Contracting Guidelines with EHR Vendors

In general, if a contract is presented to your group from a software company, it will be written from the perspective of the software company. You can request language changes to make the intent of the contract more "equal," although many companies may not be flexible about language changes. Do not be afraid to ask.

SPECIFICS TO CONSIDER:

GENERAL:

1. The contract should have bi-lateral termination clauses without penalty given within a certain notice period.

2. The contract should stipulate that it shall not be transferred by one party without written approval of the other party.

3. The contract should have a definition section for anything that is not readily understandable. Don't be afraid to require the vendor to spell out clauses in acceptable language.

4. The contract should spell out what happens in the event of default by either party and should be as evenly weighted as you can possibly negotiate.

5. The contract should clearly outline how the product is to be delivered. Is it run as an on-site application or delivered in an Application Service Provider (ASP) model through internet connectivity.

SOFTWARE:

1. The contract should spell out or explicitly address that you should own the data and that the data will be returned should the agreement between the two parties be terminated for any reason.

2. Contract should outline the minimum hardware required to run sufficiently the application as demonstrated. Contract should have provisions for hardware support if sold with system.

3. Contract should describe process on how upgrades to hardware are handled and notifications when upgrades are required for future releases.

4. The contract should also include language about the vendor turning over source code, data models, etc. should it for whatever reason cease to exist. This is usually handled through a process of escrowing the source code with a third party.

5. The contract should spell out whether the cost of the system includes upgrades, patches, etc. and, if so, how many, who is responsible for applying them, at what cost, and what happens if an upgrade negatively impacts the system.

6. The contract should spell out how non-vendor upgrades, patches, etc. (such as for the OS or DBMS) are handled, who is responsible, etc., similar to above.

7. If the system includes third party software and/or content, the contract should spell out the associated cost, who is responsible for those costs, who is responsible for support, and how updates are handled.

8. The contract should include language regarding the vendor ensuring the confidentiality of patient and practice information. The vendor should be required to execute a separate HIPAA Business Partner Agreement.

9. The contract should state that the vendor agrees to comply with HIPAA requirements and to make the necessary government-required modifications to ensure this compliance is at no additional cost to the practice. The vendor should provide changes that are required to sell or certify software in the current environment.

10. Access to system through dial-up or internet for the purpose of support should be clearly documented and list who will have access to data during on-line support fixes. This data should be a part of the HIPAA access record.

11. Access to system for updates should be defined. Clearly spell out procedures for changes and updates and when they can occur.

12. The contract should include delineation of test environments and whether there is one included within the system.

13. The contract should provide provisions for the ability of data to be separated if multiple practices will be using the same database. The application should allow for some data export in the case of a doctor that splits from the practice. Likewise, how is data combined if practices merge?

14. The contract should be structured to include a progressive payment schedule based on the achievement of certain implementation milestones.

15. The contract should specify the conditions under which a breach of contract has occurred, such as the system not performing as specified, consistent poor performance, etc. and at what point money is refunded, or payments may cease.

SUPPORT:

1. The contract should outline what support hours will be available (including time zone) and what level of support is included.

2. Costs for additional support should be itemized on the contract.

3. The contract should clearly outline the term of the support agreement.

4. The contract should have a clearly delineated escalation path for those issues which are not resolved by first-line support.

5. The contract should outline when a resolution has been achieved.

6. The contract should outline where support is delivered and that vendor support staff should speak clear English. Many vendors have outsourced support to other countries.

INTERFACES:

1. For each interface to another system, e.g., laboratory, billing, scheduling, etc., the contract should indicate whether the cost of the interface includes interface-programming time and, if so, how many hours are included. It should detail what happens if, and when, those hours and the associated costs are exceeded.

2. The contract should also identify what is included with the interface, for example interface specifications or programming.

3. The contract should state what happens either if subsequent programming is needed because of initial errors or if additional modifications are needed.

4. The contract should stipulate who owns the interface and who will troubleshoot it when it goes down.

5. Each interface should have terms outlined regarding which party is responsible for upgrading it, and which party will assure that it functions with new upgrades of main products.

TRAINING:

1. The contract should identify how many training hours are included, who is covered, and what is included with the training, e.g., training material, customized cheat sheets, etc.

2. The contract should explain what happens if additional training is needed and what the billing rate is for additional time.

3. The contract should spell out what are acceptable and non-acceptable costs and establish a per diem rate for trainers (if there are on-site sessions).

4. The contract should stipulate what (if any) follow-up training is provided, and at what cost.

IMPLEMENTATION AND TRAINING:

1. The contract should spell out what is and is not included in the implementation costs: what services will you receive, how many hours, who the resources will be, what sort of materials will be provided (e.g., project plan, implementation guides, specs), etc.

2. The contract should spell out what are acceptable and non-acceptable costs and establish a per diem rate for implementation staff.

