

Next-gen cloud computing: How healthcare can prepare for the future

Don't leave it up to tech vendors to drive the next phase of integrated data that gets channeled between doctors, payers, providers and patients.

By [Bill Siwicki](#)

August 01, 2018

10:22 AM



There has been a notable shift in healthcare clouds from simple data storage to using the technology to lower costs, gain efficiencies and even move on to tasks such as personalizing patient care.

Black Book Research, in fact, found that 93 percent of hospital CIOs are actively acquiring the staff to configure, manage and support a HIPAA-compliant cloud infrastructure.

This is happening as the service offerings of cloud technology vendors such as Amazon AWS, Google Cloud, IBM Cloud and Microsoft Azure, in particular, are constantly changing. What's more, 91 percent of CIOs in the Black Book survey report cloud computing is allowing more agile, nimble products and services with the proliferation of healthcare data.

So healthcare CIOs and other executives have to be prepared for the changing cloud landscape. Here's a look at what to expect in the near future.

Security and Blockchain

For the next generation of clouds, security is a big consideration moving forward by cloud technology vendors and healthcare organization clients alike.

"The cloud provider must ensure through regulatory audits that physical security requirements are effectively met, therefore, they are employing strict facility and asset access controls through a combination of biometric and token-based security protocols," said Black Book President Doug Brown.

In addition to security, multiple EHRs within the same health system can cause problems in patient identification and patient safety. At the same time, the promise of Blockchain technology for security and records is getting riper, and can meld into the cloud.

"The need for cybersecurity measures has never been more critical, and it's organic in the evolution of healthcare cloud computing," Brown said. "As more hospitals get serious about their unique needs for increased governance, risk management and business continuity measures, national organizations are working to see how Blockchain could be best applied and are about to open the floodgates."



"Forward-thinking healthcare organizations must embrace technology at every point of the patient's care. Specifically, those web-based technologies that allow us to comprehensively engage at the clinical level with the provider and the patient."

— Brian Owens, Bendcare

State of the art: real-time data

Moving into the next generation of cloud computing, healthcare organizations will have to embrace the knowledge that state of the art patient care requires state of the art data

in real time, said Brian Owens, chief technology officer and CIO at Bendcare, a national rheumatology group practice that uses cloud technology from CareCloud.

“Simply put, forward-thinking healthcare organizations must embrace technology at every point of the patient’s care,” Owens said. “Specifically, those web-based technologies that allow us to comprehensively engage at the clinical level with the provider and the patient. This must include EHR strategies certainly but should also extend to complementary mobile applications and Internet-based access points that integrate information from the entire clinical ecosystem to capture and support the needs of the patient.”

Hospitals also will need to commit to data partnering and information sharing, he said. Data is out there, but too often in the healthcare industry it is fragmented, incomplete and siloed. To truly understand what is best for a patient, and most importantly to allow providers to comprehensively understand how their treatment plan is affecting the patient’s disease state, providers must have the entire picture – and here, cloud computing can help, Owens said.

“This means finding ways to obtain, integrate and channel information from the physician, pharmacies, insurance companies, test providers, and even the patients themselves to create a holistic view of the patient journey,” he explained. “In addition to building and managing our own infrastructures and tools, we must create partnerships that allow information to deliver value in ever greater and ever more creative and immediate ways.”



"Efficient and crisp adoption of cloud IaaS/Platform/SaaS models in healthcare require adaptation from both the cloud service provider and the healthcare organization."

– Jim Fitzgerald, CloudWave

Adapt, collaborate and optimize

Jim Fitzgerald, chief strategy officer at CloudWave, a cloud technology vendor that focuses on healthcare, believes the next steps for the evolution of cloud technology in healthcare are for cloud services vendors and healthcare organizations to adapt, collaborate and optimize.

