Healthcare Cloud Is Rolling In

Cloud computing offers important economic and research benefits for healthcare organizations. But are cloud services a safe place for such sensitive data?

Healthcare Cloud Helps Patients, Research—But Has IT Risks

Several years back, I cut my arm on a neighbor's old chain link fence. The wound got infected, and I eventually ended up in the ER.

And sure enough, I was asked if I had received a tetanus shot in the past five years. I had no idea, and unfortunately none of my healthcare records were available for reference in the cloud at the time.

Ouch. That needle hurt.

The shot stung me figuratively, too, as I pondered why I didn't have easier access to my medical records. Granted, there are EHRs not in the cloud even today, but in the big picture, we're all heading there—whether we go willingly or kick and scream our way down the road.

It's not just electronic records, either. Storage, software as a service, platforms, digital imaging and research all have a place in the healthcare cloud. In this handbook, news writer Kristen Lee offers a fascinating story about Nationwide Children's Hospital and a technology vendor working together to perform genomic studies using Amazon Web Services.

The core of the research resides in an algorithm developed by the hospital, which the development team eventually realized could scale up well in the cloud.

It's not just EHRs. Storage, software as a service, platforms, digital imaging and research all have a place in the healthcare cloud.

Having done some prior work covering genomics, I know the amount of data that comes from mapping a genome is staggering. What the cloud offers in storage of terabytes (and more) is also its potential drawback, as security in the cloud continues to worry

organizations that send up their files.

Contributor Trevor Strome looks into the pros and cons of the healthcare cloud, including the problems that could endanger data. In the end, Strome concludes that "most of these security concerns also apply to a healthcare organization's self-hosted IT infrastructure."

Wrapping up the handbook is a list of factors that healthcare IT executives should evaluate when making purchasing decisions for cloud services, as explained by contributor Reda Chouffani. He encourages leaders to think about which pieces of their technology infrastructure make sense in the healthcare cloud, rather than jumping full force in.

Whatever approach you choose, don't forget patients like me and others who could benefit from the freedom that the cloud offers. ■

Scott Wallask
News Director, SearchHealthIT
@Scott_HighTech

The Case for Cloud Computing in Healthcare

Cloud computing has much more to offer than simply hosting email services, sharing photos or backing up mobile devices on Google Drive, Dropbox or iCloud. In many ways, we're still in the early stages of determining how the cloud fits into the healthcare information management and technology ecosystem. Providers are still calculating how to balance the possible benefits with the obvious security, technical and legal risks.

One definition of cloud computing from the National Institute for Standards and Technology states that it is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

According to a white paper titled Cloud Computing in Health by Canada Health Infoway, cloud computing models support three ways of provisioning computing resources as services:

- **Software:** Applications such as monitoring and dashboard apps, content delivery, communications and finance tools.
- **Platforms:** Middleware, databases and identity management systems.
- **Infrastructure:** Storage, CPU and networking.

The white paper further states that deployment of these three services typically occurs in one of four ways:

- **Private:** IT services are dedicated to a single organization.
- **Community:** Common services for organizations are provided that have a shared purpose or business domain.

- **Public:** IT services are made available openly to a range of customers.
- **Hybrid:** Some combination of private, community and public deployments are arranged to meet an organization's unique IT requirements.

Rather than being a one-size-fits-all offering, cloud computing presents a variety of services and deployment models for healthcare organizations to choose from in order to address current gaps and future needs in business provisioning.

WHO NEEDS CLOUD COMPUTING?

There are many reasons why healthcare organizations should consider the cloud part of their services delivery strategy, including its important economic, technical and innovation benefits.

Most providers have invested heavily in their health IT infrastructure in the form of clinical and business software, hardware such as application and database servers, and extensive high-speed data networks. Due to continuing budget constraints, healthcare IT executives are under pressure to rein in costs while continuing to meet minimum service levels and deliver applications with the speed and availability that today's healthcare professionals require.

Healthcare organizations invest in health IT so they can provide clinicians and administrators with information to make better, evidence-informed decisions. In many cases, the rate of change in many organizations is outpacing their IT department's ability to keep up with the newest software, processes and regulatory requirements. This is causing health IT provisioning to be a limiting factor in innovation and healthcare transformation, rather than the enabler that health IT was once envisioned to be.

The potential of cloud computing in healthcare is to enable providers to be more proactive and nimble in meeting changing regulatory and market demands by focusing their resources on the best use of technology. A cloud platform allows providers to offer value to clinical and business end users beyond merely keeping servers, software and networks up to date.

