BUILDING TRUST IN THE CLOUD: OVERCOMING CYBERSECURITY CONCERNS TO REAP CLOUD'S BENEFITS

A recent HIMSS Media survey finds that security concerns are significantly limiting health care's use of cloud services. But in a few years, organizations may not have that choice.

By any indication, two major trends will dominate the health care industry in 2019: the growing presence of the cloud in health care and the increasingly complex cyber-threat landscape it finds itself in.

"Many vendors who provide critical applications – such as EMRs – are aggressively moving to the cloud. In many cases there will not be an option."

JOHN HOUSTON | VICE PRESIDENT, PRIVACY & INFORMATION SECURITY, ASSOCIATE COUNSEL | UPMC

The HIMSS Media survey, Cloud Security Insights, sponsored by the Center for Connected Medicine, sought to better understand attitudes and perceptions about cloud security among hospitals and health systems. It's findings: among the IT, cybersecurity and informatics professionals surveyed, more than half cited cybersecurity concerns as "significantly limiting" their use of cloud services.

The most commonly cited concerns with the cloud were theft of data, maintaining regulatory compliance, and managing identity and access. But when it came to making decisions to invest in new cloud applications or rip/replace existing applications, hospitals said they were investing in the cloud for both mission-critical and non-mission critical applications.

"They don't have a choice," John Houston, Vice President, Privacy & Information Security, Associate Counsel at UPMC, acknowledged. "Many vendors who provide critical applications – such as EMRs – are aggressively moving to the cloud. In many cases there will not be an option." The cloud is coming – now how do we address our concerns?

Trust in a black box

The survey found that while hospitals may have security concerns, less than 10 percent of respondents could point to a known security incident linked to cloud infrastructure or applications. Furthermore, respondents in IT and cybersecurity were even less likely to report a known security incident linked to the cloud; whereas nearly half of respondents in informatics roles were unsure of whether such an incident had occurred. It's hard to trust what you don't know.

As Houston explained, "When I can host an application within my data center, I control the servers and I can manage the security. As soon as I move to the cloud, I am now dependent upon a third party to ensure that that application is secure. It becomes a black box for me."

The challenge here, Houston points out, is that not every vendor is committed to security and understands what is involved in delivering an application that is truly secure. That's why in August of 2018, Houston banded together with CISOs from Wellforce/Tufts Medical Center, Cleveland Clinic, and other leading health systems to create the Provider Third Party Risk Management Council. The council works with HITRUST CSF and its assurance programs to better manage and streamline the security vetting process for third-party vendors. "Our aim is to put the responsibility on the vendor," he said. "If you want to do business with my organization, I need to see the certification that proves your application and infrastructure have appropriate security controls in place."

Private vs. public cloud

Nearly two-thirds of survey respondents claimed they "trust" public clouds to keep some health care data safe – but it depended on the type of data. Respondents were overall more comfortable putting health care data in a private cloud than in the public cloud. When asked about specific types of data, respondents were more comfortable putting de-identified EHR records or data from general business apps in the public cloud and more likely to put passwords, staff records and financial information in the private cloud.

This again points to vote of confidence. As Houston explained, "The private cloud can be viewed as an extension of your data center. A third party is still processing my data, but I have more control over it."

> *"If you go through a methodical process to define what your needs are, and part of that process involves security upfront, you can evaluate your options in the market, decide which one best meets your needs and then – and only then – move forward."*

To build comparable trust in the public cloud, Houston believes it's important for an organization to do its due diligence on the front end. And since many vendors today go to the end-user to sell their product, it's crucial for IT professionals to collaborate with their end-users from the start. "If you go through a methodical process to define what your needs are, and part of that process involves security upfront, you can evaluate your options in the market, decide which one best meets your needs and then – and only then – move forward," he said.

The choice

As cloud technology rapidly integrates into the care continuum, the industry must address concerns and misconceptions over data and cloud security. Houston predicts that five years from today, almost everything will be processed in the cloud: "We'll be faced with a new reality. So how do we address that reality rather than simply digging our heels in and saying no?" The work starts now to identify strategies that ensure health care's move to the cloud is secure, cost-effective and reliable.

Learn more about cloud security and the Center for Connected Medicine at www.connectedmed.com

Center for Connected Medicine

About The Center for Connected Medicine:
The Center for Connected Medicine (CCM) is a gathering place where those seeking to drive improvements in health care through technology come to connect with and inspire each other, both in the real and digital worlds. The CCM, operated by GE Healthcare, Nokia and UPMC, connects and inspires leaders and innovators to join the CCM community by cultivating thought-leadership activities, creating a relevant content hub, and fostering trusted relationships through exclusive events.