Specific Contract Considerations Dealing with Cloud Computing and EMR

1. **Data security and privacy**

   i. Data hosted must be secure (protected from hacking) and compliant with laws (HIPAA, HITECH, state laws like Mass.Gen’l Law 93(h), which requires encryption in some cases). Data provided by the Health Care Provider (Provider) may need to be encrypted where it is stored. This is a moving target by definition, because standards and abilities to get into systems or break encryption change. Storage of data must be compliant with PCI standards. Data storage must meet minimum standards like firewalls, encryption, SSL (secure sockets layer) transmissions. Right now, the AMA seems primarily occupied with criticizing new rules regarding “meaningful use,” but it could jump into the fray, issuing standards for both operation of EHR systems and storage of data. New meaningful use standards were just issued July 20, 2010.

   Sample language: “Data Security and Privacy. Vendor shall (i) establish and maintain safeguards against the destruction, loss, unauthorized alteration of, or unauthorized access to Provider’s Data stored on Vendor’s systems (“Vendor Systems”) in compliance with applicable laws and regulations, (ii) store all Provider Data, in each case in accordance with PCI (or successor) standards then in effect (“PCI Standards”); (iii) encrypt personally identifiable information and credit card data as it is transmitted between the Vendor Systems and Provider, Provider Patients or End Users; and (iv) ensure that data storage complies with all relevant laws, regulations and standards, including but not limited to HIPAA, HITECH, states laws, and applicable regulatory and professional standards.”

   ii. Data transmission must be secure. T.J. Maxx was hacked in transmission of the data at store locations, and information from several million credit cards was captured via wireless transmissions in those stores!

   Include provision that applies to the handling of data; for example do not allow transmission by wireless of full credit card numbers in the same transmission

   Sample language for payment data: “(iv) ensure that all payment data transmitted by Vendor stores within the Vendor Systems is comprised of nothing that, by itself, would divulge protected personal information or complete credit card information (for example, no more than the last four digits of any credit card or other incomplete credit card data.”

   iii. Both Vendor and Provider must comply completely, and warranty and indemnification language should reflect that requirement to comply. [See an example at paragraph 6 below]
iv. A hosted service must have separate instances of information stored. If
data is stored in the “cloud,” security is purely a matter of safeguards; the
sites of the data may be anywhere. But if the service stores the
information itself, there are more options. Does the customer get a
dedicated/secure server? If not, how does the vendor secure that
information? Can it secure data on a shared server with dedicated
files/ports and limited access? The economics of this will depend on size.
The contract should specify that access to your information is segregated,
and only accessible to authorized users.

v. Specify what authentication is required to obtain data, including level of
questions, or refer to a standard or attachment. At a minimum, make it
accessible only to those with rights of access who provide required
identification (user ID and password). In some cases, you may also
require the user to answer certain questions before accessing. Any abuse
due to the Provider’s failure to regulate is not the Vendor’s problem.
Inadequate Provider/user control vs. inadequate process control is a trade-
off. When is inadequate user control due to poor process?

vi. Hold the Provider to tight standards regarding access to the system and
user names and passwords. Those standards must be spelled out.

Sample language: Provider agrees to take appropriate measures [Better to
specify what they are] to protect against the misuse of and/or unauthorized
access to the consumer data within the services provided through any
methods, including unauthorized access through or to Provider’s user
identification numbers or passwords (“Account ID’s”). Provider agrees
to investigate any such misuse or unauthorized access and to take
appropriate measures to address any such misuse or unauthorized access.
Provider is responsible for the administration and control of Account ID’s
by its respective employees and by third parties who are provided access
to the Services. Provider shall identify a security administrator to
coordinate with Vendor. Provider shall manage all Account ID’s, and
notify Vendor promptly if any Account ID becomes inactive or invalid.
Provider shall follow the reasonable policies and procedures of Vendor
with respect to account maintenance as they may be communicated to
Provider, as applicable, in writing from time to time. In the event that
Provider learns or has reason to believe that consumer data hosted within
the services provided has been disclosed or accessed by an unauthorized
party via the Provider Account IDs, Provider will immediately give notice
of such event to Vendor.

2. Who owns the results and data?
Ownership of data: The contract must be very clear about who owns what. The Provider should own the raw data, subject to specific ownership of personal information by the patient. Health care law covers patient’s rights to access data. The contract must require that the Vendor comply with that requirement (for ex. 24 hour access). The vendor may have a right to keep it in some cases. The contract also should indicate who owns how it is analyzed/sliced and diced. This depends on what contract says, but again, the patient may have rights.