PROS AND CONS OF CLOUD COMPUTING

Healthcare organizations exploring cloud computing options must identify where their greatest health IT-related needs are in order to determine if and how cloud computing offers an advantage. Provisioning certain IT services over the cloud brings some distinct benefits compared with traditional self-hosting of the software, hardware and other networks associated with modern health IT.

Several commonly cited benefits of cloud computing include:

- **Reduced cost pressure:** Depending on the exact deployment approach, healthcare organizations will pay for only the cloud computing resources they use.
- **Speed and flexibility:** Cloud service options can be configured to meet the unique and changing needs of individual clients in an organization.
- **Increased scalability:** Using cloud services, providers can increase the processing or storage capacity they require, rather than purchasing hardware that will sit idle until needed.

The security of healthcare information and the protection of individuals' privacy are major concerns. It is a challenge for IT teams to keep their systems updated and protected from both external and internal threats. Cloud computing providers are known to double down on their efforts to ensure the security of cloud resources.

Healthcare organizations understand that the use of the cloud is not without risk, and this is perhaps one of the most significant barriers to cloud adoption. A report from the Cloud Security Alliance, *The notorious nine: Cloud computing top threats in 2013*, identifies major security concerns associated with use of the cloud, including the following six:

- **Data breaches:** Perhaps the most significant nightmare scenario associated with storing health-related information on the cloud, data breaches occur when sensitive or personal information is exposed to or stolen by individuals with no right to view that information.
- **Data loss:** The cloud is not immune to sensitive information being deleted and rendered

irrecoverable through an accidental or malicious act.

- **Account hijacking:** Phishing, fraud and software vulnerabilities are used to gain unauthorized access to services and/or data on a cloud service.
- **Denial of service:** Authorized users of a cloud service are denied access to applications and data as a result of a deliberate attack that causes an intolerable system slowdown.
- **Malicious insiders:** This category encompasses employees, former employees or business partners who inappropriately use their privileges to access private information.
- **Insufficient due diligence:** Organizations expose themselves to great risk if they don't fully understand their cloud service provider environment, the applications and services associated with it, and the incident response and security duties required of them.

Most of these security concerns also apply to a healthcare organization's self-hosted IT infrastructure. These issues should give pause to healthcare organizations and spur them to ensure that prospective cloud providers expertly and completely mitigate these risks, and that a strategy and action plan are in place to identify and address evolving and emerging security and privacy risks.

There are risks (known and unknown) that must be mitigated to ensure the security and privacy of data stored in the cloud.

There are clear benefits and risks associated with cloud use in healthcare. There are opportunities for significant financial, technological and service-related benefits that come along with adopting cloud computing. Yet, as with most emerging technologies, there are risks (both known and unknown) that must be mitigated to realize the potential benefits and, most importantly, to ensure the security and privacy of any data stored in the cloud. Healthcare executives must balance the risks, benefits and business and IT needs of the organization to best determine if, how and where cloud computing should be featured in their health IT provisioning strategy. —*Trevor Strome*

CASE STUDY

Cloud Services Lifts Hospital's Genome Project

While genome sequencing—the act of analyzing the genetic makeup of a person—is at the forefront of medical research, the data involved is oppressive from a technology perspective, potentially barring healthcare professionals from achieving population-scale genomics.

Sequencing genomes "spits out masses and masses of raw data," said Peter White, Ph.D., principal investigator and director of the Biomedical Genomics Core at Nationwide Children's Hospital in Columbus, Ohio. To put it into perspective: Sequencing just one human genome produces 1 terabyte of data.

For years, healthcare professionals have lacked efficient technology to not only handle the data, but also find value in it.

"Technology is certainly a limitation. There's no doubt about it," said Thomas Handler, M.D., a research vice president at Gartner Inc. who focuses on precision medicine and genomics, among other areas of healthcare IT.

This lack of technology has slowed advances in analyzing genomes that would make rapid diagnosis, precision medicine and population-scale genomics possible.

But, White said, in seven days he and his team at Nationwide Children's successfully analyzed 2,500 whole genomes and 2,500 exomes—a part of the genome in which the majority of genetic diseases result from due to mutations. He added that it took the 1000 Genomes Project—a group that conducted the first project to sequence the genomes of a large number of people and to provide a comprehensive resource on human genetic variation—18 months to analyze the same data set.

