Answers to Healthcare Leaders' Cloud Questions

iHT2
Institute for Health
Technology Transformation

Contributing Executives

Jeff Pearson, MBA, CHCIO

Vice President, Chief Information Officer, Trinity Mother Frances Hospitals and Clinics

Chris Logan

CISO, Care New England

David Reis, PhD, CGEIT, CISSP, CRISC, ScrumMaster, CISO

VP of IT Governance, PMO and Security, Lahey Health

Luis Taveras, PhD, SVP

CIO, Barnabas Health

Drew Koerner

Chief Healthcare Solutions Architect, VMware

Table of Contents

Introduction

Compared to other industries, healthcare has been a relatively slow cloud adopter. While a KLAS Research survey in 2011 found that 55% of healthcare providers had something in the cloud, these included many different kinds of applications and data, ranging from e-mail to picture archiving and communications systems (PACS) to other kinds of clinical applications. Nearly a quarter of this group—largely physician practices and smaller community hospitals--had remotely hosted EHRs. But on the whole, respondents were reluctant to move their main information systems to the cloud.[1]

Two-thirds of the hospitals that were interested in the cloud, KLAS revealed, preferred "private clouds" that were dedicated to their data and applications. And, in a 2012 roundtable discussion conducted by the Health Information Management and Systems Society (HIMSS), senior health IT executives said they were more comfortable using a private cloud than the public cloud and were more likely to store administrative data than clinical data in the cloud.[2]

A HIMSS Analytics study published in mid-2014 showed healthcare providers' cloud usage accelerating. Of the 150 survey respondents—most of them hospitals and health systems—83% were using the cloud in some way. Half of those organizations had clinical applications in the cloud, and 73% used cloud services for administrative or IT functions. Three quarters of respondents were using private or hybrid cloud services that gave them more control over their data than if they'd put everything in the public cloud.[3] Just 23% said they were relying on the public cloud, compared to 39% of cloud users in all industries in a separate 2013 survey.[4]

The top reasons for adopting cloud services, HIMSS found, were cost (56%), speed of deployment (53%), lack of internal staff/expertise (52%), disaster recovery (50%), need for a scalable, always-on solution (45%), regulatory compliance (42%), security (27%), and workforce mobility (27%).

Among those providers that were not using the cloud, the major reasons were security (62%), a continuing focus on in-house IT operations (42%), and availability and uptime concerns (39%).

Other surveys and iHT[2] interviews with healthcare executives indicate that the most important concerns that healthcare organizations have about the cloud are related to security and control of data, regulatory compliance, availability, bandwidth, and cost. Nevertheless, it is clear that these concerns are gradually diminishing as providers begin to see the many benefits of going to the cloud. Those benefits include lower infrastructure costs, enhanced security, scalability, speed of deployment, the expertise of cloud services in running data centers, the ability to access and share data anywhere at any time, and the efficient use of health IT staff.

This paper will examine the barriers that still prevent many healthcare providers from adopting cloud computing. Those objections will be analyzed and balanced against cloud vendors' arguments in favor of the technology.

Security

Healthcare leaders point out that their business is different from others, because healthcare can mean the difference between life and death for some patients and can determine others' future quality of life. So when they talk about "mission critical" applications and data, they're not just referring to systems that keep their organizations running.

In addition, the healthcare business is regulated to an extent that would be almost inconceivable in any other industry except, perhaps, for airlines. The consequences of noncompliance with government regulations—particularly those related to data security and privacy—can be very significant for healthcare organizations, both in terms of fines and their ability to contract with Medicare and Medicaid. Moreover, data security breaches can expose organizations to very expensive lawsuits.

