Doctors' Office Quality - Information Technology (DOQ-IT) Project

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.

6. All responses to RFP's, if completed, should be included in the contract.

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 sufficiently run 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. Contract should also include details regarding supported versions of the software (i.e. vendor will support current General Available release and one prior release).

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 (both software and services), 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, service packs etc. (such as for the OS or DBMS) are handled, who is responsible, how customers are notified etc., similar to above.

7. If the system includes third party software and/or content, the contract should spell out the associated costs, who is responsible for those costs, who is responsible for support, and how updates are handled, as well as notification if 3rd party software vendors change and associated cost changes.

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 all state, federal and 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. Contract shall define requirements for access to system (i.e. 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 needed/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 include language providing you governmentally required regulations and/or changes should be provided as updates at no-charge.

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

This material was prepared by MassPRO, the Medicare Quality Improvement Organization for Massachusetts, under contract with the Centers for Medicare & Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services. The contents presented do not necessarily reflect CMS policy.

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 and after-hours 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.

7. The contract should specify when support/maintenance fees being (i.e. at time of implementation vs. go live).

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 if subsequent programming is needed either 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.

6. The contract should specify if there are support/maintenance fees for vendor developed interfaces.

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:

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 (i.e. can vendor outsource services to be supplied by a 3rd party), 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.

Disaster Recovery and Planning:

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

2. If 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 down-time.

    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 ASP is down for a significant time.

3. If the Owned and installed model is selected:

    a. The contract should outline when service should be performed, how often, and how long it should take, and why customer is responsible for in terms of regular (daily/monthly) maintenance.

    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.

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 to be "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.

This material was prepared by MassPRO, the Medicare Quality Improvement Organization for Massachusetts, under contract with the Centers for Medicare & Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services. The contents presented do not necessarily reflect CMS policy.