Altogether, Nationwide Children's, in partnership with GenomeNext LLC, a bioinformatics company, analyzed 5,000 samples and 70 terabytes of data in seven days, said James Hirmas, CEO at GenomeNext.

White and his team embarked on this endeavor in November 2014, when they submitted a proposal as part of the Intel Head in the Clouds Challenge on Amazon Web Services. At the AWS WWPS Government, Education and Nonprofits Symposium back in July 2014, Intel challenged attendees to think about a problem within their agency, organization or industry that they would most like to solve and submit it to Intel with a proposed solution. White and his team proposed using an algorithm they had developed called "Churchill" with GenomeNext's software as a service (SaaS) analytical platform, which runs on Amazon Web Services (AWS), to analyze the largest publicly available data set of population scale genomic data from the 1000 Genomes Project, he said.

"The algorithm is an extremely important piece of the overall platform" that GenomeNext provides, Hirmas said.

Churchill is able to efficiently distribute the analysis process. White and his colleagues found that Churchill has an accuracy of 99.99% and an overall diagnostic effectiveness of 99.66%, according to the standards set by the National Institute of Standards and Technology, the federal technology agency that works to develop and apply measurements and standards.

Churchill has an accuracy of 99.99% and an overall diagnostic effectiveness of 99.66%.

"Also what distinguished [Churchill] was that it's 100% reproducible. So every time you run the analysis you get the same results," White added. Churchill is also deterministic, which means "that regardless of whether you run this on your local server or you run it on a supercomputer or you run it up in the cloud, you get exactly the same results back."

The initial goal of White and his team was to use the Churchill algorithm for rapid diagnosis in a pediatric setting. Then the team realized Churchill could scale "really well in the cloud and could be used for population-scale studies," White said.

GenomeNext licensed Churchill for exclusively commercial use. The company built the

infrastructure, security and HIPAA compliance around the algorithm, and made it fully automated to give customers the ability to upload sequencing results "to a platform running on the cloud that then allows them to do mass computer analysis or genomic analysis on the sample," Hirmas said.

Organizations that use GenomeNext to analyze genomes get free storage and pay for only what they use. "It's like the electric company: You turn on your lights, you pay for it. Once you turn them off, you stop paying. [It's] the same concept," Hirmas said.

Here's how the whole process works: Once a DNA sample has been collected and put into a format that allows the data to be sequenced, the sequencer runs for about 40 hours and produces an output called a FASTQ file, which is in a format that stores genome sequences, White explained.

Once those FASTQ files are generated, GenomeNext's analytical SaaS comes into play: A lab technician uploads the file to AWS, and "Churchill's able to take it through that entire process of what we call secondary data analysis—that's the alignment, the post alignment processing, the variant discovery and genotyping," White said.

After that point, the tertiary analysis piece—annotating the genetic variants and figuring out which may cause diseases—occurs, White said.

"The data's uploaded to AWS, and then that entire process of secondary and tertiary analysis is fully automated," White said.

Nationwide Children's Hospital is currently using this technology in its clinical diagnostic laboratory.

"What we're working toward is: How do we start to integrate a patient's genomic signature with their electronic health record?"

—PETER WHITE, Ph.D., principal investigator and director of the Bio-medical Genomics Core, Nationwide Children's Hospital

"What we're working toward is: How do we start to integrate a patient's genomic signature with their electronic health record?" White said.

That EHR aspect will be challenging, according to Handler. "In the same way that right now the EHRs will remind me not to prescribe penicillin to someone who's allergic to penicillin, presumably in the future, when we know that there are classes of drugs that shouldn't be given to individuals with a certain genetic make-up, that decision support role needs to fire. And how that will be done is going to be fairly complex," he said.

And while these technologies are certainly a step in the right direction toward rapid diagnosis and population-scale genomics, Handler said he believes it will be about 10 years until these goals are fully reached.

For White, the results he and his team got using GenomeNext and the Churchill algorithm are a hopeful step forward.

"By reducing the computational burden and cost, the technology enables any group to perform genomic analysis of [thousands] of individuals using universally available cloud compute resources," White said.

—Kristen Lee

Tips for Adopting Healthcare Cloud Services

Because of the enhanced security and disaster recovery capabilities of many cloud vendors, health IT executives have been chipping away at their locally hosted infrastructures and replacing them with healthcare cloud services. The increased level of trust that technology decision makers have in cloud vendors allows their organizations to hand much of the cloud transition process off. But a business should still check in with the vendor during the installation process to avoid challenges that have plagued other IT departments when moving to the cloud.