Despite these concerns, healthcare has not had a great track record on security. According to one survey, 19% of healthcare organizations had experienced a security breach in the previous year. From 2009 through 2013, 29.3 million patient records were compromised in 804 data breaches involving more than 500 records each. Theft accounted for 83% of the compromised records in 2013.[5]

Cloud services have not been exempt from security breaches, notes David Reis, CISO and vice president of IT governance, PMO and security at Lahey Health, based in Burlington, Mass. He cites the 2011 breach of 100 million user accounts on Sony's PlayStation 3 service, which was hosted by Amazon Web Services.[6]

Drew Koerner, chief healthcare solutions architect for VMWare, a cloud vendor, argues that, on the whole, cloud services provide better data security than healthcare organizations do. VMWare's own hosting environment, he says, is more secure than what's required by the HITRUST Common Security Framework, the gold standard for many healthcare providers.[7] Other organizations measure security with SAAE 16 Service Organization Control (SOC) reports on internal controls.[8]

According to the HIMSS survey, 27% of healthcare cloud users went to the cloud partly because they thought it would improve security. But our interviews show that there's still some distrust of the cloud in this respect.

Luis Taveras, CIO of Barnabas Health, based in Livingston, NJ, says that while he sees advantages in cloud computing, he's still concerned about security, including who has access to sensitive patient data and whether it will be encrypted in the cloud. Although he admits that cloud vendors may be more sophisticated and have more resources than Barnabas does, he still feels more comfortable with his own organization's security procedures than with those of cloud services.

According to the HIMSS survey, 27% of healthcare cloud users went to the cloud partly because they thought it would improve security. But our interviews show that there's still some distrust of the cloud in this respect.

Security

Jeff Pearson, vice president and CIO at Trinity Mother Frances Hospitals and Clinics, based in Tyler, Tex., sees a rising level of comfort with cloud security among healthcare executives. This is partly because more and more cloud vendors are signing business associate agreements that describe the extent of their liability under the privacy and security regulations of the Health Insurance Portability and Accountability Act (HIPAA).[9] However, he notes, "Your name and your reputation are always at stake if there's a security breach. So you have to worry that it you make a poor choice of a cloud vendor, your organization is still going to suffer."

Keeping data separate

Some providers are concerned that if they use shared infrastructure in the public cloud, their data may be commingled with that of other companies. Chris Logan, chief information security officer of Care New England, based in Providence, R.I., notes that Cerner hosts his organization's EHR remotely and that he is broadly open to expanding its cloud operations. But Care New England still prefers a dedicated infrastructure to placing its data in a multi-tenant public cloud.

"Most cloud vendors have huge servers and are carving pieces up to give to customers," he notes. "The thing that scares me about that is, what if the controls aren't in place and my data slips into somebody else's environment, or their data slips into my environment? What's the downstream issue there? What's the effect? It's significant."

Koerner says that a multi-tenant server does not present a security problem for VMWare's customers, because each environment on the server is strictly segregated from the others. If a virus attacked one part of a server, for example, it could not spread to other environments, "because it's completely segmented off."

As for Taveras' question about encryption, he notes that it is up to individual customers to encrypt their data in cloud storage. "If all they did was buy a chunk of cloud hybrid service, then all the traffic and all the access and the related pieces would be encrypted. But as far as the storage itself, that would not be encrypted unless they did it themselves."

VMWare's cloud service is SAML-certified for user authentication. Some providers view that certification as a safeguard for single sign-on access to their applications. In addition, Koerner notes, the vendor allows customers to see who has accessed every piece of data as part of its compliance with HIPAA auditing procedures.

Koerner says that a multi-tenant server does not present a security problem for VMWare's customers, because each environment on the server is strictly segregated from the others. If a virus attacked one part of a server, for example, it could not spread to other environments, "because it's completely segmented off."

Compliance

Healthcare is a highly regulated industry. HIPAA security and privacy rules govern the use of health IT by HIPAA-covered entities, which include all healthcare providers and health insurers. Another federal rule restricts access to information about substance abuse,[10] and most states have their own privacy regulations governing mental health and substance abuse records. In addition, 47 states require notification of individuals affected by security breaches.[11]

Some cloud vendors advertise that they have HIPAA-compliant data centers. Reis is not impressed, because many smaller vendors don't actually run their own data centers. Instead, he notes, they contract their operations to Amazon Web Services, which is estimated to have a 70% market share.

Some cloud vendors advertise that they have HIPAA-compliant data centers. Reis is not impressed, because many smaller vendors don't actually run their own data centers. Instead, he notes, they contract their operations to Amazon Web Services, which is estimated to have a 70% market share.