“Adapt is a simple term with a lot of technical depth behind it,” he said. “Efficient and crisp adoption of cloud IaaS/Platform/SaaS models in healthcare require adaptation from both the cloud service provider and the healthcare organization. The cloud service provider needs to take a step outside strict auto-provisioning and one-size-fits-all

models of provisioning compute, storage, networking, platform and security and adapt to the unique needs of healthcare applications that have a collected depth of industry content but are often not well-suited to cloud implementation.”

Using their technical expertise to create a bridge to cloud technology is a way cloud services providers can help the industry. Healthcare providers can assist and enable this adaptation process by doing inward-looking technology reviews and assessments that analyze their existing platforms and consider means of consolidation and aggregation that will allow successful, efficient adoption of a cloud model, Fitzgerald said.

“On another note, collaboration is essential to adaptation and essential to helping the healthcare industry take best advantage of cloud IT models,” he added. “From the vendor perspective, it means that signing an agreement and then leaving design and provisioning solely in the hands of the customer is not an acceptable or helpful practice. From the healthcare provider perspective, it means letting go of the ‘we’ll fix it in hardware’ paradigm and considering the overall needs of systems that might benefit from cloud migration.”

And optimization is the end goal, allowing the power of the cloud model to improve availability, security and recoverability for the healthcare enterprise while also developing new efficiencies – but new efficiencies compared to a secure, highly available environment, not necessarily what the healthcare provider was used to operating on premises, Fitzgerald explained.

“As in the prior steps, there is work here for both the cloud services provider and the healthcare provider, and both need to engage collaboratively,” he said. “A major wild card in this process is the vendors of healthcare software buying into migrating their underlying software architecture from 2000’s era client/server models to cloud native platform capabilities. This shift is slowly underway, and it is encouraging over the long term.”



"A huge barrier to cloud adoption is that healthcare organizations want to run their own private environments and do not trust public cloud providers to secure their data."

— Michael Robinson, VMware

Hybrid clouds

On another front, a hybrid cloud is a combination of public and private cloud technology to facilitate a secure cloud computing environment. Some experts believe next-generation cloud setups are going to rely heavily on hybrid technology.

For the next generation of cloud, healthcare organizations will need to embrace the hybrid cloud, said Michael Robinson, vice president of healthcare, North America, at VMware, a subsidiary of Dell that specializes in cloud infrastructure.

“This may sound very basic, but a huge barrier to cloud adoption – and tapping the efficiency and security gains that come with it – is that healthcare organizations and clinical labs want to run their own private environments and do not trust public cloud providers to secure their data,” Robinson said. “Healthcare IT is understandably security-focused, but the security risk to an organization is more heightened from a lost device or stolen password than it is a cloud breach of patient information.”

Trusting external cloud experts – who specialize, research and invest in developing a capable and secure cloud – will remove a lot of the burden of building and securing entire environments from the healthcare organization, allowing them to focus elsewhere, he added.

Additionally, healthcare organizations looking to the next generation of cloud technology will have to design with flexibility in mind, Robinson advised.

“While many graphics portray the move to cloud with a bridge, this image is not 100 percent accurate,” he explained. “Bridges are static structures and it takes a disruptive reconstruction to change the destination of that bridge. IT leaders must build flexibility into their cloud architectures so that they can take advantage of future circumstances, such as beneficial financial offerings, changes in business priority, and emerging or as yet to be defined technologies.”

This means that the cloud destination must be easy to add on to or change, without disrupting IT or business operations.

“Think of the cloud bridge as having many different on-ramps and exits that can be built in a matter of days without completely rebuilding the entire bridge,” he said. “IT leaders must consider many possible scenarios. Will cloud services always be in the cloud, or will there be a need to provide cloud analytics at facilities or remote locations? Building with flexibility is critical, and taking a platform-centric approach is foundational to enabling it.”

Twitter: [@SiwickiHealthIT](https://twitter.com/SiwickiHealthIT)

Email the writer: bill.siwicki@himssmedia.com