Subject: Cloud Service Providers
Date: Tuesday, July 26, 2016 2:00:51 PM

Good afternoon –

If you review or negotiate Business Associate agreements for cloud services, please take a few minutes to read this short article and share it with others who negotiate BAAs – it might keep us from the $2.7M penalty that Oregon Health & Science University just paid for a HIPAA violation related to cloud services. Let me know if you have any question.

Thanks! Jill

Some cloud service providers and data centers have been in denial that they are HIPAA Business Associates. They refuse to sign Business Associate Agreements and comply with HIPAA.

Their excuses:

"We don't have access to the data so we aren't a HIPAA Business Associate."

"The data is encrypted so we aren't a HIPAA Business Associate."

Cloud and hosted phone vendors claim "We are a conduit where the data just passes through us temporarily so we aren't a HIPAA Business Associate."

"We tell people not to store PHI in our cloud so we aren't a HIPAA Business Associate."

Wrong. Wrong. Wrong. And Wrong.

2.7 million reasons Wrong.
Oregon Health & Science University (OHSU) just paid $2.7 million to settle a series of HIPAA data breaches "including the storage of the electronic protected health information (ePHI) of over 3,000 individuals on a cloud-based server without a business associate agreement."

Another recent penalty cost a medical practice $750,000 for sharing PHI with a vendor without having a Business Associate Agreement in place.

The 2013 changes to HIPAA that published in the Federal Register (with our emphasis) state that:

"…we have modified the definition of "business associate" to generally provide that a business associate includes a person who "creates, receives, maintains, or transmits" protected health information on behalf of a covered entity.

…an entity that maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the protected health information. We recognize that in both situations, the entity providing the service to the covered entity has the opportunity to access the protected health information. However, the difference between the two situations is the transient versus persistent nature of that opportunity. For example, 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."

A cloud service doesn't need access to PHI – it just needs to manage or store it– to be a Business Associate. They must secure PHI and sign Business Associate Agreements.

The free, consumer-grade versions of DropBox and Google Drive are not HIPAA compliant. But, the fee-based cloud services, that utilize higher levels of security and for which the vendor will sign a Business Associate Agreement, are OK to use. DropBox Business and Google Apps cost more but provide both security and HIPAA compliance. Make sure you select the right service for PHI.

Encryption

Encryption is a great way to protect health information, because the data is secure and the HIPAA Breach Notification Rule says that encrypted data that is lost or stolen is not a reportable breach.

However, encrypting data is not an exemption to being a Business Associate. Besides, many cloud vendors that deny they have access to encrypted data really do.

I know because I was the Chief Operating Officer for a cloud backup company. We told everyone that the client data was encrypted and we could not access it. The problem was that when someone had trouble recovering their data, the first thing our support team asked for were the encryption keys so we could help them. For medical clients that gave us access to unencrypted PHI.

I also know of situations where data was supposed to be encrypted but, because of human error, made it to the cloud unencrypted.

Simply remembering that Business Associates are covered in the HIPAA Privacy Rule while encryption is discussed in the Breach Notification Rule is an easy way to understand that encryption doesn't cancel out a vendor's status as a Business Associate.

Data Centers

A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate.

Taken together, a cloud vendor that stores PHI, and the data centers that house servers

and storage devices, are all HIPAA Business Associates. If you have your own servers containing PHI in a rack at a data center, that makes the data center a HIPAA Business Associate. If you use a cloud service for offsite backups, or file sharing, they and their data centers are Business Associates.

Most data centers offer 'Network Operations Center (NOC) services,' an on-site IT department that can go to a server rack to perform services, so you don't have to travel (sometimes across the country) to fix a problem. A data center manager was denying they had access to the servers locked in racks and cages, while we watched his NOC services technician open a locked rack to restart a client server.

Our client, who had its servers containing thousands of patient records housed in that data center, used the on-site NOC services when their servers needed maintenance or just to be manually restarted.

Cloud-Based and Hosted Phone Services

In the old days, a voice message left on a phone system was not tied to computers. Faxes were paper-in and paper-out between two fax machines.

HIPAA defines a conduit as a business that simply passes PHI and ePHI through their system, like the post office, FedX, UPS, phone companies and Internet Service Providers that simply transport data and do not ever store it. Paper-based faxing was exempt from HIPAA.

One way the world has changed is that Voice Over Internet Protocol (VOIP) systems, that are local or cloud-based, convert voice messages containing PHI into data files, which can then be stored for access through a portal, phone, or mobile device, or are attached to an e-mail.

Another change is that faxing PHI is now the creation of an image file, which is then transmitted through a fax number to a computer system that stores it for access through a portal, or attaches it to an e-mail.

Going back to the Federal Register statement that it is the *persistence* of storage that is the qualifier to be a Business Associate, the fact that the data files containing PHI are stored at the phone service means that the vendor is a Business Associate. It doesn't matter that the PHI started out as voice messages or faxes.

RingCentral is one hosted phone vendor that now offers a HIPAA-compliant phone solution. It encrypts voice and fax files during transit and when stored, and RingCentral will sign a Business Associate Agreement.

Don't Store PHI With Us

Telling clients not to store PHI, or stating that they are not allowed to do so in the fine print of an agreement or on a website, is just a wink-wink-nod-nod way of a cloud service or data center denying they are a Business Associate even though they know they are maintaining PHI.

Even if they refuse to work with medical clients, there are so many other types of organizations that are HIPAA Business Associates – malpractice defense law firms, accounting firms, billing companies, collections companies, insurance agents – they may as well give it up and just comply with HIPAA.

Jill Bush Raines
Assistant General Counsel, Office of Legal Counsel
and University Privacy Official
The University of Oklahoma
1105 N. Stonewall Avenue, Suite 221
Oklahoma City, OK 73117-1221
(405) 271-2033
(405) 271-1076 (fax)
jill-raines@ouhsc.edu