BakerHostetler

Evolving Issues for Healthcare IT Contracting

By: Alan L. Friel

This client advisory is based in part on an article appearing in *FierceHealthIT.*

The emergence of mega-suite vendors, more use of the cloud, increases in data breach frequency and cost and big data privacy impacts make healthcare IT (HIT) vendor arrangements more complex, and solid agreements with HIT vendors more important than ever. Addressing key legal and business issues during the RFP and contracting process reduce healthcare providers' risks and help minimize expensive change orders. Here are tips for doing so:

Develop and Follow a Roadmap

Healthcare providers have complex IT needs. Further, as modern healthcare organizations (HCOs) develop more integrated HIT systems, they are increasingly turning to consultants to develop overall HIT strategic plans, which may include engaging a primary "mega-suite" vendor (some consultants are getting into this business themselves) to outsource development, implementation, scalability and operation of myriad HIT product and service portfolios through multi-vendor supply chains. A strategic roadmap will help in managing electronic health records, revenue cycle management, patient access and care tools, analytics and reporting systems and data processing and storage over time. Whether the HCO executes the plan by directly contracting with and coordinating multiple vendors, or relying on a mega-suite vendor, care needs to be taken in structuring and documenting the parties' rights, obligations and remedies to help avoid vendor problems and disputes, and to better manage them when they occur. As new HIT services and vendors are added over time, the roadmap should also help guide system-wide interoperability and functionality requirements.

Use the RFP Process Wisely

While RFPs can be time-consuming, the RFP process is an opportunity to pre-establish desired deliverables, including material legal term expectations, as well as to undertake due diligence on the vendor's track record, its data protection and service continuity programs and controls and its relevant resources and capabilities. This is particularly important regarding data privacy and security since vendor risk assessment prior to engagement, with appropriate controls documented in the service agreement, is crucial to an HCO meeting its own obligation to have and follow a defendable and appropriate risk assessment and corresponding program. Chief Information Officers should work together with legal and IT risk management to develop RFP parameters that set the stage for strong contractual protections for the HCO when the vendor relationship is formed and documented. Vendor references should also be requested and checked. Trial licenses may be available and helpful in evaluating which products and services

to select based on performance and interoperability. Also consider simultaneously negotiating with the two top RFP respondents so you are not stuck if the agreement negotiation does not yield commitments to the expectations that were called for in the RFP, or at least have a second choice you can turn to if negotiations with the first choice fall apart. Finally, as the standard agreements for HIT vendors are weighted heavily in the vendor's favor, ask for a version with the "gives" that have been agreed to with other HCOs in comparable transactions. Occasionally, where a deal is very significant in spend, you can even get some sort of favored nation commitment on certain key terms.

Carefully Scope the Fees, Services, Deliverables and Dependencies

The scope of the services and technology licenses, as well as the deliverables specifications and any interoperability, scalability and interface requirements, and any permitted dependencies that limit the vendor's responsibilities, are material business points that should have been called out in the RFP. At minimum, they need to be carefully articulated in the agreement, and the definition of key elements such as authorized users, facilities, supported equipment, third-party equipment, product, services, support services, vendor software, third-party software, components, modules, interfaces, specifications, documentation, interoperability, releases, updates, upgrades, versions, enhancements, and material changes are crucial, and determine what will be delivered for the contracted price and what the vendor will be responsible for or not. In some cases, third-party standards can be used to set element definitions, such as the definition of interoperability established by the Health Information Management Systems Society or by the Institute for Electrical and Electronic Engineering, the standards your existing systems operate on and applicable Health Information Exchange requirements.

The fees for the various services and deliverables should also be well defined, advisably with renewal term increases pre-determined. Beware of hidden fees and add-ons, such as implementation fees related to "free" enhancement or updates. A change order process should also be agreed upon to address inevitable changed circumstances and is preferable to set the basis for rates for change orders in advance as opposed to then-current market rates.

Pay particular attention to dependencies outside of the HCO's control that limit the vendor's responsibility, such as third-party equipment or software changes, which may result in additional costs to the HCO and/or be exclusions to the vendors' interoperability and/or warranty or maintenance obligations. If the vendor is relying on third-party solutions for interoperability with other technology, try to make the vendor contractually responsible for that.