3. The contract should have liability clauses for who is responsible during building of on-site applications and templates.

4. The contract should include who will be responsible for implementation of hardware if not provided by software vendor.

5. The contract should spell out what is and is not included in the training costs: what training will you receive, how many hours, who the training resources will be, what sort of materials will be provided (e.g., training guides, workflow designs), supplemental training, etc.

DISASTER RECOVERY AND PLANNING:

1. The contract should spell out how product is delivered – either via SAAS (ASP) or via installed on-site client-server application. The contract should detail ownership of data through either system.

2. If SAAS (ASP) or remote operations model is selected:
   a. The contract should include guarantees for uptime and service level agreements (SLA).
   b. The contract should provide guarantees on data availability, when service is performed, and notification of scheduled downtime.
   c. The contract should provide a detailed plan of how data is secured, back-up and restored along with a testing methodology utilized.
   d. The contract should provide for contingency planning if SAAS (ASP) is down for a significant time.

3. If the Owned and installed client-server model is selected:
   a. The contract should outline when service should be performed, how often, and how long it should take.
   b. The contract should clearly delineate what hardware is required for backup and how frequently that should be run. This includes tape backup, battery or UPS devices required, workstations and server protections required, and a defined environment in which servers should operate.
   c. The contract should outline expected times for backup and processes for testing backups.
   d. The contract should offer a model for escalating support for failures and downtime and include a priority list of who should be contacted for catastrophic events.

4. The contract should include definitions of support and recovery of physical and/or wireless networks and how passwords are recovered.

5. The contract should clearly outline what network security is required for supporting connectivity to the internet. This is usually listed as firewalls, virus protection, spyware protection, password security, and other security devices to limit access to networks and applications.

MEANINGFUL USE CERTIFICATION:

Since your EHR is crucial to your ability to comply with Federal Incentive Program regulations for meaningful use, it is advised that you include that the vendor product you are purchasing from the vendor must be certified and retain meaningful use certification.

1. Meaningful Use Certification means meeting and satisfying all applicable meaningful use criteria as designated by the Office of the National Coordinator for Health Information Technology (ONC), United States Department of Health and Human Services, once regulations are published and become effective.

2. The EHR products and systems must comply within a reasonable timeframe in order to allow you as an eligible provider to qualify for any associated incentive revenue programs adopted by the Centers for Medicare and Medicaid Services (CMS) provided you can satisfy the program's requirements. If you qualify for either the Medicare or Medicaid Incentive Program and in the event that your product fails to meet the respective year's reporting period, the EHR

Vendor will specify, in its agreement with you, the participating physician and group medical practice, how it will make reparation to said physician or group medical practice for not qualifying for that year's incentive.

Reparation shall occur as follows:

a. in the event Vendor fails to deliver any regulatory meaningful use criteria (this specifically includes core objectives and clinical quality measures from core and alternative menu sets) necessary for the Vendor's applicable EHR software to become and/or remain a certified EHR under the published meaningful use final rule, the Vendor will waive the annual maintenance fees applicable to the affected EHR software for twelve (12) months (the "Credit") in any 'incentive payment' year in which the EHR software fails to comply with the meaningful use requirements for the licensee.
b. The foregoing Credit shall apply only in the event the Vendor fails to deliver revised software which allows the licensee to successfully achieve and comply with a certified meaningful use EHR product within the incentive-eligible year.
c. The EHR Vendor must notify physician or group medical practice within a commercially reasonable timeframe, not to exceed 5 business days if any of its EHR products or systems purchased by physician or group medical practice fails to achieve or loses Meaningful Use Certification.

CAVEATS:

1. Look at the warranty, disclaimer and limitation of liability sections very carefully. Usually these are written all in caps, and they severely limit the software company's liability. They are not likely to change either section substantively (if at all), even if you request it, so read and understand this part and what it means for you.

2. Check carefully to see what the software company warrants to you and what your responsibilities are with regard to it.

3. Look to see if they specify minimum hardware requirements and be prepared to meet them. If you use what they consider "substandard" equipment (to try to save some money) it may invalidate the agreement.

4. Read the indemnification section carefully as well. This is another section that they are not likely to change for you, so understand what it is stipulating.

5. Check the duration and termination clauses – again, you should be able to "free" yourself from this with relatively little organizational pain. (No handcuffs or shackles.)

6. Understand the different ways in which the vendor can terminate the agreement and make a contingency plan for this.

7. Software "Source" code is to be placed in escrow to be turned over to the physician practice in the event the vendor is taken over by another company, merges with another vendor company, no longer wishes to remain in business, or files for bankruptcy or becomes insolvent.

PLEASE NOTE:

This document is not meant to serve as legal advice by MSSNY. This is only to be used for informational purposes. Please consult your attorney when reviewing or agreeing to any contract provisions.