Fortunately, a number of online resources and consultants offer advice on how to select the right cloud services for healthcare IT. Whether the cloud service under consideration is software as a service, infrastructure as a service (IaaS) or platform as a service, accelerator programs and pilot initiatives have a tendency to cause problems that don't arise until weeks or months after the initial deployment of services. To proactively address precursors of project failures or cost leakages, IT executives are familiarizing themselves with the common challenges of migrating to the cloud.

What follows is a list of critical areas healthcare IT executives should evaluate when making a purchasing decision for cloud services:

- **Ensure that cloud services meet regulatory requirements.** Whether an organization must guarantee the protection of patients' health data to meet HIPAA requirements, receive a signed business associate agreement from a service provider or have a valid verification that satisfies Code of Federal Regulations Title 21 requirements, it's an absolute must to validate the security practices of vendor(s) under evaluation. This can confirm that a healthcare provider will stay compliant with applicable regulations and help avoid any penalties.

■ **Perform a detailed cost analysis.** Although online calculators can estimate the cost of healthcare cloud services, it takes a detailed cost analysis to truly determine the price of replacing or buying a new product. The price of the required bandwidth and transferring data will play roles in determining the final cost of migrating to the cloud. For certain services such as IaaS, many vendors offer measurements of their processor and memory usage as well as inbound and outbound traffic to help prospective customers accurately measure what their services would cost.

■ **Monitor performance of the system, even when internally hosted.** A process must be in place to monitor all systems, including cloud, to ensure that they are performing up to anticipated standards. Cloud-based services are not always guaranteed to function at the highest level. Variables such as connectivity and service issues can cause slowdowns if they are not addressed in a timely manner. IT departments must treat cloud-based services the same as they treat on-premises systems. Continuously monitoring a system's performance is the surest way to confirm that end users can use the system effectively.

■ **Evaluate ongoing costs and fluctuations.** Similar to deals offered by today's cellular data providers, some cloud services operate under the pay-as-you-go model. This approach reduces total up-front costs but can result in inflated costs if the data storage and outbound traffic figures exceed expectations.

■ **Prevent disaster even when systems are "disaster proof."** Risk assessments help healthcare providers determine whether a cloud provider, in combination with hardware and software safeguards, can guarantee controlled access to internal systems and protection of patients' data. Providers should also have a disaster recovery plan ready to set in motion to ensure care continuity after a security incident or system failure. Although the cloud offers better protection against power outages, hardware redundancy and connectivity redundancy, it is still subject to outages and downtime. This means that IT must keep its disaster recovery plans and business continuity plans updated.

Doing so can provide insights into possible gaps that should be addressed before they cause major issues.

■ **Transfer data from one cloud to another.** Understanding a cloud provider's portability and component interoperability capabilities is critical before committing to long-term cloud services. Healthcare providers should determine if they will be able to move systems, data sets, platforms, infrastructures or all of the above into a new environment before committing to a cloud product. They should also find out if the vendor they're evaluating works well with—or its systems are interoperable with—other vendors' systems.

Deploying cloud services for healthcare has provided tangible value and a return on investment for many organizations. Many services can be hosted through the cloud, including email, EHR, storage and servers. Any IT executive can find an area of the business where a cloud service can reduce on-premises dependency. However, turning too many business operations over to the cloud comes with its own set of risks. The long-term costs and growing severity of cyberattacks are causes for concern for health IT professionals.

Deploying cloud services for healthcare has provided tangible value and an ROI for many organizations.

—Reda Chouffani

TREVOR STROME, *M.S., PMP, is the informatics and process improvement lead for the Winnipeg Regional Health Authority Emergency Program and the founder of HealthcareAnalytics.info.*

KRISTEN LEE *is a news writer for SearchHealthIT. Email her at klee@techtarget.com and follow her on Twitter: @Kristen_Lee_34.*

REDA CHOUFFANI *is vice president of development at Biz Technology Solutions Inc. Follow him on Twitter: @healthcareITGuy.*

TechTarget

Healthcare Cloud Is Rolling In
is a SearchHealthIT.com e-publication.

Jacqui Biscobing | *Managing Editor*

Scott Wallask | *News Director*

Shaun Sutner | *News and Features Writer*

Alex DelVecchio | *Site Editor*

Linda Koury | *Director of Online Design*

Neva Maniscalco | *Graphic Designer*

Stephanie Corby | *Publisher* | scorby@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com