Cloud Computing in Health Care

Educational Briefing for Non-IT Executives

Executive Summary

Cloud computing has received plenty of buzz as a cost-friendly, labor-saving option for health IT systems, and has already started to heavily influence how business is done, even through basic processes like sending an email or hosting a blog. Cloud technology offers hospitals and health systems several potential benefits, such as lowering capital costs, enabling flexible, on-demand addition of computing resources, boosting scalability, and improving reliability (e.g., data backup and recovery). Despite the many advantages of cloud technology, concerns still linger about data ownership, security, and access that have hindered widespread adoption among health care providers.

What is cloud computing?

Cloud computing is the delivery of on-demand computing resources (e.g., servers, databases, storage) over the Internet on a pay-for-use basis. Cloud computing delivers value by increasing agility, making more efficient use of hardware resources, and reducing the need for certain specialized roles needed to manage physical data center resources. To be considered a cloud, a system must be elastic, scalable, and metered, and it must use pooled or shared IT resources.

Cloud architectures can be divided into several deployment models:

- **Public cloud**: A public cloud is owned and operated by a third-party service provider and available to any paying customer on a metered basis. With this model, the user does not need to purchase hardware, software, or any supporting infrastructure. Many public clouds operate data centers at massive scale, provisioning hundreds of thousands of servers in data centers around the world. The scale of these operations allows them to make investments in reliability, efficiency, and security that are impractical for smaller organizations. Examples of public clouds include Amazon Web Services and Microsoft Azure.
- **Virtual private cloud (VPC)**: A VPC provides a way for a public cloud offering to "fence off" a set of resources to provide added security guarantees for a tenant.
- **Private cloud**: A private cloud runs on infrastructure hosted internally by the organization. Private clouds require the organization to purchase hardware and operate a data center, but differ from traditional data center operations by using a comprehensive virtualization layer to manage the details of provisioning of computing resources (e.g. servers, networks, and disks). A private cloud does not deliver the same ability to "rent" or "surge" resources as a public cloud; the hardware in a private cloud needs to be purchased and installed, just as with traditional data center models.
- **Hybrid cloud**: This model deploys a mix of private cloud and public cloud resources under a common management platform. For example, a large health care entity could locate core critical services or sensitive applications (like an electronic health record) on a private cloud, but gain the ability to scale workloads to a public cloud when demand spikes.
- **Community cloud**: In a community cloud, several organizations pool resources to create a private cloud. They may choose to share data among themselves, but sharing is not a prerequisite. When combined with a private high-bandwidth network, a community cloud becomes very well protected from external security threats.

There are a variety of service models for cloud computing:

- **Infrastructure as a service (IaaS)**: This service provides on-demand access to foundational computing resources such as servers, networks, and operating systems. An example of IaaS is Amazon EC2.
- **Platform as a service (PaaS)**: This service allows customers to create their own applications within a framework provided by a cloud provider without having to manage any underlying infrastructure (e.g. servers and storage devices). An example of PaaS is the Google App Engine system.
- **Software as a service (SaaS)**: This service provides on-demand access to software applications over the Internet, typically through a web browser. Examples of SaaS include Workday, Microsoft Office 365, and Salesforce CRM.

Source: Health Care IT Advisor research and analysis.

How is cloud computing used or applied in health care?

A health care entity might want to leverage a cloud-based infrastructure in order to:

- **Decrease capital expenditure and reduce initial cash outlays**: Given the pay-for-use approach, utilizing public cloud resources converts capital expenditures to operating expenses and reduces initial cash outlays.
- **Increase agility:** Public cloud resources can be provisioned and destroyed in minutes, eliminating the weeks or months that many projects might otherwise wait while data center hardware is approved, purchased, and installed.
- **Improve business continuity and disaster recovery**: Most public cloud providers have multiple data centers with broad geographic distribution, and secondary sites can be run on fewer resources until needed during a failure.
- **Improve security**: Although many organizations still worry about cloud security, these concerns have started to ease. Cloud networks can be more secure than private data centers because cloud providers have the scale and budget to invest in advanced security programs, allowing health care organizations to focus more on their core business. Cloud providers can run security tests on a regular basis and share the responsibility of HIPAA compliance with hospitals and health systems.

How does cloud computing affect health care providers and IT leaders?

Enhanced agility and efficiency

- Cloud technology can increase a health care organization's efficiency by merging department-level data centers, increasing standardization, and providing a faster time to market of new applications and technologies. The scalability of cloud computing allows IT teams to rapidly adjust resources to meet fluctuating business needs.

Changing staff requirements

- Most IT departments are dealing with constrained resources, and it can be difficult to adequately cover all expected skills. With cloud computing, the routine work of maintaining, upgrading, and protecting hardware and software can be offloaded to the cloud vendor. In-house skills and training requirements will vary depending on deployment model.

Shared data ownership

- Departments that are used to managing their own servers will now have to cede some control to IT for the centralized cloud resource. The cloud can be a "black box" if the provider organization doesn't know where the data is physically stored and doesn't have direct oversight of it.

Questions That Hospital Executives Should Ask Themselves

1. What are we trying to accomplish with cloud computing (e.g., lower costs, enhance reliability)?
2. What applications would be good candidates for cloud deployment?
3. What type of cloud deployment model would work best for our organization?
4. Are our staff prepared to manage a cloud environment?

Additional Advisory Board research and support available

Report: Virtualization and Cloud Computing in Health Care

Daily Briefing: Why Health Care Is Finally Embracing Cloud Computing

Source: Health Care IT Advisor research and analysis.