Sample language: Data Security. Vendor shall establish and maintain reasonable safeguards against the destruction, loss, alteration of, or unauthorized access to Provider Data stored on Vendor’s systems (“Vendor Systems”). Vendor shall store all Provider Data in Vendor’s possession in a password-protected database and shall, in accordance with the highest standards in the industry, in compliance with all applicable laws under HIPAA, HITECH, states laws, and applicable regulatory and professional standards, use security measures, including, but not limited to, encryption and firewalls, to protect such Provider Data from unauthorized disclosure or use. Such measures shall be no less rigorous than those measures maintained by Vendor for its own data of a similar nature. When Vendor stores Provider Data in an offsite facility, Vendor shall use an offsite storage facility reasonably acceptable to Company that shall, without limiting the foregoing, be in full compliance with all confidentiality provisions of this Agreement. [Additional language may be required for cloud storage.]

What are the patient’s rights? Vendor may want to use process data and compile/aggregate data. Some of the data may be required at some point by the Provider, either to respond to patient request or insurance. The contract should require the Provider to safeguard against reverse engineering data back to patient; keep it anonymous. The contract may restrict how data (even aggregate data) is used (for example no sale to 3rd parties).

Any hosted system is not just storing data, it is also preparing reports, analysis, etc. Provider wants to own all data, even results of reports created, but the Provider does not own the tool that does it. This is where the conflict exists, because the Provider wants access to data, including how it is analyzed, but the Vendor wants to retain sole rights to the tools.

Customer needs right to get original data back (Contract and bankruptcy-proof). One way to ensure this is to require that data is backed up and provide periodic reports of data to Provider, so Provider has frequent periodic copies of the data. This, however, increases the security risk and requires a cross-rep by the Provider that it will also secure the data.
iv. How do you protect against bankruptcy of the Vendor? One way is to include a form of escrow agreement to provide source code in the event of Vendor problem. This, however, really provides little real protection, because source code alone is almost worthless. The Provider needs access to the platform, not just source code. Iron Mountain and others provide 3-way agreements that may provide access to the platform, but it is not clear that it really will be effective. This is a business risk of hosted platforms that is difficult to solve. Even the platform has limited use without access to the people who know how to solve inevitable problems. Those skilled people often are mere employees of the Vendor with no privity of contract with the Provider (or the patient).

v. The contract needs to provide for transition services to move data to another platform. The Vendor may fight this, but the Provider and the patients need a right to get data. It should be a seamless transition – the Vendor needs to get paid, and the transition period needs to be finite. There should be a specific notice period. Probably will depend on regulatory requirements.

What transition period is needed? Does it take place before or after termination of the agreement? Many of the contract terms should continue to apply. What will the Provider pay the Vendor to supply data/services in transition? What format is the data that is provided?
3. Ownership of IP

i. The Provider/Customer wants to own the right to use his/her/its own ideas and specific medical info. For example, if a Provider determines that a new way to present the material makes it more acceptable for reimbursement purposes, who owns that improvement? The Provider will want to own that and have the ability to carry that new presentation with it when it leaves the Vendor, but the Vendor may want the right to use that presentation with other Providers.

ii. Vendor wants to be sure that software, methods, algorithms, etc – anything they incorporate into the process – remains theirs. Vendor wants to own what it creates with sweat equity, even if the kernel idea came from elsewhere. But Provider may say if I had the idea, I retain a license to use that elsewhere.

Example language: See attached IP language

4. Where will the data be hosted?

Jurisdiction is key. You want data to remain in the U.S., if possible. It might be problematic to store data, even as a back-up, in countries where privacy protection and IP protection is a particular problem. This needs to be understood clearly in the agreement. We recommend that all data is stored in the U.S. Even Canada can become an issue, only because it puts you under Canadian standards for breach and security. These are not “bad” standards, but they are different. Where will disaster recovery be provided? That must be in the U.S., as well.

5. Efficacy of the system:

What is expected vs. what is promised. Some systems do not provide all parameters of practice management. Some allow a menu of choices. Unrelated systems tend to not “play well” together. If a Provider is choosing a system that is not comprehensive, it needs to understand the ability of the Vendor to provide a comprehensive solution later. If the Vendor cannot provide such a comprehensive solution, the agreement should say so.

What is the level of availability and service? There are some legal standards here, but you must be specific.

What is the compensation if service levels are missed? Both parties need liquidated damages in these agreements, or valuing the breach becomes complicated. Is there a cap on service levels or fees? What is the response time to find and/or fix an error?

