Advanced Issues in HIT Contracts & Negotiation Strategies

March 3, 2016
Steven J. Fox, Esq., Principal
Post & Schell, P.C.

DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS.

www.himssconference.org
Conflict of Interest

Steven J. Fox, Esq., J.D.

I have no real or apparent conflicts of interest to report.
Agenda

• Learning objectives
• Pre-contract preparations
• Contract structural issues
• Contract negotiations
Learning Objectives

• Assemble the "right" team members for a successful contract negotiation

• Identify essential contract issues that need to be resolved in order to achieve a favorable outcome and successful partnership with the HIT vendor

• Construct a methodology designed to achieve a positive negotiation process
STEPS: Savings from a well negotiated contract

- Improve ability to budget
- Enhance alternative dispute resolution procedures
- Improve cooperation & win-win outcome

- Minimize likelihood of unanticipated expenses
- Decrease risk of potential litigation
- Reduce TCO
Pre-Contract Preparations
Foundation For A Solid Contract

At the beginning:

• Define expectations
• Understand the limits of technology you are acquiring
• Build organizational consensus; involve key stakeholders
• Recognize your org.’s capabilities
• Establish a shared understanding
• Ascertain budgetary requirements, but do not share org.’s internal budget details with vendor
Foundation For A Solid Contract (cont’d)

• What are the key components required?
• Are there hidden costs that may lead to rework, added costs & disputes?
• Formal selection process
  – Request for information (RFI) or request for proposal (RFP) based on comprehensive market research (e.g., industry ratings)
  – Functional requirements
  – Reference checking
  – Site visits
  – Financial viability
  – Development roadmap
Negotiating Team

- Key decision-makers (or maybe not)

- Team members who understand how to negotiate

- CIO, CMIO & senior tech staff

- Outside consultants

- Legal team
Contracts: Structural Issues & Negotiations
Definitions

• Customer, Affiliate
• Software, Enhancement, Upgrade, Version
• Documentation
• First Productive Use ("FPU" or "Go-Live"), Acceptance
• Regulatory Compliance
• System
• Third Party Software (incl. other proprietary content)
License Issues

• Use in connection with ACO & HIE

• Ability to process data for non-employed physicians and other healthcare providers who have staff privileges

• Expansion/contraction metrics
  – Allow for “organic growth”
  – License fee adjustments (up and down)
License Issues (cont'd)

- Beware of unusual limitations or restrictions on licensing metrics, e.g., the number of CPUs or computers that the software may be used on vs. number of actual users
  - May impact copyright infringement issues
Payment Provisions

• Tie payments to objective milestones, not dates or timelines. For example, 20% due upon contract execution; 25% due upon installation; 25% due upon First Productive Use; and the final 30% due upon acceptance
  – Familiarize yourself with esoteric Revenue Recognition Rules

• Price increase limitations and decrease triggers

• Require vendor to provide TCO (total cost of ownership) information
Acceptance Testing

• Establish customer-centric acceptance testing procedures & protocols

• Testing should take place both pre-live and post-FPU

• If software fails acceptance tests, Vendor should have a designated period of time to remedy any problems. If Vendor is unable or unwilling to remedy the problems after X attempts, Customer should have right to terminate and receive a full refund of all fees and charges paid
Support & Maintenance Services

• Describe, in detail, scope & price of support & maintenance services to be provided

• Service Level Agreements (SLAs)
  – Especially important for outsourcing, remote hosting, “cloud” contracts
  – Also necessary for run-of-the-mill support/maintenance
  – Need to include definitive measurement criteria

• Include meaningful remedies, e.g., a credit against future support and maintenance fees
Warranties

• Software, third-party software, hardware and custom programming will function together as a System in accordance with the Documentation (including the Vendor’s response to an RFP or RFI, if any)

• All software, hardware & related technology required for the project is included or specified in the contract

• Vendor may not restrict or withhold Customer’s ability to use or access its data under any circumstances (i.e., holding data hostage)
Warranties (cont’d)

• Compliance with applicable laws & regulations, including Meaningful Use
  - Focus on the language – regulations are not usually directed at HIT vendors, so contract must require Vendor to modify software if regulations impact the Customer’s use of the software

• Restrict Vendor’s use of and access to all of Customer’s data (incl. users, but especially patient data)
Warranties (cont’d)

• Interoperability/interfaces

• Sunset issues

• Warranty Period

• Minimum insurance requirements, e.g., workers’ compensation, commercial general liability, cyber insurance, errors and omissions (aka contractual or professional liability), product/completed operations & umbrella liability insurance
Special Considerations for Cloud Agreements

Due diligence considerations include the following:

- How long has Vendor been in business?
- Is Vendor publicly traded or a wholly owned subsidiary?
- Does Vendor have financial wherewithal to step up to the plate for data or privacy breaches?
- Is the vendor the owner and operator of all cloud resources and facilities?
- Require vendor to provide key staff commitments
Due diligence considerations (cont’d):

• Require Vendor to provide its disaster recovery plan (if it exists)

• Need to really check references (not just those supplied by Vendor)
  – Talk to conference attendees
  – Attend user-group meetings if possible
  – Review Vendor’s reputation in the industry (e.g., KLAS surveys or other reliable third party surveys or rankings)
  – What is the turnover rate of Vendor’s employees?
Cloud Agreements (cont’d)

How safe is your data?

• Where is it actually stored, in the United States or elsewhere?

• Does Vendor intend to use your data, even if “deidentified”?

• Need ability to access & download data as needed

• Is data stored in proprietary format or readily readable and convertible to other systems?
Cloud Agreements (cont’d)

How safe is your data (cont’d)?

• Has Vendor demonstrated ability to successfully create interfaces (if needed) to your particular system(s)?
• Need ability to use system (access data) if no Internet access
• Are robust backup, recovery & replication systems in place?
  – Does Vendor use differential, incremental and whole backups?
  – Are the backups verified to ensure their integrity?
• What happens if Vendor goes bankrupt or out of business?
Cloud Agreements (cont’d)

Technical due diligence considerations include the following:

• Does Vendor have any third party certifications (e.g., FedRAMP or SSAE16, SOC 2)?
• Where are the cloud provider & data center(s) located?
• Where are the disaster recovery sites located?
• What are Vendor’s privacy and security policies and procedures?
Cloud Agreements (cont’d)

Technical due diligence (cont’d):

• Ability to audit Vendor’s operations

• How long does it take to restore information and where would you be in the queue, if there were a need to restore?

• When was the last time Vendor conducted a risk assessment and is the report available for review?

• Has Vendor had any privacy or security breaches?
Cloud Agreements (cont’d)

Technical due diligence (cont’d):

• Does Vendor use encryption for data at rest, in motion and archived?

• What, if any, third party vendors or subcontractors does the cloud provider use?

• Other considerations: review the HIMSS Privacy and Security Toolkit, HIMSS Cloud Security Toolkit, HIMSS Risk Assessment Toolkit & others freely available
Cloud Agreements (cont’d)

Technical due diligence (cont’d):

• Is Vendor’s supply chain secure (i.e., is vendor reliant on a third party for any of its essential services or products)?

• Who is the actual developer of the software?
  – Vendor may be a licensee of the actual software developer
  – This may result in intellectual property issues
Cloud Agreements (cont’d)

Cloud Contract Review Issues

• What kinds of remedies make sense if Vendor does not perform? Is termination a practical alternative?

• Service Level Agreements (SLAs)
  – What are service level (uptime/downtime) guarantees for power availability, network availability, hardware availability and (if applicable) application availability?
  – Is the availability sufficient for your organization’s needs (e.g., is 99.9% or 99.999% available)?
  – What are the remedies if Vendor fails to meet the guarantee? Are there service credits? Include response times.
  – Can you terminate underlying agreement if Vendor fails to perform after a specified number of occurrences?
Limitation of Liability / Damages

• Cap on direct damages – how computed
  – Make it mutual
• Consequential damages
• Carve-outs
  – Vendor’s indemnification and confidentiality obligations (including HIPAA); and
  – Damages due to personal injury or death, including claims arising from Vendor’s negligence or misconduct
Indemnification & Hold Harmless Provisions

• Some form of Intellectual Property Infringement usually included

• More important than ever due to increase in patent trolls & I. P. infringement-related claims

• Insist that Vendor pay all costs incurred, not just those “awarded” by a court
Indemnification (cont’d)

• Typically requires Customer to assume liability for third party claims brought against HIT vendor

• Increasingly demanded by vendors

• Intended to shift liability and remedial burdens to physicians, nurses & hospitals, even when HIT users are strictly following Vendor instructions

• Requires high level discussion and negotiation
Indemnification (cont’d)

• Often paired with disclamatory “practice of medicine” language
  
  – Relies on legal doctrine of “learned intermediaries”
  
  – HIT vendors claim they are not responsible for errors their systems cause in patient treatment, because clinicians should be able to identify—and correct—such errors generated by software faults
  
  – Vendor is simply providing a software “tool”
Indemnification (cont’d)

• Ignores reality that medicine is moving to clinical decision-support systems
  – Clinicians encouraged to rely more and more upon software and hardware to practice medicine