Amazon is well aware of what's required to conform with HIPAA requirements and has published documentation of that, Reis says. But some cloud vendors aren't sophisticated enough to know about those requirements and haven't configured their web services to comply with HIPAA, he avers.

HIPAA final rule

On Jan. 25, 2013, the Department of Health and Human Services (HHS) published an Omnibus Final Rule that implemented provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. This final rule significantly modified the existing HIPAA security and privacy regulations. Among other things, it conferred new obligations on business associates of HIPAA-covered entities and their subcontractors.[12]

Even before this final rule, healthcare providers were required to enter business associate agreements (BAAs) with their business associates, and some cloud vendors had BAAs in place with their healthcare customers. The HIPAA final rule, however, specifically defines cloud services as business associates, and it significantly expands the obligations of all BAs. Not only do BAs have to comply with HIPAA security rules, but they also have direct liability for security breaches and must sign BAAs with certain subcontractors. Moreover, business associates must report a security or privacy breach both to HHS and to the affected individuals.[13]

Compliance

Many cloud vendors, including Amazon, Microsoft, Google, Verizon, Dell, Box and VMWare, now offer BAAs to their customers. But most healthcare organizations want to use their own agreements or modify the vendor pacts.

Reis explains why: Cloud services, he notes, will agree to pay for direct damages in the event of a breach caused by their negligence. But they try to minimize their liability by capping the amount they'll pay if a class action suit is filed against the provider. Typically, that's where the bulk of the cost is.

"There's a modicum of comfort associated with the signing of a BAA, but it's not a panacea for the problem," he says.

Taveras agrees. "We have BAAs with everybody that we deal with, but that's a contractual vehicle to deal with a breach. I just don't want to deal with a breach. It's not the right thing for us to expose our patient data."

Reis explains why: Cloud services, he notes, will agree to pay for direct damages in the event of a breach caused by their negligence. But they try to minimize their liability by capping the amount they'll pay if a class action suit is filed against the provider. Typically, that's where the bulk of the cost is.

Availability

Healthcare providers must have patient information available to them at all times. Therefore, the availability of that data from a cloud service is a key consideration in deciding whether to go to the cloud.

Availability can be divided into two parts: the reliability of cloud vendors and disaster recovery. Healthcare providers tend to rate the cloud's disaster recovery capabilities highly, while remaining skeptical about its day-to-day reliability. But cloud vendors argue that their data centers are far more reliable than on-premises information systems are, because this is their core competency.

In fact, says Koerner, the biggest reason for healthcare organizations to use the cloud is that "their business is to take care of patients and not run a data center. Most on-premises systems have downtimes, and the people who run the cloud-based infrastructure—including us—have got ten times less downtime than you would have within an on-prem system," he says.

One minute of downtime in a 500-bed hospital costs $264, according to VMWare research. On average, these large hospitals have 1% of downtime a year, which costs them $4 million each. "If you can reduce that downtime cost and increase the availability of those servers, that's a big thing," Koerner says.

Among the reasons why the leading cloud vendors are so reliable, he explains, is that they constantly upgrade and add new servers that have the latest technology. They have the best firmware available. They understand how to prevent problems with incompatibility between hardware components. And the physical environments of their data centers are superior to those in many hospitals.

VMWare, he said, hasn't had a single outage in the past year with any of its healthcare customers. Some other cloud vendors may have similar track records. But 23% of the cloud users in the HIMSS survey said they'd had downtime or occasions when their data was unavailable. A third of cloud users said they'd experienced slow responsiveness of hosted applications and/or data.[14]

One minute of downtime in a 500-bed hospital costs $264, according to VMWare research. On average, these large hospitals have 1% of downtime a year, which costs them $4 million each. "If you can reduce that downtime cost and increase the availability of those servers, that's a big thing," Koerner says.

Availability

Service level agreements

One way that cloud vendors seek to assure customers that their data will always be available is by signing service-level agreements (SLA) that specify a certain level of uptime and penalties for failing to achieve that level. VMware, for example, specifies in its SLAs that the data will be available 99.999 of the time. According to Koerner, any cloud vendor worth its salt should be able to promise three nines to the right of the decimal point. Nearly half of the HIMSS cloud users said their SLAs specified at least two nines.