6. Indemnification and limitation of liability

Typically, indemnification is not limited if the Vendor improperly manages confidentiality or data security. A relatively standard software license
indemnification will be pressed by the Vendor, but the Provider will want exceptions to that limitation similar to the language provided below.

Sample language: “[The Parties] agree that except for actions arising out of (i) a Party’s gross negligence or intentional misconduct, (ii) a Party’s indemnification obligations; or (iii) a breach by Vendor of any law or regulation or of the confidentiality or data security provisions set forth in this Agreement, a Party’s aggregate liability for any and all losses or injuries arising out of any act or omission of a Party in connection with anything to be done or furnished under this Agreement or any Statement of Work shall never exceed the greater … . Further, except for actions arising out of (i) a Party’s gross negligence or intentional misconduct, (ii) a Party’s indemnification obligations; or (iii) a breach by Vendor of any law or regulation or of the confidentiality or data security provisions set forth in this Agreement, in no event will either Party be liable to the other for any indirect, special, consequential, punitive or incidental damages, whether based on breach of contract, tort (including negligence), or any other legal theory, even if advised of the possibility of such damages.” (emphasis added)

7. And interview with a SaaS / Cloud provider of web-based EHR

A president of a new electronic health records provider, specializing in small and single-physician practices, provided the following perspective. His company’s product is currently in advanced beta testing and is based in part on a system proven effective in hospital situations in another country, modified for U.S. requirements and to fit a smaller practice environment. I thought hearing from the perspective of a Vendor may be of interest. These are excerpts of our discussion, mildly edited in some cases. I provide these only as a perspective of how a Vendor providing an EHR system (SaaS) views this.

Why do you believe that a web-based solution will be the platform of choice for EHR?

There are several reasons that a web-based solution will be the only solution for EHR. The standards are ever changing, both technical and legal, so a program located at the user’s location would have to be updated constantly at many locations. In fact, standards for things like data at rest [encryption] seems to change all the time. Billing requirements, including Medicare/ Medicaid/ Insurance reimbursement coverage and procedures, change constantly. Any system will require connectivity for immunization records, lab results, billing access, patient access and other things. And if you open the system for daily updates by the web, why not just have the program itself sited at the web? The risks and the challenges to protect data are basically the same once you open that door. Upgrades are expensive, but not as much when they only need to be made in one place. Most doctors are small businesses, and they need plug-and-play, which a web-based system must provide. Also, their cash flow does not favor large initial investments, which a web-based solution can avoid.
What are the primary challenges to a web-based solution for EHR, and especially for a cloud computing solution?

The primary challenge is safety of the data; placing sufficient safeguards in the system to protect against unauthorized access. However, virtually nothing will protect against unauthorized access due to misuse of an ID and password by the Provider. If you compare to use of paper records, the efforts being used to safeguard patient data is extraordinary. An old fashioned doctors’ office has few protections. A locked door and a locked file cabinet – usually with the key in the front drawer of someone’s desk – is about it. Barriers to entry are location and a crowbar, or in some cases just a stiff plastic card. Few small practices have electronic security or cameras. The difference is that stealing paper information is cumbersome. The thief must steal a lot of paper or copy that paper to take it away for analysis. It is just practically difficult, unless you are looking for a few people. What makes electronic records more dangerous is that it can be done from anywhere – proximity to the doctor is not necessary – and once you gain access, you may be able to copy all the records in seconds. And having them in electronic form makes it easier to search for what you want and to manipulate the data. So, it’s not easier, it’s harder, but it can be done from anywhere with little trace, and it’s also much more efficient.

We are developing a system of firewalls, passwords, key questions, etc. to keep out the bad guys, but no system is impenetrable. A web-based system will have more “points of entry,” but any system will have several. Protecting this is a bit more complicated when persons with access can log on from different IP addresses. We are working on that now. However, as I said, by far the largest potential for compromise is from accidental or purposeful sharing of Provider ID and password to third parties. That’s the equivalent of someone in the office giving a stranger a door key, and very little can protect against that.

Another primary challenge is keeping up with the changing standards. Medicare and Medicaid change payment terms and processes in some way almost quarterly. That is challenging, although the dealing with those changes is more straightforward in a web-based system than a system resident at each Provider’s office. We must ensure that the EHR is certified and complies with requirements for “meaningful use.” Those new standards just came out. We also need to integrate as best we can with certain open source programs favored by the NIH.

Does doing this as a web-based system, and particularly as a cloud computing system, make protecting this more difficult?