• Consider scope of indemnity provision
  – Who is covered (e.g., employees, agents, officers, directors, affiliates)
  – What types of claims are covered (e.g., negligence, breach of contract)
  – Is “hold harmless” language included?
Sample Vendor Indemnity Provision

As a result of the complexities and uncertainties inherent in the patient care process, You agree to defend, indemnify and hold Vendor harmless from any claim by or on behalf of any patient of You or your personnel, or by or on behalf of any other third party or person claiming damage by virtue of a familial or financial relationship with such a patient, which is brought against Vendor, regardless of the cause if such claim arises for any reason whatsoever, (including without limitation Vendor’s negligence, except as provided below) out of the operation of the Software licensed to You under this Agreement. To the extent applicable, You will obtain Vendor’s prior written consent to any settlement or judgment in which You agree to any finding of fault of Vendor or defect in the Software or Vendor’s services. The indemnification under this Section will not apply if the proximate and direct cause of the event giving rise to the claim for indemnification is Vendor’s sole negligence with respect to an error in the Software and You and your personnel have, in connection with this claim, operated the Software accurately, used the Software only in accordance with the Documentation, and satisfied each of the customer responsibilities. Vendor will promptly notify You in writing of any claim subject to this indemnification, promptly provide You with the information reasonably required for the defense of the same, and grant to You exclusive control over its defense and settlement.

Note: this is from an actual vendor agreement.
Indemnification (cont’d)

• Note that this clause requires Customer’s indemnification even for Vendor’s own negligence

  – Exception if claim directly caused by Vendor’s “sole negligence” regarding a Software error, and Customer has been perfect in every way

• Unlikely that Customer would ever meet that unrealistically high standard
Indemnification (cont’d)

• Huge disparity in bargaining power

• Idea of not-for-profit hospitals indemnifying large, for-profit HIT vendors is offensive
  – Although probably not against public policy
  – Vendors profit hugely from HIT marketplace; need to step up to the plate & assume liability for themselves
Indemnification (cont’d)

• Healthcare providers who unwittingly assume vendors’ liability thinking it will be covered by their own liability or malpractice insurance may be in for rude awakening
  – Most insurance policies exclude “assumed contractual liability”

• Ironically, vendors could easily solve the problem by obtaining their own insurance policies
Indemnification (cont’d)

• If hospital agrees to indemnify, it should be written very narrowly and limited only to the hospital’s own fault

• Not agreeing to indemnify does not mean hospital is attempting to avoid liability
  – Vendor may still sue or file a cross claim if it believes the hospital is cause of the problem
Bankruptcy / Source Code

• Consider whether a source code escrow is applicable (not for cloud contracts), essential, viable or practicable.

• If no source code escrow, need ability to obtain access to the source code under §365 of the Bankruptcy Code for the software to continue Customer’s permitted uses under the license.

• The escrow account should be updated on a regular basis to include the current version of the source code.

• Carefully review pertinent source code escrow agreements.
Confidentiality / Privacy

• Include comprehensive provisions to protect confidential information, including financial records & patient information

• Incorporate Customer’s Business Associate Agreement by reference into a confidentiality section or attach as an exhibit to the agreement

  – If possible, use your BAA rather than vendor’s
Implementation

Detailed implementation workplan

- Timeline
- Fixed price vs. time & materials
- Milestones
- Accountability
- Measurement, monitoring approaches
- Disputes
- Multiple vendors
Dispute Resolution / Termination

• Build in escalation provision to resolve most disputes

• Consider alternative dispute resolution
  – Mediation, arbitration (approach with care)
  – Use litigation as last resort, but seek to have all claims adjudicated in your state, not the vendor’s

• Require transition assistance from Vendor at agreed upon price for a specified period pre- and post-termination

• Assure that Customer has the ability to continue to use the software during that period
Miscellaneous

• Include a force majeure clause with right to terminate the agreement if Vendor’s force majeure event lasts more than 60 to 90 days, with full or prorata refund of all fees paid

• Provide for survival of specified terms after termination, e.g., confidentiality and indemnification provisions
STEPS: Savings from a well negotiated contract

• Improve ability to budget
• Enhance alternative dispute resolution procedures
• Improve cooperation & win-win outcome

• Minimize likelihood of unanticipated expenses
• Decrease risk of potential litigation
• Reduce TCO
Discussion / Questions

Steven J. Fox, Principal & Chair
Health Care Information Technology Practice
Post & Schell, P.C.
607 14th Street, N.W. Suite 600
Washington, DC 20005
202-661-6940 (phone)

sjfox@postschell.com
www.postschell.com
LinkedIn: https://www.linkedin.com/in/stevefoxatty