Balancing the Risks and Rewards of Cloud-Based Healthcare Information

Rebecca N. Shwayri, J.D.

We are in the early stages of the electronic health record (EHR) era. And while EHRs offer many benefits, their proliferation is presenting challenges that some healthcare organizations are not equipped to handle.

For example, storing, harvesting, and accessing EHRs on a regular basis require significant investments in technology and personnel. To mitigate these costs, many healthcare organizations use cloud vendors for these services, which has some inherent risks. Storing EHRs in the cloud is still a good option, though, if organizations take the appropriate steps to mitigate these risks.

Cloud Benefits and Risks

The benefits and risks of outsourcing EHRs to the cloud are both quantitative and qualitative.

Benefits

On the benefit side, using a cloud vendor can dramatically reduce costs and enhance patient outcomes.

First, by deploying a cloud solution, the organization need not pay for hardware or the IT personnel that would be required to maintain EHRs onsite. In addition, a cloud option can be deployed to address an exponential increase in EHRs more quickly and cost-effectively than an onsite solution can be.

Second, deploying a cloud solution has the potential to enhance patient outcomes. When informa-

tion is stored in the cloud, physicians can access it at any time and can collaborate with hospitals and other physicians regarding a patient's care.

Risks

On the risk side of the equation, using a cloud solution could increase liability if the cloud vendor is not compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the 2013 HIPAA Omnibus Final Rule, which provides a more expansive definition of "business associates" that likely encompasses most cloud vendors.

According to the January 25, 2013, issue of the *Federal Register* (available at *www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf*), "…a data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis. Thus, document storage companies maintaining protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold."

While the Omnibus Final Rule imposes direct liability for security breaches on business associates, covered entities (like healthcare providers) are also liable.

While deploying a cloud solution can enhance patient outcomes, it can also detrimentally impact a patient in an emergency situation if vital health information stored there is not available. In addition, a security breach of that cloud-based information might expose additional patient information such as financial data, name, and address, which can be used to wreak havoc on an unsuspecting victim.

There is also the potential for violating international data privacy laws if EHRs are held on cloud servers located outside the United States.

Further, data stored in the cloud must be accessible and produced if it is relevant to litigation. Properly implementing a litigation hold and producing data stored with a cloud vendor can be difficult, and failure could subject the organization to sanctions for spoliation of evidence.

Security Issues in the Cloud

Records managers working within the healthcare industry need to be intimately familiar with HIPAA's Security Rule in order to mitigate the risks and liabilities from using a cloud vendor to hold electronic records. The Security Rule applies to health plans, healthcare clearinghouses, healthcare providers, and business associates.

Records managers working within the healthcare industry need to be intimately familiar with HIPAA's Security Rule …

Pursuant to the HIPAA Omnibus Final Rule referenced above, subcontractors that create, receive, maintain, or transmit protected health information (PHI) on behalf of business associates are now also business associates and must comply with the Security Rule. This more expansive definition of subcontractors encompasses most cloud vendors. Thus, a healthcare organization should ensure that the cloud vendor operates within the parameters of the Security Rule.

The Security Rule explains certain steps a covered entity must take to:

- Ensure the confidentiality and integrity of PHI
- Protect electronic PHI against any reasonably anticipated security threat or hazard
- Protect against any reasonably anticipated uses or disclosures of electronic PHI
- Ensure the covered entity workforce's compliance with the Security Rule

The Security Rule delineates several types of safeguards that are administrative, physical, and technical in nature.

Safeguards

Administrative safeguards are policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI. They may include such measures as conducting risk assessments to evaluate whether electronic PHI is vulnerable, developing an incident response plan to deal with a security breach, and creating policies for establishing access to sensitive systems that permit access to electronic PHI.

Physical safeguards encompass physical measures, policies, and procedures to protect a covered entity's electronic information systems and equipment from natural and environmental hazards and unauthorized intrusions.

Technical safeguards are the technologies, policies, and procedures for electronic PHI's use that protect and control access to it. Technical safeguards include audit controls to monitor activity in sensitive IT systems and encryption of data transfers.

Mitigating Security Risks

Utilizing a healthcare cloud storage solution can result in significant cost savings. Often, the cost savings can outweigh the risks if an organization takes appropri-

ate steps to mitigate them.

First, a healthcare organization should assess the cloud vendor's compliance with HIPAA. Do not take the cloud vendor's word at face value. Ask to examine its audit reports and its administrative, technical, and physical safeguards.