No, I don’t think so. Using a web-based system makes the system easier to manage and more effective. There are so many points of entry anyway, even in a provider-hosted system, that we believe the security concerns are only marginally more difficult in this kind of system. Yes, it’s a software challenge, but that’s what we do. We are still testing and have not made a determination about whether we are doing this via the cloud or with dedicated servers.
What are the advantages of using the cloud?

The cloud has several advantages. The cloud provides great computing power and almost immediate scaling. Data storage is almost unlimited. Most of the cloud vendors allow incremental use, so pricing is based on what you use. The cost is more difficult to calculate, because the vendors charge differently for different types of storage. The pricing is complicated, and that makes it difficult to predict with precision the exact costs of increasing use. This difficulty in predicting cost would be the reason we don’t use cloud in our final model, although we are testing it now. It is not clear to us, yet, that cloud data storage is necessarily cheaper than using dedicated servers. It is more flexible, but we do not know that it will save money. The other problem is what happens when data is lost. Yes, there are back-ups, but you have to know what back-ups to access, precisely which data to replace. When you are using a dedicated server, you can see quickly what was lost or corrupted and replace it. In the cloud, the loss is more difficult to assess. It is difficult to tell what was affected, so you might have to replace numerous files that were not really affected. That costs time and money. All of this will be part of our decision.
Ownership. Provider agrees and acknowledges that, unless otherwise specified in an attached schedule, Vendor owns and will continue to own all right, title, and interest in and to the Services and any Deliverables, and in each case all modifications, improvements, upgrades, and derivative works in any way related, and all related Intellectual Property. Unless otherwise specified in an Initiative Schedule, Provider agrees to assign all right, title, and interest it may have in the foregoing to Vendor. Provider further agrees that it or its employees or agents may provide or create certain feedback or innovations regarding the attributes, performance or features of the Services or Deliverables (collectively "Feedback"). Provider assigns and agrees to assign all right, title, and interest it may have in any Feedback to Vendor. Vendor agrees to reimburse you for your actual reasonable cost of providing Vendor any requested cooperation in effecting such assignment. Provider provides any such Feedback to Vendor “as is” and without any warranty of any kind. If for any reason Provider’s assignment of the Feedback is ineffective, Provider grants and agrees to grant to Vendor a non-exclusive, perpetual, irrevocable, royalty free, worldwide right and license to embed such Feedback into the Services and otherwise use, reproduce, disclose, sublicense, distribute, modify and otherwise exploit such Feedback without restriction. Subject to the terms and conditions set forth and to Provider not using the Feedback to develop a service that competes with the Service during the term of this Agreement, Vendor grants to Provider a non-exclusive, perpetual, irrevocable, royalty free, worldwide right and license to use, reproduce, disclose, sublicense, distribute, modify and otherwise exploit the Feedback provided by Provider (the “Grantback License”). Such license shall be provided “as is” and without any warranty of any kind.

Restrictions. Provider agrees not to, either directly or indirectly, (i) modify, adapt, reverse engineer, disassemble, de-compile or otherwise derive source code from the Services or any software associated with the Services; (ii) create derivative works based on the Services or any software associated with the Services; (iii) make unauthorized copies of any software or other copyrightable materials associated with the Services; (iv) transfer the Services or any part or software or material associated with the Services to any third party without Vendor's prior written consent, (v) use the software that embodies the Services other than as intended and directed by Vendor in connection with its integration with a Provider website and as contemplated by an Initiative Schedule, or (vi) resell the Services other than as provided by an Initiative Schedule. Provider agrees not to remove, alter, cover or obfuscate any copyright notices, logo or other proprietary rights notices or proprietary mark placed or embedded by Vendor on or in the Services.

Data Ownership. Vendor acknowledges that Provider will own all right, title, and interest in and to any data that Vendor may collect from Provider or Provider Customers (defined below) in connection with their respective use of the Services (“Provider Data”). Provider grants and agrees to grant to Vendor a non-exclusive, royalty-free license to use the Provider Data during the Term (i) to provide the Services to Provider and/or to Provider Customers; and (ii) as necessary to monitor and improve the Services. Further, Provider grants to Vendor a perpetual, irrevocable, non-exclusive, royalty-free license to use the Provider Data in aggregate, anonymous form (e.g., with any and all personally identifiable components removed)(“Provider Aggregate Data”) (A) for statistical purposes; and (B) for marketing the Services to others. Notwithstanding the foregoing, with respect to Provider Data consisting of specific information provided by Provider about non-profit enterprises and not constituting Provider Customer transaction data (“Provider Non-Profit Data”), only “(i)” and “(ii),” above, shall apply.