EHRs in the Cloud: Contract Protection for a Rainy Day

Save to myBoK

By Marilyn Lamar, JD

Cloud computing has been suggested as a cost-effective way to use electronic health records (EHRs), particularly for small providers that may not have an IT staff. Cloud-based EHRs store patient health records and the EHR software on computers operated by the EHR vendor.

The healthcare provider accesses patient records and related data only through the Internet. It does not have a license to the EHR software or a copy of the patient records.

The advantages of cloud-based EHRs include lower cost, availability from multiple locations, and disaster recovery services. However, organizations must consider some key legal issues when contracting to use EHRs maintained by another entity.

Cloud-Computing Risks

In many ways cloud computing is not very different from an application service provider, service bureau, or outsourcing approaches that have been used in healthcare for years. The main difference is that the vendor may move the data and processing as needed throughout the day using the Internet to access greater distributed computing power and storage.

The risks inherent in cloud computing primarily stem from the lack of control by the organization. For example, patient records will not be accessible if the Internet is unavailable, the vendor's system is down, or the vendor makes its system unavailable due to a dispute with the organization.

A vendor's financial problems could also result in an interruption or termination of its business. Organizations should evaluate the vendor's financial stability as one of its selection criteria.

Legal Considerations for Cloud Computing

Organizations must review certain key legal issues when contracting for cloud EHRs. These issues are described below for general information purposes. This is not a complete list of all issues an organization may need to address and does not constitute legal advice. Providers should consult with counsel experienced in cloud-based services to obtain appropriate contract protection.

Privacy and Security. Organizations should have the protection of a HIPAA-compliant business associate agreement to address privacy and security issues. They should also perform their own review of any privacy and security risks presented by the use of a cloud vendor, including data back-up and disaster recovery plans. A qualified IT professional should review the vendor's disaster recovery plans and its Statement on Auditing Standards (SAS) 70 Type 2 audit.

General Warranties. The vendor should warrant that the EHR will function as described in a detailed description and will interface with other systems depending on the organization's specific needs. The organization or its consultant should review the detailed description before the contract is signed to ensure that it adequately describes the features and functions the organization expects. The vendor's sales materials and proposal typically will not be binding unless expressly warranted.

Meaningful Use Certification Warranty. The vendor should warrant that the EHR is certified for the stage 1 requirements of the meaningful use program and will be certified for phases 2 and 3 before the applicable deadlines.

HITECH Warranties. HITECH requires that if a patient elects to self-pay, the record of that care may not be disclosed to payers. It also changes the accounting requirements for disclosures made with EHRs. The vendor should warrant that it is

able to meet these requirements. The contract should also require the vendor satisfy future regulatory requirements, although it may be necessary to agree to share the cost of changes.

e-Discovery and Litigation Holds. Complying with e-discovery requests and administering litigation holds may be challenging in the cloud-computing environment because data are held by a third party and moved often to minimize costs. Organizations should discuss these requirements with the vendor and ensure the vendor's commitment (and associated fees) are reflected in the contract.

Availability, Support, and Response Times. The contract should specify the availability of the EHR system and support depending on the organization's needs. Response times and a commitment to work outside of normal support hours to resolve critical problems should also be included.

Organizations may also negotiate the minimum average response times for functions, such as accessing a patient record. The vendor may insist on limiting its financial obligations for the service-level agreements regarding system availability and response times.

In addition to reaching an appropriate limit on these performance credits, organizations must evaluate whether they can terminate the agreement if the service-level agreements are not met on a continuing basis or whether the limited credits against future fees are the "sole remedy" so that the organization cannot terminate and/or seek other damages.

Limitations and Exclusions of Liability. Vendor contracts will limit the vendor's exposure for damages, but the organization must determine whether the limits proposed are reasonable in amount and scope given the risks. For example, an exclusion of damages for "lost data" may not be acceptable if patient records are stored in the vendor's cloud. Limiting the vendor's exposure to the amounts paid by a customer in a 12-month period may not provide sufficient protection if the breach occurs in the initial months.

Data Ownership and Access Rights. The contract should state that the vendor does not have any rights of ownership to patient records or other organization data. Any right of the vendor to de-identify such information or use it for benchmarking should be carefully reviewed. Organizations should have the right to obtain a copy of all patient records and other data at any time regardless of whether there has been a breach.

Transition Services. Organizations should negotiate to obligate the vendor to provide transition services to help migrate all data to another EHR in a generally accepted data format. Organizations may have to pay for these services, but they are often critical when a contract is terminated.

Indemnification. Vendor contracts may require the organization to indemnify the vendor from claims of third parties (such as patients) that arise from use of the EHR even if the damage was caused by errors in the vendor's EHR. Organizations may find this an unacceptable allocation of risk and negotiate for each party to be responsible for its own actions (e.g., programming errors of vendor versus organization error in using the system). If the vendor is unwilling to change this language, the organization should be aware that its insurance may not cover payments made to the vendor under such a contract provision.

Pricing and Acceptance Testing. Pricing provisions are often ambiguous and subject to unrealistic assumptions, meriting careful review. Initial payments should be delayed until satisfactory acceptance testing has been achieved. The organization should seek to limit future price increases within the contract.

Cloud computing may play an important role in increasing adoption of EHRs but the special risks should be understood and addressed as far as possible in the contract.

Reference

Dinh, Angela K. "Cloud Computing 101." *Journal of AHIMA* 82, no. 4 (Apr. 2011): 36–37.

Marilyn Lamar (mlamar@lamarhealthlaw.com) is a partner at Liss & Lamar PC.

Article citation:
Lamar, Marilyn. "EHRs in the Cloud: Contract Protection for a Rainy Day" *Journal of AHIMA* 82, no.7 (July 2011): 48-49.