March 2020 | Volume 20, Issue No. 3

Briefings on HIPAA

Credit:Ipopba. Image Source: www.gettyimages.com

In this Issue

P1 **Navigating the challenges of a big tech partnership**
Hospitals must consider many factors when storing data with Google, Microsoft, or Amazon.

Navigating the challenges of a big tech partnership

As we move into a new decade, the burgeoning partnerships between giant tech companies and healthcare organizations bring great promise and many questions.

Google, Amazon, and Microsoft, among others, are swiftly entering the healthcare space. These companies can provide obvious benefits to both patients and healthcare organizations; medical records are more easily accessible for patients today than ever before, and at no other point in history have organizations been equipped with the tools to perform instant analysis on millions of records. The leading technologies provided by these companies can help healthcare organizations gain deep insight into trends that they otherwise might not be able to recognize.

Of course, the partnerships also raise concerns, particularly regarding patient privacy. Protected health information (PHI) is being shared by healthcare organizations and put into the hands of giant tech conglomerates, who may house the data in the cloud and provide solutions that organizations use to analyze the data. If the data is stored on a cloud-based service or the data is accessed by a vendor, the covered entity (CE) and the vendor are required to enter into a business associate agreement (BAA), which means the business associate (BA) must abide by relevant HIPAA regulations and adhere to the BA contract.

In 2019 we saw the formation of many partnerships between tech giants and prominent healthcare organizations. Cerner linked up with Amazon Web Services (AWS) as its preferred cloud provider. Mayo Clinic announced a 10-year partnership with Google last July. Mayo intends to "use advanced cloud computing, data analytics, machine learning and artificial intelligence to redefine healthcare delivery."

In addition to these partnerships, there has been a rise in the number of software as a service (SaaS) vendors building specialty products on cloud-based systems like AWS or Microsoft Azure, says **Chris Apgar, CISSP,** CEO and president of Apgar & Associates LLC in Portland, Oregon. In these instances, the CE is not entering into a BAA directly with the giant tech company, but rather with the specialty vendor to fill a specific need.

The big tech companies can provide sophisticated software, but CEs need to do their part too. There are many important steps that healthcare organizations must take as they aim to protect patient data in this new era of big tech partnership.

HCPro
a Simplify Compliance brand

Get specific in the contract

Healthcare organizations partnering with companies like Google, Microsoft, or AWS need to take the same approach they would take with a smaller vendor. The language of the BAA needs to be as specific as possible. This way, everyone is on the same page.

CEs need to be asking the following questions:

- Will the data be encrypted at rest? Who will have the keys?
- How is data in a virtual environment kept separate from others?
- What are the perimeter controls and firewalls?

Even when dealing with leading tech companies, healthcare organizations cannot make assumptions about the services that will be provided. Everything must be explicitly stated in the business contract.

"As an example, in AWS, I can set up an environment, but that doesn't mean it's secure," Apgar says. "It could be on an Amazon server and that Amazon server is secure, but I haven't paid for the bells and whistles to protect that information, such as generating and monitoring audit logs, deploying firewalls, and things like that. If you approach any of the big guys, you specifically have to say, 'I want a HIPAA-compliant environment' and be willing to pay for it."

One of the issues, though, is that tech giants are not generally willing to bend on some of the clauses within a BA contract. They present their version of the BAA to the healthcare provider, and it's up to the covered entity to sign it or walk away. There is often little room for negotiation, says **Kate Borten, CISSP, CISM, HCISPP**, founder of The Marblehead Group in Marblehead, Massachusetts.

"I have a philosophical problem with that, because the covered entity is really the organization that is responsible to the patient or the plan member," Borten says. "And the CEs are the ones that have the right and obligation to set the terms and set the control to dictate what downstream business associates can or cannot do with that patient data."

The time frame for incident and breach notification is a common point of contention and negotiation between CEs and BAs, says **Frank Ruelas, MBA**, principal of HIPAA College, based in Casa Grande, Arizona. HIPAA requires the BA to report a breach within 60 days, but CEs often push for a short deadline—five days, for example—to help protect themselves and their patients in the event of a breach. If the CE doesn't ask for a five-day deadline, the BA certainly won't volunteer it. And large tech companies typically don't make such a commitment in their version of the BA contract.

In addition to a timeline for breach notification, healthcare organizations should establish a business contract that specifically outlines the support CE will receive to restore data and the time it will take to resume full operations, says **Peyman Zand**, vice president of advisory services at CereCore in Nashville, Tennessee.

At times, healthcare organizations negotiate with their BAs about the BA contract language. If a CE encounters a large tech company with its own BA contract containing language that does not meet the CE's expectations, the CE must weigh the benefit of working with this BA against the security or privacy risks of a weaker contract. When a healthcare organization encounters a situation like this, it should take the minimum step of expressing its specific reservations in writing.