Obtain assurances that the vendor will be timely compliant with known and projected regulatory obligations that affect HIT systems, such as ICD-10, and build in a reasonable manner to accommodate unforeseen government or insurance industry mandates. Also address scalability as the HCO's needs may increase or decrease over the life of the system, and how fees and services will be revised accordingly.

Work out the details of implementation, including schedule and training. Consider if there needs to be integration with systems that will be replaced and detail the vendor's obligations regarding that conversion. Ensure that there will be adequate customer support, and additional future training as may be desired, and the cost therefor.

Finally, look closely at all the related agreements and governing documents that can affect the engagement, which may include end-user licenses agreements, master services agreements, work orders, bills of material, service level agreements, maintenance agreements, hosting

agreements, development agreements, various specifications documents and addenda, user guides and operating manuals, and even travel policies. Collateral agreements and documents can materially impact the main agreement and the parties' obligations.

Build Flexibility into Licenses and Consider Ownership of New IP

The license should be as broad as possible, including as to permitted users, equipment, facilities and territory, and should be applicable to affiliates and assignable in a merger or change of control. It is a good idea to specify that the fees for expanding the license in the future and to try to limit the remedy for exceeding a license, especially if inadvertently, to those additional license fee rates.

If custom software is being developed, articulate who owns it and what the non-owner can do with the new intellectual property. Even where the HCO owns the new intellectual property, it is likely to be derivative of vendor and third-party materials and dependent upon the continued ability to use and update them, which will need to be addressed. If the HCO is expecting to obtain proprietary deliverables it owns and controls, it also needs to consider how use of open-source software in the creation of those deliverables may result in the derivative software being required to be made available to the open-source community, and thus may want to restrict use of "copyleft" software.

Also consider providing for the possibility that the vendor does not remain financially or otherwise able to fulfill its obligations, and could even go out of business, and address these risks through appropriate insolvency provisions, and potentially take over rights with software code and developer manuals held with a commercial software escrow that the HCO can access upon a triggering event.

Plan for Changes, Transitions and Termination

Obtain termination rights for material breaches, chronic service failures, undesired vendor changes and changes in your circumstances and legal obligations. Try for a termination for convenience right, even if it includes a reasonable kill fee. Provide for an orderly exit process on termination, including appropriate transition support and data delivery or destruction, and establish the cost thereof.

Address Data Protection

HIT programs necessarily generate and/or process, store and transfer data. First, agreements need to establish who owns what data as between the parties, and who can use what data for what purposes. This has regulatory data privacy and security implications discussed below. In addition, a HCO should require that all its data be exportable upon demand on usable formats. A negotiated point will be what, if any, additional charges the vendor may impose for doing so. The contract needs to specify what data is to be available, and on what basis, which may require consultation with the HCO's clinicians for services related to clinical care. Contracts need to provide for the retention and destruction of data consistent with the HCO's information governance policies and needs, and particularly when vendors and/or their sub-suppliers are no longer performing services.

HCOs have a host of privacy and data security obligations that will apply to their HIT service providers, including regarding personally identifiable information of employees and consumers,

credit card data, and protected healthcare information (i.e., most individually identifiable health information held by entities subject to state and federal healthcare privacy and security laws) (PHI). The HCO is ultimately responsible to the data subjects and regulators for its vendors. The HCO's overall data risk assessment should be applied to each vendor, the vendor's policies and practices assessed and the vendor appropriately contractually obligated. In addition, information governance obligations should be specified, including data segregation, residency, redundancy and backup obligations and response times for providing access to or delivering stored data, and in what formats, and for its retention and destruction and certification of destruction. Residency is particularly important for cloud services and other outsourced processing and storage, since many countries outside of the U.S. prohibit data access from, or transfer to, the U.S. absent commitments that exceed U.S. legal standards, even if the data originated from the U.S. Consider addressing redundancy and backup by permitting the HCO to periodically backup its data on its own, or another vendor's, servers, or in the case of mega-suite vendors requiring them to multi-source this task with its sub-suppliers.