Reis claims that SLAs are unsatisfactory in healthcare, because healthcare organizations need to know there will be zero downtime. But Logan notes that under the 99.9% SLA that Care New England has with Cerner, that company can have outages totaling half an hour per year without triggering the penalty clause. While Cerner hasn't exceeded that so far, Care New England has "downtime-based PCs that can deliver census-based data to the clinicians should the EHR not be available to them," he says. This includes ADT information and "everything they need to process that patient and document their care in the proper manner."

Pearson is worried about the additive effect of external and internal downtime. That includes the possibility of the Internet going down, as well as network effects. "If the internal ring goes down, you can't get to the externally hosted system, and you can't get to the internally hosted system," he points out.

In the past, he adds, "We've had isolated outages to some of our clinics, sometimes because they lose power. We've also had maintenance outages caused by the broadband vendor."

Providers are concerned about the possibility of losing Internet access, which would be a disaster if their data were in the cloud. Trinity Mother Frances is about to activate a connection with a second Internet service provider for redundancy, and Care New England already has multiple ISPs. "We just have to ensure that the Internet pipe that we've established to Kansas City is constantly up and running," Logan says.

> Pearson is worried
>
> **about the additive effect of external and internal downtime. That includes the possibility of the Internet going down, as well as network effects. "If the internal ring goes down, you can't get to the externally hosted system, and you can't get to the internally hosted system," he points out.**

Availability

Backup and disaster recovery

The other side of the availability coin is backup for disaster recovery. Organizations with on-premises systems typically make flash copies of their hard drives once a day and also create tapes for longer-term, off-premises backup, notes Koerner.

If a healthcare provider uses the cloud for its primary storage of data and applications, the cloud vendor can restore an EHR down to the individual file level if something gets corrupted, he says. To do that with on-prem data storage, he points out, "You'd have to have a fully redundant environment sitting there. That's very expensive. At a bare minimum, you'd need to replicate storage to a secondary system."

If your on-premises data center went down, you could run in a "crippled mode" with 50%-75% of full capacity, he says. "In the cloud, you'd be 100% up and ready to go in the same environment with the same performance" as the original server had.

Lahey Health is fully prepared for disasters with its on-premise system, Reis says. "We have two data centers mirrored with like equipment purchased at the same time, with a portable [Oracle] Data Guard between the centers," he notes. "In cases where we can't use Data Guard, we're using VMax from EMC—a SAM-to-SAM application—and the data is kept completely in synch at the hardware level. If one data center goes down, the other can take up where it left off, with no data loss."

Barnabas Health also uses mirrored data centers for backup, Taveras says. The only problem with the setup, he says is that the servers are not yet in synch with each other, so they can't replicate the data right up to the minute.

Some providers have outside parties host their secondary data centers. That's the case at Trinity Mother Frances, which recently contracted with an external hosting vendor to back up its Epic EHR.

If a healthcare provider uses the cloud for its primary storage of data and applications, the cloud vendor can restore an EHR down to the individual file level if something gets corrupted, he says. To do that with on-prem data storage, he points out, "You'd have to have a fully redundant environment sitting there. That's very expensive. At a bare minimum, you'd need to replicate storage to a secondary system."

Bandwidth

As recently as 10 years ago, Internet bandwidth was too limited and computers were too slow to provide good service to physicians who used cloud-based EHRs. But now that has all changed with the explosion of computing speed and power. As a result, more and more physicians and hospitals are using remotely hosted systems.

Although broadband is not available everywhere, bandwidth is no longer a problem in 95%-99% of the country, Koerner says. That's partly because the technology used to access remote servers has improved. This began some years ago with Citrix, which hosted data and applications for thin-client networks. Today, he says, VMWare uses optimized display technology that is based on embedded DisplayPort (eDP) and is highly efficient.

"Gaining access to the full virtual desktop only requires 50K per connection now, depending on workload. So a T-1 line out to rural Nebraska should be enough."

Sending diagnostic images over the Internet is still a challenge, however, he notes. Using a build-to-loss protocol, a cloud service can download an image to a user, but it's not of diagnostic quality.

"You wouldn't do diagnostic-quality images across a T-1 anyway," he points out. "What we recommend is that you do the initial read of the image [on a network PC] and then decide whether you need to come into the radiology workstation."

