TOP 10 Things to Consider About Omnibus for Cloud Storage

#1. The Omnibus rule introduces five major changes to the original HIPAA requirements.

Some of the changes to the original HIPAA requirements are directly related to the use of cloud services, while others are only loosely related or not related at all. In any case, healthcare providers must familiarize themselves with these changes. The following are the five areas in which the Omnibus rule introduces change:

- Omnibus requires breach notification for unsecured patient health information under the HITECH Act.
- There are more stringent limitations on the use of patient health information for marketing and fundraising. The sale of patient health information is also prohibited without individual authorization.
- Business associates — in this case cloud storage providers — are directly liable for compliance with privacy and security rules.
- The Omnibus rule uses the tiered civil monetary penalty structure established by the HITECH Act.
- The HIPAA privacy rule has been adapted to comply with the Genetic Information Nondiscrimination Act, which prohibits health plans from using or disclosing patients' genetic information.

#2. It is critically important to perform a full risk assessment prior to using a cloud storage provider.

Any organization that is subject to HIPAA regulations should perform a full-blown risk assessment on the cloud storage providers they are using or are considering using. Under the Omnibus rule, cloud providers are treated as business associates and are therefore required to adhere to the same privacy rules as the organizations whose data they store. As such, it is important to make sure that the cloud storage provider has a full compliance program in place. Some of the things to check for include the provider's continuity of business plan, its media disposal plan and its physical security.

TOP 10 Things to Consider About Omnibus for Cloud Storage

#3. Contracts with current cloud storage providers should be updated to include a business associate agreement.

Probably the single most important thing for healthcare providers to understand about cloud storage with regard to the Omnibus rule is that cloud storage providers are officially regarded by the government as business associates. This holds true for any cloud provider that is in possession of electronic protected health information, and the provider does not actually have to view the information in order for it to be considered a business associate. The Omnibus rule officially designates a provider as a business associate if it creates, receives, maintains or transmits electronic protected health information on behalf of a healthcare provider.

Because cloud storage providers are officially recognized as business associates, it is important for healthcare providers to get their cloud storage providers to sign a business associate agreement. This agreement is a legal document that acknowledges the relationship between the covered entity and the cloud storage provider and sets rules and expectations for each party. The agreement's main purpose is to convey to the cloud storage provider that as a business associate of a covered entity, it is required to take steps to implement appropriate safeguards (administrative, technical and physical) to protect the security and privacy of the data it is storing.

#4. The provider's audit record should be checked.

Under the Omnibus rule, the covered entity shares responsibility for a business associate's security. Given this fact, it would be extremely risky to simply accept a cloud storage provider's word when it claims to be HIPAA-compliant. It is critically important for healthcare organizations to do their due diligence and verify that their cloud storage providers are truly HIPAA-compliant.

One of the best ways to verify a cloud provider's HIPAA compliance is to ask to see its audit reports. In order for a cloud storage provider to be HIPAA-compliant, it must undergo an annual HIPAA audit. Additionally, this audit should conform to the OCR HIPAA Audit Protocol. The protocol was adopted in 2012 and serves as a set of guidelines stipulating how HIPAA audits should be performed.

TOP 10 Things to Consider About Omnibus for Cloud Storage

#5. What type of encryption does the provider offer?

One of the big myths about cloud storage is that data must be encrypted in order for the cloud storage provider to be HIPAA-compliant. Surprisingly, storage encryption is not mandated by HIPAA. However, even though an organization can achieve HIPAA compliance without storage encryption, it does not mean that it should.

Although not technically required, HIPAA encourages the use of storage encryption as a sort of "get out of jail free" card. As previously mentioned, one of the Omnibus requirements is that covered entities and business associates are responsible for sending the appropriate notifications in the event of a security breach. This requirement applies not only when a network has been hacked, but also when a device containing patient data is stolen.

When device theft occurs, the government usually imposes large fines. For example, in 2012, at least four organizations received multimillion-dollar fines from the U.S. Department of Health and Human Services for security breaches. The largest of those fines was $4.3 million. There were also numerous fines levied against smaller organizations, typically costing tens of thousands of dollars.

Fines (and the breach reporting requirement) could have been avoided in one particular case had a stolen laptop's hard disk been encrypted. Furthermore, this was far from being an isolated incident. There have been numerous cases over the past few years of covered entities receiving large fines as a result of devices containing unencrypted data being lost or stolen. Because a covered entity now shares responsibility when its business associate has a security breach, healthcare organizations should demand that their data be encrypted — both at the transport level and at the storage level — using NIST-approved encryption methods.

#6. How will using a cloud storage provider affect your continuity of business plan?

HIPAA has long required healthcare providers to establish a continuity of business plan that allows them to remain functional in the event of a large-scale disaster. The use of cloud storage was once hailed as a mechanism that could make it easier to maintain continuity of business because data is stored off-premises.

TOP 10 Things to Consider About Omnibus for Cloud Storage

While it is true that cloud storage can make it easier to develop a continuity of business plan, it is equally true that under the right circumstances, the cloud storage provider could become a single point of failure. That being the case, it is important to make sure that your cloud storage provider also has a continuity of business plan that will allow it to continue to operate in the event that its data center is struck by an unforeseen disaster.

#7. Are you confident in the provider's ability to prevent a security breach?

Obviously, no healthcare provider wants to have a security breach of any kind, but under the Omnibus rule, it becomes especially important to use a cloud storage provider you have confidence in when it comes to security. While it is true that the Omnibus rule makes business associates directly liable for security breaches, covered entities (health-care providers) are also held responsible. In other words, if your cloud service provider experiences a security breach, your organization shares responsibility for the breach under the Omnibus rule.

#8. What will the provider do with your data once it has it?

When a healthcare organization stores protected patient data in the cloud, it is essentially handing confidential data to another entity that operates outside of its direct control. That being the case, healthcare providers should insist that their cloud storage providers fully disclose in writing what they will do with the data once it is in their possession.

Normally, a cloud storage provider will do only that — store the data. However, it is in your best interest to insist on seeing the provider's data storage policy so that you can answer questions such as:

- Will the provider back up the data, and if so, what is its policy for data restoration?
- Are there circumstances in which the data will ever be read by the provider's staff?
- Are there situations in which the provider might turn data over to law enforcement, with or without a warrant?
- What happens if you exceed your storage quota?
- Does the provider have a contingency plan for returning your data to you in the event that it goes bankrupt?

In light of the Omnibus rule, you should also make sure that the provider in no way uses your data for any sort of marketing purposes. Omnibus prohibits using protected health information for marketing or fundraising purposes, except under very special circumstances.

http://www.hipaasurvivalguide.com/hipaa-omnibus-rule.php

#9. Is the cloud storage provider fully compliant?

This one is tricky, but it is a good idea to verify that the cloud storage provider is fully HIPAA-compliant. There are some cloud service providers that advertise themselves as being compliant with certain aspects of HIPAA, but they may not be fully compliant. Similarly, a cloud provider might advertise HIPAA compliance but use a less expensive, noncompliant data center unless a customer specifically requests HIPAA compliance.

#10. The cost of penalties have increased.

Another important thing to understand about the Omnibus rule is that penalty fees have increased. Omnibus uses the increased and tiered civil monetary penalty structure outlined in the HITECH Act.

As you can see, the Omnibus rule has a significant impact on healthcare providers, especially when it comes to cloud storage. As such, it is essential to use a cloud storage provider that fully grasps the requirements of the Omnibus rule.