"If something happens down the road, at least you've got that," Borten says. "You've made a record that you're not thrilled with these terms and then you move on. It's unlike working with a smaller business associate where the covered entity can and should dictate the terms in that business associate contract."

Connect with other healthcare organizations

When CEs are contracting with cloud providers, it's always smart to check in with other healthcare organizations using that specific provider, Ruelas says.

Cloud-based vendors have well-developed books of clients. Touching base with just a few of them can give a healthcare organization a good idea of what to expect in the partnership and, by extension, what to consider including in the BAA. Genuine, real-time feedback

Questions Comments & Ideas

Contact Steve Andrews at *sandrews@hcpro.com*

from compliance officers at other hospitals can help shape an organization's expectations in dealing with a large tech vendor.

Properly de-identify PHI

As tech companies move into the healthcare space, the issue of identifiable health information becomes even more pressing.

Tech companies cannot sell PHI for research or marketing purposes, but "all bets are off" once the information has been de-identified, Borten says. According to HHS, the Privacy Rule does not restrict the use or disclosure of de-identified health information, as it is no longer considered PHI.

The tricky part is the process of de-identification.

Some organizations have standard BA contracts explicitly stating that they are not giving a tech vendor or another BA permission to de-identify PHI. Others may overlook the pitfalls associated with allowing a tech vendor to de-identify PHI. In some situations, this could be viewed as a cost of doing business with the vendor.

If the organization has granted permission for a BA to de-identify health data, it must be sure the de-identification process is carried out in the most effective way possible. The Privacy Rule outlines two methods for de-identification: safe harbor and expert determination.

Organizations using the safe harbor method must remove the following identifiers:

- Names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
  - 1) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people and
  - 2) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
- All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
- Telephone numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Fax numbers
- Device identifiers and serial numbers
- Email addresses
- Web Universal Resource Locators (URLs)
- Social Security numbers
- Internet Protocol (IP) addresses
- Medical record numbers
- Biometric identifiers, including finger and voice prints
- Health plan beneficiary numbers
- Full-face photographs and any comparable images
- Account numbers
- Any other unique identifying number, characteristic, or code,
- Certificate/license numbers

Since "Any other unique identifying number, characteristic, or code" is difficult, if not impossible, to determine without statistical expertise, the preferred method, according to Borten, is to de-identify data by expert determination. This usually entails employing a statistician to ensure that no combination of the remaining data could be used to identify an individual who is the subject of the information.

Keep the lines of communication open

Healthcare organizations should stay in frequent contact with their BAs, particularly the ones housing an abundance of PHI.

"The days of 'no news is good news' are long gone," Ruelas says. "You need to be knocking on the door and asking, because you need to be in a position to say, 'Look, I'm doing my best to keep up to date.' If you can show that you've worked with your business associate, especially those that are cloud-based, you're really trying to show that you are on the side of the individual. You are aligning yourself in a very positive manner when situations start to get dissected by the Office for Civil Rights."

This is a simple step, but an important one. CEs should be checking in with their cloud-based BAs every two weeks—or, at the very least, once per month—to ask about possible data breaches, Ruelas says. These are large vendors dealing with many contracts. Even if the BAA stipulates that the BA must notify the CE within two weeks of a security breach, the incident can still get lost in the shuffle.

"When you're talking about the megabytes if not gigabytes of data that are involved, why would you not want to take some level of simple effort?" Ruelas says. "I always laugh when somebody spends a half-hour explaining to me that they're too busy to do something that takes five minutes. But that seems to be the norm. I say, 'Get over it.' You're paid to do a job. Learn the tools that are available and do your job."

A proactive approach can make a world of difference when a breach occurs.

Understand security differences

Naturally, security solutions for cloud providers differ greatly from standard security methods when data is stored on the premises.

The most vulnerable periods, Zand says, are when the data is moved to the cloud and when data on the cloud needs to integrate with data that is either on-premises or in different locations.

For smaller organizations making the transition, an agreement with a cloud provider likely means the implementation of much stronger security solutions. The fact that these cloud providers are storing millions of health records makes them prime targets for hackers—"it's like a dangled carrot," Ruelas says—but it also forces them to employ unprecedented and constantly evolving levels of security.

IT security staff must be trained adequately. This also applies for healthcare organizations transitioning from one cloud service to another. As Borten indicates, the security solutions are specialized and differ from vendor to vendor.

In addition, healthcare organizations should be sure the security responsibilities are delineated. This requires effective communication between the CE and the BA. As the transition to the cloud is occurring and new security solutions are implemented, both parties need to be sure that there aren't any responsibilities falling through the cracks. ■