If providers use the cloud for backup, they should also look at the cost of the bandwidth required to replicate their data in real time, Pearson observes. Those costs have come down so much, he said, that organizations like his can afford to have a secondary data center hosted. Moreover, the amount of bandwidth has increased dramatically, he says. "You spend less to get 10 times the bandwidth you used to be able to get."

If providers use the cloud for backup, they should also look at the cost of the bandwidth required to replicate their data in real time, Pearson observes. Those costs have come down so much, he said, that organizations like his can afford to have a secondary data center hosted. Moreover, the amount of bandwidth has increased dramatically, he says. "You spend less to get 10 times the bandwidth you used to be able to get."

For its Cerner-hosted system, Care New England bought extra bandwidth to handle "bursts" of user demand that tax the system's resources. "That extra bandwidth is critical to ensure availability," Logan notes. But with telehealth and genomic data coming down the pike, much more bandwidth will be needed in the future, he says.

Cost

The cost of going to the cloud is hard to compare with the cost of buying and maintaining an on-premise system because the two approaches use different business models. While there's a bigger upfront cost associated with purchasing your own system, including the required servers, the long-term cost of having your applications and data hosted in the cloud can be similar or even higher, providers say. That's because the cloud vendor charges a monthly fee that generates substantial costs over time.

Koerner argues that healthcare providers can save 20% if they choose a dedicated infrastructure in the cloud and 40% if they're willing to share data centers, compared to the cost of operating their systems onsite. To calculate the potential savings, he says, you have to include the cost of servers, replacement equipment, stored arrays, maintenance, power, and IT staff over a five-year period.

Organizations do not necessarily reduce their staff when they go to the cloud, he acknowledges. "They just become more efficient at what they do. They can handle more projects."

That's an advantage that appeals to Taveras. With the ongoing shift to value-based reimbursement, he says, the number of IT projects at Barnabas Health has multiplied, but his staff spends 80% of their time supporting operations. He'd like to reverse that ratio. "We need to have people doing 80% value-added work and 20% support."

Reis is dubious that IT staff will save that much time on operations, however, because some applications and databases will still have to be supported onsite. "Going to the cloud doesn't get rid of all of my infrastructure," he points out.

Pearson looked at the comparative costs closely before Trinity Mother Frances decided to hire an outside vendor, Sungard, to host the secondary data center for its Epic system. While he didn't find that the 10-year cost of external hosting was less than that of buying a system and hosting it on-premise, he said the costs have come much closer in recent years, partly because of the cloud's economies of scale.

Overall, he says, "You can get a higher degree of business continuity, disaster recovery, and backup and storage in the cloud and get it for less money because of the way that cloud vendors are able to spread that over multiple customers."

> Koerner argues
>
> **that healthcare providers can save 20% if they choose a dedicated infrastructure in the cloud and 40% if they're willing to share data centers, compared to the cost of operating their systems onsite. To calculate the potential savings, he says, you have to include the cost of servers, replacement equipment, stored arrays, maintenance, power, and IT staff over a five-year period.**

Cost

Operating vs. capital budget

Reis points to a little-noticed cost factor that discourages some not-for-profit institutions from employing cloud services. “Most cloud services are by subscription, and subscription fees come out of our operating budget. When we buy a system, we can capitalize that cost and it doesn’t count against our operating budget. So financing these cloud services is a very significant inhibitor.”

Paying monthly fees to cloud vendors, he continues, reduces the amount of money available to cover other operating expenses, such as rent, staff, and training. Moreover, it lowers the organization’s operating margin and, ultimately, reduces its bottom line. That, in turn, can affect bond ratings, increasing the organization’s borrowing costs. The ability to borrow for capital investments is critical to not-for-profits that can’t raise money on the stock market.

“This has been a significant conversation at Lahey for the 2 ½ years I’ve been here,” Reis says. “It’s the undiscussed story of the cloud. It was true at the organizations I worked at before, and it’s true at Lahey.”

Logan agrees that the cloud business model can be an issue in healthcare bond ratings. But he argues that an organization’s overall financial management is more important to bondholders than how it allocates its operating budget. If the organization pays close attention to balancing expenses against revenues and meeting its financial obligations, migration to the cloud should not materially affect its borrowing ability, he says.