Under HIPAA (Health Insurance Portability and Accountability Act), as supplemented by HITECH (Health Information Technology for Economic and Clinical Health Act), a party with data transmission to or from a covered entity (or its business associates), with routine access to PHI, is a "business associate" subject to privacy and security obligations with regard to PHI. An appropriate business associate agreement (BAA) setting forth its privacy and security obligations as to the PHI, including what it can do with PHI and how it will secure it, is a necessary part of the vendor engagement, any breach of which should be a material breach of the vendor agreement that is not subject to limitations of liabilities or damages. Mega-vendors should be required to have a form of BAA that meets defined standards signed by its sub-suppliers, and should remain ultimately liable for any breaches by their sub-suppliers. Although HIPAA allows for covered entities to disclose PHI to business associates for the purpose of de-identifying it to HIPAA de-identification standards (including limiting re-identification), which would render no longer PHI and then subject to expanded use by the vendor, care should be taken in defining the de-identification obligations. Further, if it is the vendor accessing PHI and doing the de-identification itself, rather than receiving de-identified data sets, accepting a payment or even a discount in exchange for PHI access for purposes unrelated to performing necessary services for the covered entity would seem to violate HIPAA's prohibition on remuneration for PHI, absent a defined exception that apply to other situations (e.g., cost-reimbursement of sending prescription refill reminders). In addition, as state and federal medical data privacy and data security laws are evolving, with new state legislation introduced frequently and enacted not irregularly, the vendor's data rights and obligations need to be subject to future applicable law, and the HCO should have the ability to restrict usage and increase obligations in the future if it deems so necessary or otherwise appropriate.

HCOs have notification obligations to data subjects and regulators under federal and state law in the event of a data security breach of unsecured PHI, and accordingly the vendor agreements need to provide for vendors to give the HCO immediate notice of suspected incidents and spell out the vendors' cooperation and remediation obligations.

Where a mega-suite vendor has been engaged, HCOs need to keep in mind that they, not the master vendor, remain ultimately responsible for conducting a HIPAA / HITECH risk assessment of using a multi-vendor supply chain and having the mega-suite vendor implement the controls deemed necessary by the HCO throughout that multi-vendor supply chain. Transparency and contractual standards on how subcontractors and other suppliers and service providers are selected, engaged and monitored is recommended. Even for a single-source vendor, contracts should require that the vendor workforce with access to the HCO's data is

limited, except as necessary to perform the services and that staff is responsibly selected, appropriately trained and effectively monitored and managed.

Agreements need to accommodate for evolving compliance obligations and vulnerabilities not yet contemplated by allowing for the addition of additional controls and obligations, or the ability to terminate.

Establish Milestone, Testing, Approval and Revision Terms

Performance and fees can be broken into deliverable obligations at various milestones, including scoping, development, acceptance, installation, training, implementation, go-live and operation and maintenance periods. Each milestones can have detailed deliverable specifications and a submission, testing and acceptance process can be established. The HCO should have the right to request revisions until acceptance is obtained, and the ability to terminate for cause if acceptance cannot be timely obtained with minimal revisions. Penalties can also be provided in the event of schedule delays in meeting milestones. Consider also an ability to terminate without cause at each milestone, which can sometimes come with a kill fee.

Obtain Guarantees and Warranties, Provide for Maintenance and Service Levels, and Consider Enhancements

The agreement should establish minimum acceptable levels of service consistent with detailed specifications and free of material errors or downtime other than during established regularly scheduled maintenance (during appropriate dates and times where usage is minimal). Following a typically limited warranty period, a maintenance contract may be required to continue the service level commitment. Beware of exclusions to maintenance obligations. Maintenance should include doing everything necessary to maintain compatibility with crucial third-party equipment and software, as such may change or be updated or enhanced. Maintenance contracts can also include making additional enhancements and improvements, especially up to a certain time allotment not otherwise used to perform routine maintenance. This is advisable to address changes to the HCO's HIT environment, which is likely to expand and change over time. Beyond any allotted time for this have the contact set a predetermined cost for additional work.

A service level guaranty should spell out how acceptable service and downtime will be measured, ways the vendor will minimize service outages, how problems are reported and managed, the minimum time for the vendor to respond to and solve differing levels of problems and provide for credits for failures and a termination right for chronic failures. The more critical the system, the higher the service level commitment should be and the more severe the remedies for failing to meet it. For mega-suite vendors, the vendor's service levels should apply to all of its sub-supplies, though the mega-suite vendor should be ultimately responsible. One value of a multi-vendor supply chain managed by a master vendor may be the vendor's ability to rapidly move services to another sub-supplier in the event of a problem and that can be established as response obligation. Dedicated contact persons or numbers available 24/7 are recommended, as is a ticketing system and regular reporting on ticket status while service is being remedied.

