s personnel or software; as well as claims that the software infringes on third party patents, trademarks or copyrights, or misappropriates trade secrets.

Most troubling, perhaps, are the indemnification obligations imposed by vendors on provider-customers. It is not uncommon for vendors to require customers to indemnify them for any third-party claims brought against the vendor as a result of the vendor-provider relationship, even when the claims arise from the vendor’s own fault or negligence. Agreeing to such a provision could be disastrous for providers whose existing contracts with malpractice insurance carriers may exclude such indemnifying arrangements from coverage. In other words, if a provider agrees to indemnify one’s EHR vendor, and incurs damages as a result of this obligation, that provider’s malpractice insurance company may refuse to cover such damages.

**TESTING AND ACCEPTANCE**

The agreement for implementation of an EHR system or other technology required for achieving meaningful use and qualifying for the ARRA incentive payments should include comprehensive acceptance testing procedures, a methodology and remedies for failure to achieve successful acceptance testing, including but not limited to a refund of all monies paid. However, such a refund remedy will leave the customer without a means of achieving meaningful use, and, therefore, unable to collect the incentive payments. Thus, a healthcare provider should consider whether a vendor’s failure in this context should warrant additional or alternative damages, as described above.

**PRICING AND PAYMENT TERMS**

In reference to payment terms, it is best to negotiate objectively measurable performance milestones that the vendor must achieve before payment is required, rather than the standard calendar or time-based milestones common in vendor contracts. These milestones should be coordinated with detailed acceptance testing criteria. For example, 10 percent of the contract price may be paid upon execution, 20 percent upon delivery, 30 percent upon completion of installation, and the remaining 40 percent upon final acceptance.

However, be aware that vendors are increasingly resisting the use of objective milestones, often resting their position on revenue recognition rules. It is strongly recommended to resist giving in on this issue and the use of carefully drafted performance milestones is highly encouraged. Otherwise, the form contract may require the majority of the purchase price and license fees to be paid before the purchaser is satisfied that the software performs as warranted.

(Continued on p. 60)
TERMINATION RIGHTS
Vendors should not be able to terminate the contract, except for a very serious breach by the customer. Even if such a breach occurs, the agreement should provide the customer with plenty of time to cure the breach and require the vendor to notify multiple executives and representatives of the breaching party. On the other hand, make sure there are adequate provisions for terminating the agreement if the vendor is in breach. In addition, it is imperative to include transition terms, to permit an orderly transition from one vendor’s product to a replacement.

VENDOR FINANCING
Some vendors offer financing both for traditional software and equipment products as well as ASP, remote hosting, cloud, and SaaS models of their EHR systems. These subscription-type models pose a few significant additional risks to healthcare providers, especially in vendor-financed transactions. One of the biggest disadvantages for healthcare providers using these models for their EHR systems is that such customers have no actual access to, or possession of, their data, independent of the vendor. Thus, there is a real concern about the vendor’s ability to hold its customer’s data hostage (e.g., because of a payment dispute), or concerns arising if the vendor ceases business operations altogether.

In vendor-financed deals, this concern multiplies the already large disparity in leverage between the healthcare client and the larger, wealthier technology vendor, which is also financing this transaction. Therefore, customers need to negotiate broad protections and rights to access their data in such deals, including: barring vendors from ever holding customer information, including protected health information (PHI), hostage (i.e., denying customer access to such data); mandating regular backups of data; and explicit provisions regarding return of any customer data, including PHI, to the customer upon termination of the agreement, especially if the agreement is terminated due to the vendor going out of business.

MUTUALLY BENEFICIAL CONTRACTS
The acquisition process for health IT systems is generally complex, intensive, and critically important to all of the participants. However, if the concepts described above are used, the ultimate outcome is likely to be a contract that protects the provider and benefits both parties by creating a mutually beneficial and sustainable partnership.

Steven J. Fox is a partner, and Vadim Schick is an associate, in the Washington, D.C. office of Post & Schell, P.C. Fox is chair of the law firm’s Information Technology Group and co-chair of its Data Protection Group. Fox and Schick focus on health information technology agreements and data privacy and security compliance.

Don’t miss your chance to be listed in the Healthcare Informatics 100, one of our most popular issues!

For the past 20 years, Healthcare Informatics has been ranking the 100 vendors with the highest revenues derived from healthcare IT products and services earned in the U.S. based on revenue information from the previous year.

The Healthcare Informatics 100 list provides readers with a unique information resource and financial overview of vendors active in the healthcare IT market. Healthcare Informatics relies on companies to provide self-reported revenues, but in some instances estimates are listed.

To ensure that your company is considered for the HCI 100, please be sure to fill out the online survey posted on www.healthcare-informatics.com from March 1 – April 1.