Care New England’s finance people were concerned about the loss of tax-deductible depreciation when the organization adopted Cerner’s cloud version, Logan adds. But over a 10-year period, “the model for hosting was much more desirable,” he says, because it would have been a struggle to finance the large upfront cost of an onsite data center and the IT staff to support it.

Paying monthly fees to cloud vendors, he continues, reduces the amount of money available to cover other operating expenses, such as rent, staff, and training. Moreover, it lowers the organization’s operating margin and, ultimately, reduces its bottom line. That, in turn, can affect bond ratings, increasing the organization’s borrowing costs. The ability to borrow for capital investments is critical to not-for-profits that can’t raise money on the stock market.

Other Challenges

The abovementioned issues are the greatest concerns for the healthcare executives who were interviewed for this paper. But other factors also affect the decisions of healthcare organizations, including perceived technical complexity, the hiring and retention of qualified IT staff, the cost of data storage, and the details of migrating systems to the cloud.

In a 2013 survey by North Bridge Partners, 65% of respondents from all industries cited reliability/bandwidth/complexity as among their main concerns about going to the cloud.[15] Our contributors, however, don't believe that operating in the cloud is any more complex than running on-premises systems.

Taveras, for instance, says, "I don't see any additional complications in a hybrid [cloud] environment. It would be less complicated. Of course, if you make that commitment, the more you push up to the cloud, the better off you'll be."

Koerner also dismisses the notion that healthcare systems are too complex to transfer to the cloud or that it's too complicated to run both on-premise and cloud-based systems in a hybrid scenario.

"The reality is that the application doesn't care whether it's in the cloud or not," he notes. "When you apply our software layer, it's the same exact view as if the servers or the storage were on-premises. But you don't have to worry about installing the server, the amber lights on the driver array, the interconnectivity on the back of the switches for unified communications—you don't have to worry about any of that stuff. You're on step 2 of 3, and all that complexity should be gone."

Regarding software upgrades, he points out, "The whole environment could be in the cloud, or just the test component of that could be in the cloud. In the latter case, you could use the [public] cloud to get the upgrade up more quickly and move it onto your private cloud."

A major software upgrade typically takes a hospital a couple of months, he notes. By using the cloud as a test environment, an organization could have the upgrade up and running in a fraction of that time. The provider could also customize an application just as easily in the cloud as on premise, as long as it puts the network piece in place first to ensure security, he adds.

In a 2013 survey by North Bridge Partners, 65% of respondents from all industries cited reliability/bandwidth/complexity as among their main concerns about going to the cloud. Our contributors, however, don't believe that operating in the cloud is any more complex than running on-premises systems.

Other Challenges

IT staff

IT staff shortages have been worsening in the healthcare industry in recent years, and Logan believes this factor will push more and more provider organizations to the cloud.

For example, Care New England is now considering the best way to bring its three hospitals and its large employed physician group into a single, interconnected clinical system to meet the challenges of Meaningful Use and accountable care, Logan notes. The organization recently implemented an Epic ambulatory EHR to replace a number of disparate EHRs used in its physician practices. But it still uses the hosted version of Cerner in its flagship hospital; another recently acquired hospital has Meditech.

In considering whether to switch everything to Epic, Logan says, his organization has to consider the cost of building an on-prem system, because Epic does not offer a cloud version. One of the major costs of doing that, he notes, would be finding an adequate number of experienced IT people. This was also an issue when Care New England earlier selected Cerner: it would have been very expensive to recruit and train the IT staff to support an on-prem system.

Currently, he says, many northeastern healthcare systems—including Partners Healthcare, Yale Medical Center, Dartmouth-Hitchcock, and Lifespan—are moving toward Epic or have already adopted it. “That requires a lot of human resources, and there’s not enough to play with at this point in time,” he notes. “There’s nobody available in the market space that we can hire.” Hiring people from out of state would add more cost, he points out.

Besides technicians who are trained on Epic, there’s also a shortage of IT staff who know how to implement and operate other vendors’ systems, he adds. “As we’re being forced to adopt electronic information systems across all of healthcare, there’s not enough qualified people to do that work.”