Explore the possibility of procuring cyber risk insurance to cover privacy-related risks. The cloud vendor could buy this insurance and name the healthcare organization as an insured or beneficiary under the policy. Cyber risk insurance can provide coverage for a data breach. While many companies carry commercial general liability insurance policies, such policies may not always cover the expenses of a data breach.

Third, there are litigation risks a healthcare organization could face if it uses a cloud vendor. For example, vendor-held information may be the subject of litigation, and the organization may need quick access to produce it for the court.

To appropriately address litigation risks, the contract should state that the healthcare organization owns the data in the cloud. The contract should also delineate what would happen in case of litigation and the steps to be taken when a hold is implemented. Before engaging a cloud vendor, carefully evaluate the vendor to ensure it has the capabilities to respond to large-scale litigation or regulatory requests.

Editor's Note: The Cloud Vendor Questionnaire on page 45, which was excerpted from ARMA International's *Guideline for Outsourcing Records Storage to the Cloud,* addresses a number of other issues an organization should investigate when considering a cloud services vendor. This guideline includes a broader discussion about retention, disposition, legal, privacy, technology, and security issues related to cloud-based storage and other tools for evaluating cloud vendors.

Balancing Benefits, Risks

Using a cloud vendor can have considerable benefits for a healthcare organization, including dramatic cost reductions, easy access to data from any location, and the facilitation of better healthcare outcomes. On the negative side, using a cloud vendor may result in additional privacy, security, litigation, and regulatory risks. These risks can result in major expenses, damage to reputation, and loss of market share in case of a data breach.

Determining whether to use a cloud vendor requires a balancing of quantitative and qualitative benefits and risks. Within your organization, determine the cost of additional hardware, software, and IT personnel if your organization were to store all of its data in-house. The technology-related cost savings represent one of the most significant quantitative benefits.

The risk of a privacy breach is most noteworthy, with the potential costs running into the millions of dollars. However, these risks can be mitigated with appropriate auditing procedures and cyber risk insurance.

In most cases, the quantitative and qualitative benefits of the cloud outweigh the risks as long as appropriate quality control metrics are put in place. **END**

Rebecca Shwayri, J.D., can be reached at rebecca.shwayri@akerman.com, *See her bio on page 47.*

Cloud Vendor Questionnaire

1. Are vendor terms and conditions consistent with the organization's goals and objectives?
2. Under what conditions, if any, will the vendor allow independent audits of systems and processes?
3. Where are the vendor's physical servers located?
4. Can the vendor provide international diversification with hubs in various geographic locations?
5. How long has the vendor been in business?
6. How long has the vendor been providing cloud-based services?
7. Who are some current clients of that vendor?
8. Can the vendor provide public, private, or hybrid cloud environments? (Circle all that apply.)
9. Can the vendor separate data depending on the data type?
10. Does the vendor have a firewall that will adequately address security-related needs?
11. Are data encrypted when using a public cloud environment?
12. What does the disclosure policy say about data on the vendor's systems?
13. Does the vendor offer redundant systems?
14. Does the vendor offer guaranteed uptime?
15. Does the vendor have redundant Internet connections?
16. Does the data center have adequate environmental control features?
17. Is the data center conveniently located (geographically)?
18. Is the perimeter of the data center protected?
19. Does the data center have a visible security presence such as a guard or monitoring cameras?
20. Is the data center location secured with systems to provide authorized access?
21. Is the data center located in a country where geopolitical instability may be problematic?
22. Identify the geographic locations the virtual environment spans.
23. Is the data center located near known or potential hazards?
24. Are applications and information distributed across systems?
25. Will data be stored so that it is segregated from (rather than commingled with) other organizations' data? If yes, specify how, i.e., what hardware and software are used?
26. Has the vendor's backup strategy been reviewed?
27. Is a backup done using disk to disk or tapes or other methods? (Circle all that apply.) Describe other methods.
28. Where are backup media located?
29. What types of drives are used for backups and are replacements available? Are they replacements?
30. How often are backup media rotated?
31. What types of redundant network links are available?
32. Can the vendor demonstrate a business continuity plan?
33. Are business-critical applications being hosted?
34. Is the data center designed around a virtualized environment?
35. Are the data on virtualized servers?
36. How is retention managed in a virtualized environment?
37. Is access to system configuration and/or administrative functions tightly controlled? Who can make changes to settings?
38. Are encryption and control lists in place to reduce the risk of inappropriate access?

Source: *Guideline for Outsourcing Records Storage to the Cloud* © 2010 ARMA International. (This publication is available for purchase at *www.arma.org/bookstore*.)