CONTRACT Review Guidelines

healthPOINT

The guidelines below are recommendations for contract review when final negotiations are in place for your electronic health record vendor selection.

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.
5. The provider should be held harmless should the EHR vendor default for any reason, including going out of business, or there is a breach of contract.
6. 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.
7. The contract should clearly outline how the product is to be delivered. Is it run as an on-site application, or delivered as an Application Service Provider (ASP) model or delivered as Software as a Service (SaaS) model via the internet.

Software:

1. The contract should spell out or explicitly address that the provider should own the data and that the data will be returned should the agreement be terminated for any reason.
2. Contract should describe process on how upgrades are handled and when notifications for upgrades are being released.
3. 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.
4. 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.
5. The contract should spell out how non-vendor upgrades, patches, etc. (such as for the OS or DBMS) are handled, who is responsible, and what happens if an upgrade negatively impacts the system.

Regional Extension Center Project Activities funded by the Office of the National Coordinator for Health IT U.S. Department of Health and Human Services ARRA Grant #90RC0062/01

6. 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.
7. 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.
8. 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.
9. Access to system for updates should be defined. Clearly spell out procedures for changes and updates and when they can occur.
10. The contract should include an explanation of test environments and whether there is one included within the system.
11. 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 leaving a practice. Likewise, how is data combined if practices merge.
12. 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 location) and identify the level of support that is included.
2. Costs for additional support should be identified in the pricing documentation.
3. The contract should clearly outline the term of the service/support agreement.
4. The contract should have a clearly outlined escalation path for issues that are not resolved by first-line support.

Interface(s):

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. Each PM/EHR interface should have terms outlined regarding which party is responsible for upgrades, and which party will assure that it functions with upgrades to the product(s).
5. The contract should guarantee interface with the State Health Information Exchange (HIE).

Training:

1. The contract should clearly define PRACTICE training, including training materials, and other documentation.
2. Costs associated with Provider and staff training should be defined and itemized.
3. The contract should provide itemized costs (including travel, per diem, etc) for on-site training or additional practice training needs, including customized training for the practice.
4. The contract should stipulate what (if any) follow-up training is provided, and at what cost.

Implementation:

1. The contract should list all associated costs for implementation including services rendered, projected hours, documentation/materials provided, (e.g., project plan, implementation guides, specs), and identify implementation personnel.
2. The contract should categorize any additional costs not included in the implementation costs.
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, SaaS or installed on-
   site application. The contract should detail ownership of data through either system.
2. If ASP or SaaS 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 servers or data center (ASP and SaaS models) are down for a significant time.
3. If the Client/Server (provider owned and installed on-site) 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 outline expected times for backup and processes for testing backups
   c. The contract should clearly delineate what hardware is required for backup and how frequently that should be run. This includes back-up type, battery or UPS devices required, workstations and server protections required, and specifications for operating environment for the servers.
   d. The contract should offer a model for escalating

support for failures and/or 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. Warranties: What is the warranty term and what are the provider responsibilities?
3. Carefully review minimum hardware requirements. Will use of "substandard" equipment render the agreement null and void?
4. Read the indemnification section carefully as well. Is it easy to understand?
5. Is it easy to understand the requirements of the termination clauses?

It is highly recommended that an attorney review the final contract with any EHR vendor prior to signing.

HealthPOINT will provide services and assistance to all providers with a signed provider service agreement, regardless of EHR Vendor selected, as long as the vendor is ONC/ACTB Certified for Meaningful Use.

If you need additional help, please contact your HealthPOINT Clinical IT Specialist; send an email to healthpoint-info@dsu.edu; or call 605.256.5555.

healthPOINT
at Dakota State University

healthpoint.dsu.edu

605.256.5555