Codify
BY AAPC

Health Information Compliance Alert

Data Security: Weigh The Benefits Vs. The Risks Of Storing Data In The Cloud

How a signed BAA doesn't ensure HIPAA compliance.

Cloud services are incredibly helpful for many healthcare providers and for some providers, cloud storage is practically essential to operations. But is using the cloud safe? How can you protect against a data breach while using cloud services?

Upside: "The features of **Dropbox** and other [cloud storage] providers like Dropbox (**Box** and **OneDrive**) include ease of use, convenience and 'anywhere access' capabilities," stated **John G. Roman, Jr., CISSP**, director of **Nixon Peabody LLP**'s Electronic Discovery and Information Technology Operations team, in a Sept. 10 blog posting for the law firm. "The good news is that most cloud-based providers have tightened their data security in the wake of recent breaches."

But according to Roman, the question remains: "Do the benefits of using the cloud outweigh the risks associated with data potentially being compromised?"

Dispel This BA Compliance Myth

First, understand that just because an entity signs a business associate agreement (BAA) doesn't make that entity automatically HIPAA-compliant, warned Nixon Peabody partner attorney **Linn Foster Freedman** in an Oct. 1 blog posting for the law firm. "The entity must actually have policies, procedures and safeguards in place that comply with the Security Rule."

"That means dozens of policies and procedures specifically designed to protect the PHI it receives from a covered entity," Freedman explained. "In my experience, many business associates have no idea that they are required to have these policies and procedures in place and have not implemented them."

Beware: No certifying agency or government body will give any entity a "HIPAA compliant" stamp of approval, Freedman continued. The only way you could really know whether you're HIPAA compliant is if you make it through an **HHS Office for Civil Rights** (OCR) investigation unscathed.

Consider 7 Factors to Weigh the Pros & Cons

Regardless of the risks involved in working with third parties, nearly all providers need to. So if you're thinking about using a cloud system, experts offer the following thoughts on weighing both the risks and benefits of using a cloud service vendor:

1. Require the vendor to sign a BAA. Although merely signing the BAA won't ensure that the cloud vendor actually complies with HIPAA, you still need to have any third party with access to PHI sign a BAA.

And be sure to verify whether the cloud vendor provides appropriate breach monitoring. You must "understand and evaluate the cloud vendor's breach response plan," according to an article by attorneys **James Wieland** and **Joshua Freemire** for **Ober Kaler Attorneys at Law.**

2. Don't use free cloud storage versions. Free cloud storage, like any other free version of an application, "typically lack[s] the full features and functions of paid versions," Roman warned. And those features and functions include security safeguards.

Also, consider the vendor's individual industry background, Wieland and Freemire advised. "Not all vendors are created equal in this respect," and you want a vendor with experience in dealing with regulated information, ideally PHI. These vendors are more likely than less-experienced ones to understand HIPAA security requirements and to have HIPAA-appropriate mechanisms in place.

3. Ensure all data is encrypted. Make sure that the vendor encrypts data both "in motion" and "at rest." You need to be certain "that as you are uploading and downloading data, as well as while being stored within the cloud provider's data centers, data is being encrypted using the highest level of data encryption," Roman stressed.

Additionally, make sure that the vendor truly segregates your data (especially your PHI) from the data of the vendor's other clients, Wieland and Freemire advised. "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."

4. Password-protect your documents. Also, you can add an extra security step by password-protecting your documents, which will provide an additional safeguard, Roman suggested.

5. Create an automatic deletion policy. Depending on how you need to utilize the cloud services, you could consider using the cloud for only temporary storage of data. This will minimize the data's exposure.

"If the primary reason for using the cloud is to upload and download documents to share ... create and enforce an automatic deletion policy that will delete any data stored in the cloud after a specified period of time," Roman suggested.

6. Implement a private cloud. "In most cases, the safest place to store data is behind your company's firewall, in your data center," Roman said. "There are several private cloud data storage options that can be implemented within your data center that work identically to a Dropbox or Box offering."

The private cloud presents a more secure environment, Wieland and Freemire agreed. "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." So make sure you explicitly ask the private cloud vendor about this.

7. Know where your data will be stored. Most importantly, make sure that the cloud vendor will not transmit or store your data outside the United States, where the federal government has no jurisdiction to help if you have a problem with the vendor, Roman stated.

Dig Deeper Into Vendors' HIPAA Compliance

If you decide to move forward with using cloud storage, you must choose your vendor wisely. "We are seeing an increase in data breaches caused by vendors, so be cautious when choosing a vendor," Freedman cautioned.

But how can you assess a vendor's compliance with HIPAA? Freedman provided the following tips:

- Make sure the vendor will sign a BAA and will indemnify you fully for any and all data breaches that the vendor causes (not just up to the amount of the contract).
- Ask the vendor to see its HIPAA Compliance Program. "If they look at you sideways, that is a clue that they are clueless," Freedman pointed out.
- For a high-risk vendor, ask to see an executive summary of its security risk assessment.
- Have the vendor complete a security audit questionnaire.

Do Your Homework Before Jumping In

"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, Wieland and Freemire contended.

Bottom line: "Cloud computing has much to offer, and, with a careful assessment of risk 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," according to Wieland and Freemire.