PUBLICATION

HIPAA Considerations in Evaluating Cloud Computing [Ober|Kaler]

2012: Issue 1 - Focus on HIPAA/Privacy

Cloud computing is a hot topic in business (including the health care business) due in large measure to the potential cost savings involved. Health care providers, however, have to consider more than just cost savings. At base, cloud computing is not a new concept and the HIPAA security risks it poses are not new. However, the risks arise in a new context. Providers interested in cloud computing will need to familiarize themselves with the new technological environment to best address the risks and formulate appropriate agreements and compliance structures.

Cloud computing, at its base, is not that different from traditional electronic storage arrangements. Traditional arrangements, however, including those for protected health information, involve a high degree of control of the system by the provider – a “silo” environment, if you will. The provider generally has sole use of the storage system (or some division thereof) and the information residing on the system, and has sole control over system access and security. In contrast, the various forms of the “cloud” environment all involve achieving cost-efficiencies by pooling physically disparate system resources in a common “virtual” environment. System resources, such as the servers on which provider information is stored, are pooled resources distributed across a number of physical locations controlled by the cloud vendor and made available on an on-demand basis. This structure is called “virtualization” by the industry, and essentially means that information appearing together on an electronic desktop may, physically, be spread across servers in several states (or even countries). Providers pay only for the resources actually used.

This article will focus on the so-called public cloud which, in addition to virtualization, typically involves the sharing of resources such as the servers on which a provider's information is stored. These arrangements, usually referred to as “multi-tenancy,” help to further reduce costs and improve efficiencies by permitting the sharing of resources that would otherwise be beyond the means of a single provider. The following are some basic, non-technical suggestions for a provider's evaluation of cloud computing and of potential vendors:

1. When evaluating vendors, consider the individual industry background of the vendor. Not all vendors are created equal in this respect. A vendor with experience in dealing with regulated information, ideally protected health information but at least information from other regulated industries (such as banking), is more likely to understand the requirements of HIPAA security and to have HIPAA-appropriate mechanisms in place than a less-experienced vendor.
2. Understand what level of encryption will be applied to protected health information in the vendor's system. By its very nature, the multi-tenant environment that characterizes the public cloud involves a certain “lowest common denominator” with respect to system features like encryption. Not all vendors are willing to deploy encryption if most of their users do not require it.
3. Make sure that the provider's data, including protected health information, is truly segregated from the data of other clients of the vendor. One of the characteristics of the public cloud – multi-tenancy – makes cloud providers a target of choice for hackers, since the data is Internet accessible and data of a number of targets is available through one source, due to what is referred to as physical and electronic proximity of the data of a number of clients of the vendor in one system. To minimize this risk, providers should understand and evaluate the steps taken by prospective vendors to segregate data stored in multi-tenant environments.

4. Bear in mind that not all cloud systems are the same and not all of a provider's data need be put into the public cloud system. The so-called “private” cloud (which, for simplicity's sake may be thought of as identical to the public cloud without multi-tenancy) presents a more secure environment. Many cloud vendors offer so-called “hybrid” cloud systems that utilize both private and public cloud infrastructures. Bear in mind, however, that vendors of private cloud systems may reserve the right to shift data to a public cloud environment if overall demands on the vendor's system require such a step. In addition, to the extent that a provider is able to segregate sensitive information, such as protected health information, from non-sensitive information, use of a public cloud may provide cost savings, while sensitive information may be better secured in a private cloud environment or even by being retained by the provider.
5. Evaluate what level of breach monitoring the cloud vendor provides. In many instances, vendors provide only very basic monitoring, such as review of access logs. In some cases, vendors may allocate responsibility for additional monitoring responsibilities to the provider. Understand and evaluate the cloud vendor's breach response plan.
6. Recognize that a provider's security policies will not necessarily follow the provider's data into the cloud. Understand, for example, what the cloud vendor's access policies are for its own work-force members, including authentication and identity proofing of those individuals to whom the vendor grants system access.
7. Have an exit strategy. That is, know how and when a provider will get its data back and in what form, when the arrangement with the cloud vendor terminates.
8. Obtain an appropriate HIPAA-compliant business associate agreement. Among other things, post-HITECH Act, a business associate must comply with the same physical, administrative and electronic security requirements as a HIPAA covered entity, which will cover some of the points discussed above. The relevant official interpretation of the HIPAA business associate requirements is the following FAQ response from the Office of Civil Rights, quoted in pertinent part:

The mere selling or providing of software to a covered entity does not give rise to a business associate relationship if the vendor does not have access to the protected health information of the covered entity. If the vendor does need access to the protected health information of the covered entity in order to provide its service, the vendor would be a business associate of the covered entity.

For example, a software company that hosts the software containing patient information on its own server or accesses patient information when troubleshooting the software function is a business associate of a covered entity. In these examples, a covered entity would be required to enter into a business associate agreement before allowing the software company access to protected health information.

It seems clear that a cloud vendor will have access to the provider's data in the course of providing its services, although some cloud providers that offer the provider the opportunity to encrypt its own data prior to submitting it to the cloud have taken a contrary view.

In sum, providers interested in cloud computing will have to learn a fair amount about a new technology without forgetting what they already know about HIPAA compliance and information security. Cloud computing has much to offer, and, with a careful assessment of risks and benefits (as well as a careful review of contractual and policy language) providers can take advantage of new technologies to increase data speeds, increase mobile data access, and decrease hosting and storage costs.