Technology Now
Timely Topics for Academic Medical Centers
a product of the AAMC's Group on Information Resources (GIR)
Group on Information Resources GIR
AAMC

Cloud Computing

By Dennis Schmidt, Director, Office of Information Systems, UNC School of Medicine, and the GIR Information Security Working Group

Cloud computing provides computing resources as an online service, not as a physical product. The user typically has little knowledge of the physical makeup or location of the supporting infrastructure. (Analogy: You buy electrical *service* instead of generating it yourself.) An entire spectrum of potentially lower cost, easy-to-use services with high reliability and rapid startup times is now available. Researchers and users are demanding access to the capabilities that these services provide, but security officers are reluctant to give them access and academic IT organizations are not typically resourced to provide them locally. This document provides some basic high level information and recommendations that institutions should consider before venturing into the public cloud.

Types of Clouds:

Public cloud: available to the general public or a large industry group and is owned by an organization providing cloud services. Lower cost, higher risk.

Private cloud: operated solely for one organization. It may be managed by the organization or a third party and may exist on premise or off premise. Lower risk, highest cost.

Community cloud: shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Hybrid cloud: a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Security Concerns:

- Access controls (Who has access to your data?)
- Data Location (Is it being stored in a foreign country, not subject to US laws?)
- Encryption (Is the data encrypted? With what technology?)
- Data Use Agreements (Do any exist?)
- Business Associate Agreements (Will the vendor agree to sign one?)
- Forensics capability, e-discovery (Can you get access when required?)
- Auditable (Will it satisfy requirements?)
- Vendor stability and longevity (Is the company stable?)
- Data retention (Can you really delete your data?)
- Data stored on same machines as other virtual machine users (colocation). (Is your data really isolated?)

Institutional Policies Should:

- Address processing or storing sensitive information in the cloud
- Require that proper technical controls be in place (access, encryption, network protections, etc.)
- Develop written policies and procedures for use
- Require Business Associate Agreements (BAAs) or data use agreements with any vendors providing the service
- Restrict unprotected sensitive information
- Consider how to enforce and manage different policies for different services

Delivery Models:

- **Software as a Service (SaaS):** Consumers can use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. *Examples: Office 365, Gmail, NetSuite, Salesforce.com.*
- **Platform as a Service (PaaS):** Consumers can deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. *Examples: Google App Engine, Microsoft Azure, Force.com.*
- **Infrastructure as a Service (IaaS):** The availability to use processing power, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. *Examples: Amazon's Elastic Compute Cloud (EC2), The Rackspace Cloud.*

Further Cloud Examples:

Mail: Gmail, Yahoo Mail, Outlook.com **Social Applications:** Facebook, LinkedIn, Google+, Yammer **File Storage:** Google Drive, Drop Box, iCloud
Document Collaboration: Google Docs, Skydrive **Virtual Servers**: Amazon, IBM **Backups:** Iron Mountain, Mozy, Carbonite **ePrescribing:** DRFIRST

Scan for link urls & more Tech Briefs

Additional Resources:

Best practices for implementation: NIST Guide to Initiating a Public Cloud Service (NIST SP-800-144), Specific considerations for academic settings: EDUCAUSE Library on Cloud Computing, PCI guidance on virtualization: PCI Data Security Standards