COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 18, Number 10. October 31, 2018 Start Slowly and Mind Security When Moving Data, Apps Into Cloud

By HCCA Staff

Health care organizations increasingly are seeking to move large parts of their data and applications—including protected health information (PHI)—into the cloud. The experience of one business associate (BA) illustrates what covered entities (CEs) and BAs need to consider when making this transition.

Nemi George, senior director of information security at Pacific Dental Services, says he's expecting improved security from the decision to move some PDS data functions to Amazon Web Services' (AWS) cloud.

"From my standpoint, security has always been a key aspect of going into the cloud," George says. "There is a debate on whether the cloud is more secure than [on premises]. I just believe that it's easier to get it right in the cloud, because there are less touch points for you if you're managing your infrastructure effectively."

Cloud's Worth on the Rise

A report released in August from MarketsandMarkets Research Private Ltd. estimates that the global health care cloud computing market will be worth nearly $45 billion in 2023, up from around $19.5 billion in 2018. That's an annual growth rate of 18.2%.

The key factors driving the growth of the market include increasing adoption of big data, wearables and internet-of-things in health care; improved storage, flexibility and scalability of data available in the cloud; and rapid changes in the overall health care industry.

According to MarketsandMarkets, the health care cloud computing market is segmented into clinical information systems and non-clinical information systems. In 2018, the clinical information systems segment is expected to account for the largest share of the global market, the report said.

Still, HIPAA-covered organizations that are considering a move into the cloud for some or all of their computing assets need to know that it won't solve all their security problems; they'll still need robust security systems and controls, tailored specifically for the cloud, experts say.

The Office for Civil Rights (OCR) has made it clear that cloud computing providers are considered BAs under HIPAA, and so health care organizations will need to have BA agreements (BAAs) in place if they're using cloud computing for any PHI that is not de-identified.

OCR offered guidance on cloud computing two years ago (*RPP 11/18, p. 5*). It said that CEs and BAs using cloud computing services must first understand the remote server environment of the provider, since the threats and vulnerabilities of the cloud service provider will affect the risk analysis and risk management plans of the CE and BA and thus the provisions of the BAA with the provider.

PDS offers business support to more than 650 dental practices, including assistance with marketing, information technology, accounting and finance, tax, personnel, legal, real estate, and other dental practice issues. "As a support services provider in the health care space, PDS is subject to HIPAA and other regulations," George says.

George, who spoke last month at a webinar on cloud computing, says that AWS makes it clear how security responsibilities are divvied up between the customer and AWS.

"For some businesses, there is some resistance to take that journey and migrate, especially in a heavily regulated environment such as health care," George says. "However, we made a strategic decision to move to the cloud about nine months ago." Some of the reasons to do this were obvious, he says. They included:

◆ Improved agility.

◆ Cost savings.

◆ Operational efficiency.

◆ Reduced infrastructure footprint.

◆ Scalability.

◆ Improved security.

"We decided to focus on the dental applications—the clinical applications that we support—and less on the infrastructure footprint that we were building," which PDS hoped would result in better operational efficiency, he says. "We started small. Our approach wasn't to go entirely cloud-based in one go. We started out looking at what are the things internally that we don't need to have on-premises."

Ultimately, the organization built a data warehouse cluster and a web application stack, then migrated its Remote Desktop Services cluster, Atlassian tool suite, and select legacy applications, George says.

Overall, this took 8 months, with the first 2 1/2 months devoted to strategy and proof of concept, another 4 1/2 months for data and app migration, 1 month for cloud transition, and then a period to run and optimize the system, he says.

The reduced infrastructure footprint was obvious immediately: "We went from 16 servers—16 racks within the data center—to just five with cloud adoption," George says.

In addition, the increased agility was apparent, he says. "We also noted the ability to scale easily up and down to support our growing customer base without the need to invest."

Other potential benefits, such as cost reduction, likely will be borne out but may prove more challenging. Moving to the cloud typically brings considerable cost savings, George says. "We have a more nimble, agile and adaptable environment able to focus on the areas we want to focus on, and also reduce our overall operating expenditures."

Still, even though the cloud can be less expensive initially, making the barrier for entry lower, "your recurring costs can spiral out of control if you're not managing this effectively," George says. "The cloud offers the ability to spin things up and down as needed. But it's very easy for people to turn things on, but not a lot of people go back to turn them off when they're not using them." Organizations need to keep tabs on the cloud resources they're using so that costs don't spiral out of control.

Moving to the cloud also presents some unique challenges, George says. First and foremost, making the move requires resources and expertise that your staff may not have, he says. "If you're looking to go into the cloud, then you need to start planning ahead on the people side," he says. "You may be using your existing team, so you need to make sure they have the relevant certifications and take the AWS training and certification program to ensure that they're ready to scale along with you."