Besides technicians who are trained on Epic, there’s also a shortage of IT staff who know how to implement and operate other vendors’ systems, he adds. “As we’re being forced to adopt electronic information systems across all of healthcare, there’s not enough qualified people to do that work.”

Other Challenges

Data storage

Another challenge that the cloud could help providers meet is the growing demand for data storage. Currently, many organizations are seeing quantum leaps in the amount of storage space they need, mainly to store images from increasingly data-hungry imaging devices. But other demands loom from health information exchange, telehealth, and genomic research, as well.

Care New England, which includes an academic medical center, has brought in a genomic researcher who is mapping 500 patients' genomes, "and we can't scale up that fast" for storage, Logan says. So the organization is considering cloud-based storage, which would allow other researchers across the country to share the data.

Although Trinity is not yet storing genomic data, Pearson agrees that on-premise data storage is getting very expensive, partly because of imaging. The cost of storage eats up a significant percentage of his capital budget, leaving less than he'd like to spend on other projects. That was the main reason, he says, that Trinity switched to Office 365 for email: the cloud provides plenty of storage at an affordable cost.

Migration to the cloud

Most providers that use cloud-based services have adopted them for only some of their systems. Even Care New England is using it mainly for the Cerner inpatient EHR, and Trinity is using the cloud for its secondary data center, Office 365, and its MultiPro HR system, which is being hosted by the vendor. The prevailing wisdom is that, even if a provider is willing to try the public cloud, it should retain some of its IT operations onsite in a hybrid arrangement.

VMWare recommends this hybrid approach for healthcare providers. Initially, Koerner advises them to migrate some legacy applications and disaster recovery/backup to the cloud. Some customers, he adds, do projects in the cloud. Another way to test the waters, he says, is to use the cloud for ambulatory EHRs that are going to be phased out when a healthcare system moves to a centralized EHR.

Despite Logan's reservations about the public cloud, he believes that Care New England will eventually use it for some applications and data. The secondary data center for the organization's new Epic ambulatory system—which is located in a different state--is costing the organization a significant amount. It would be much less expensive, he indicates, to do that backup in the cloud.

VMWare recommends

this hybrid approach for healthcare providers. Initially, Koerner advises them to migrate some legacy applications and disaster recovery/backup to the cloud. Some customers, he adds, do projects in the cloud. Another way to test the waters, he says, is to use the cloud for ambulatory EHRs that are going to be phased out when a healthcare system moves to a centralized EHR.

Conclusion

While many healthcare providers continue to have reservations about the cloud, surveys show a trend toward increasing acceptance of the new technology, and the interviews we did confirm that. Three of the four healthcare executives who contributed to this paper represent organizations that are using cloud services to varying extents; the fourth uses an on-premise Epic system for most of its IT needs.

Some EHR vendors are slowing their customers' migration to the cloud, notes Pearson. Either they don't offer remotely hosted versions or they don't support customers who use third-party cloud vendors to host their products. But he predicts that these EHR companies will change their policies, just as they did with Citrix and virtualization. When they do, he says, more providers will switch to the cloud.

"If I were in an organization that was going to Epic a few years from now, and they had a hosting cloud option, I'd be a very strong advocate for seriously considering it over building out our own servers and doing it ourselves," he says.

In general, he says, the cloud vendors' expertise and economies of scale allow them "to do more advanced and interesting things with the technology than we're able to do, because we don't have the skills. If a new application comes along that we need, and there's an option to remote-host it, I'll look at it pretty carefully."

Taveras has not progressed to this point yet. But he says he's leaning toward increasing Barnabas Health's cloud involvement, which at this point is mostly limited to remote hosting of its Oracle People Soft financial application. "We're almost there for our own private cloud, but I still have security concerns and other concerns," he says. "I'm getting there, but I'm not there yet."

Koerner recalls that in a recent focus group with healthcare executives, they told him they'd consider moving to the cloud if their main issues were addressed.

"Providers' business is taking care of patients, not running data centers," he observes. "The smart CIOs realize that. They're all ready to move, but you need to take care of the cost, the security and the availability."