The HCO should seek the service warranty to include compliance with functional, performance, and compatibility specifications, virus and malware protection, and prevention of unauthorized access or use. Beyond a basic service warranty and service level guarantees, additional

warranties related to compliance obligations, non-infringement, confidentiality and interoperability can be negotiated. Copies of vendor data protection and breach response, business continuity management and disaster recovery, information governance and other relevant policies and processes can be attached as exhibits to agreements and the vendor can represent and warrant that it will follow them throughout the term, with material changes subject to approval, and comply with all applicable laws as well as specifically articulated key contractual obligations, including the BAA terms.

Negotiate the Liability, Remedies, Insurance and Indemnity Terms

Contracts need to clarify which party is responsible under what circumstances for what with respect to compliance with law, third-party infringement claims and data protection. This can get nuanced depending on what each party is contributing and doing. For instance, both parties may be contributing software, content and data, for which they should be responsible for to the extent it is used by the other as permitted. Vendors typically want to exclude liability for clinical decisions based on erroneous data, though that can be countered by limiting the exclusion to where data errors do not arise out of failure to meet certain performance and testing requirements or from gross negligence or intentional misconduct.

Remedies limited to fees paid to the vendor (often for a partial look-back such as 12 months) offer inadequate protection for continuity, data protection and integrity, compliance with law and intellectual property infringement risks, for failure to fulfill confidentiality obligations and for patient harm or death arising out of failure of the vendor to meet a defined standard and/or certain defined obligations. Damages arising out the vendor's breach of representations, warranties and obligations related to those matters should ideally not be capped or subject to other damages limitations. This is often one of the most hotly negotiated points, with the vendor arguing that the pricing assumes that it will have limited liability and the HCO countering that the vendor must be stand behind its core obligations. Where the lines are drawn will depend on leverage, and accordingly setting expectations on these issues as part of the RFP can help minimize the negotiations.

Some intellectual property infringement and errors and omissions risk, and increasingly data privacy and security incident risk, maybe insured by vendors, and agreements can require certain specified types and levels of coverage be maintained with the HCO added as a named additional insured (with any insureds dispute exclusion not applicable). The HCO can itself insure against the risk of data loss, damage or compromise, but policy terms need to be carefully checked as exclusions and limitations can affect the practical value of such coverage. It is recommended that HCO's policies pre-qualify the HCO's law firm of choice (and its rates) as acceptable under defense and incident response coverage.

Establish Oversight, Including Self-Auditing

Ideally, contracts will provide for audit rights. For some large providers that resist such oversight, and for mega-suite vendors who undertake contractual responsibility for a multi-vendor supply chain, self-assessment and certification should be considered. Where appropriate, require copies of vendor audits (e.g., SOC 2 / SOC 3), certifications (e.g., ISO 27001, FedRamp, etc.) and self-certifications (PCI-SAQ, EU Safe harbor, etc.) and evaluate the vendor's ongoing risk profile. These types of requirements should be specified as a deliverables in the RFP. Many vendors have existing self-assessment and certification programs that can be reviewed for adequacy during the RFP process.

Vendors may also want audit rights to ensure the licenses are not being exceeded. Such inspection rights should be at vendor's cost (absent significant finding of infringement) and reasonably limited not to interfere with the HCO's business or systems.

Keep Mergers in Mind

Mergers, acquisitions and divestitures can require that the parties HIT systems be shared during a transition period, typically through an information technology transition agreement, and then some legacy systems and vendors phased out. Standard vendor agreements often require approval of assignments, which should not be the case for a HCO's assets sale, merger or change of control. HCOs also need the ability to make vendor agreements available for review as part of potential transaction due diligence, so that should be carved out of the confidentiality provisions. Finally, as such a transaction may result in the jettisoning of some HIT systems and service providers after an initial transition period, it is advisable that such a transaction provides the basis in the agreement for a termination by the HCO, and transition services from the vendor, with minimal financial impact on the HCO.

Conclusion

Taking these considerations into account will help HCOs codify the parties' agreement and their respective obligations. Thereafter, IT vendor management should be employed to ensure that vendors perform and comply and that changes in the vendor's or the HCO's business or legal obligations are evaluated and mitigated as necessary. A strong and flexible agreement will make doing so easier.