Action Points

- Security: Healthcare providers are feeling more comfortable about cloud security, partly because many cloud vendors are signing business associate agreements (BAAs). Cloud services say their data centers are more secure than on-premise operations because they have a higher degree of expertise than providers do.

- Compliance: New HIPAA rules define cloud services as business associates of healthcare organizations and increase their obligations to protect security and report breaches. Cloud vendors are paying much more attention to HIPAA than they used to, although there are still concerns about smaller vendors that use Amazon or other big hosting services.

- Availability: Cloud services have less downtime than the typical healthcare system does, because this is their core competency. They also provide a superior disaster recovery and backup resource. Healthcare providers are starting to believe in the reliability of cloud vendors, and some view hosted backup as a cost-effective alternative to on-premise backup.

- Bandwidth: Much more bandwidth is available at lower cost than in the past. Broadband is more widely available, and new display technologies make it possible to use the cloud in the most remote areas.

- Cost: While the cloud subscription model is very different from the on-premise approach to creating a health IT infrastructure, the costs of these alternatives are starting to even out. One cloud vendor says that over a 5-year period, providers can save 20% by using a private cloud and 40% in the public cloud.

- Complexity: Both vendors and providers agree that managing an IT system is no more complex in the cloud than on-premises; in fact, it should be less complex. That's true even if an organization chooses to use a hybrid cloud.

- IT support: Going to the cloud can free up IT staff time to work on projects that are vital to a healthcare organization. Because of the high cost of recruiting trained staff, more organizations are likely to favor the cloud over building new or additional infrastructure on premises.

Notes

1. Ken Terry, “Cloud computing in healthcare: the question is not if, but when,” FierceHealthIT, Jan. 9, 2012, http://www.fiercehealthit.com/story/cloud-computing-healthcare-question-not-if-when/2012-01-09
2. Terry, “Health IT Execs’ Top Worries: Security, BYOD, Cloud,” InformationWeek Healthcare, May 9, 2013, http://www.darkreading.com/risk-management/health-it-execs-top-worries-security-byod-cloud/d/d-id/1109883?
3. “2014 HIMSS Analytics Cloud Survey,” June 2014, http://apps.himss.org/content/files/HIMSSAnalytics2014CloudSurvey.pdf
4. North Bridge Venture Partners, “The Future of Cloud Computing: 2013 Survey Results,” http://northbridge.com/2013-cloud-computing-survey
5. EMC, “EMC IT Trust Curve: 2013 Survey Results,” http://www.emc.com/campaign/it-trust-curve/index.htm
6. Joseph Galante, Olgha Kharif and Pavel Alpeyev, “Sony Network Breach Shows Amazon Cloud’s Appeal for Hackers,” Bloomberg News, May 16, 2011, http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html
7. HITRUST Common Security Framework, http://hitrustalliance.net/content/uploads/2014/05/HITRUST_CSF_v6_2014.pdf
8. American Institute of CPAs, “Service Organization Control (SOC) Reports,” http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/sorhome.aspx
9. Terry, “Microsoft Updates Cloud Agreement for HIPAA Rules,” InformationWeek Healthcare, April 30, 2013, http://www.informationweek.com/regulations/microsoft-updates-cloud-agreement-for-hipaa-rules/d/d-id/1109753?
10. Substance Abuse and Mental Health Services Administration, “Health Information Privacy: Substance Abuse Confidentiality Regulations,” http://www.samhsa.gov/healthprivacy/
11. National Council of State Legislatures, “Security Breach Notification Laws,” April 11, 2014, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
12. Department of Health and Human Services press release, “New rule protects patient privacy, secures health information,” Jan. 17, 2013, http://www.hhs.gov/news/press/2013pres/01/20130117b.html
13. Godfrey & Kahn, “HIPAA Omnibus Final Rule Has Important Changes for Business Associates and Covered Entities,” March 25, 2013, http://www.gklaw.com/news.cfm?action=pub_detail&publication_id=1270
14. “2014 HIMSS Analytics Cloud Survey”
15. “The Future of Cloud Computing: 2013 Survey Results”

Institute for Health Technology Transformation
244 5th Ave #2150
New York, NY 10001

iHT² Institute for Health Technology Transformation