# Cloud Computing

## Table of Contents

- Introduction ................................................................. 2
- Defining Cloud Computing ............................................... 3
- Applications in Canadian Healthcare ..................................... 4
- Challenges Associated With Cloud Computing .......................... 5
  - Security ........................................................................ 5
  - Security Practice Considerations ................................... 7
  - Privacy and Confidentiality ............................................. 9
  - Privacy and Confidentiality Practice Considerations .......... 10
- Benefits of Adoption .......................................................... 11
- Conclusions ...................................................................... 12
- Special Thanks to the Authors and Reviewers ............................ 13
- Glossary .......................................................................... 14
- References ....................................................................... 16

November 2016
Cloud Computing

Introduction

The “cloud” is a metaphor for the Internet, and the term “cloud computing” is a broad term used to describe resources, such as storage, processing power, servers, etc. hosted remotely by a third-party. A hosting provider will have several locations where a set of servers are being held, and while the client doesn't know exactly where the data is stored, the client enters into a contract with the service provider to affirm the data is well looked after. Users can then subscribe to a provider and access resources on-demand. These services can range from access to a consumer computer with a standard operating system, to remote storage where a user can hold data, to high-performance computing clusters where one can run applications in parallel to greatly improve speed and processing power. Companies can save on the infrastructure cost of building and maintaining servers in-house, since all infrastructure is provided by a third-party. Definitions of cloud computing focus on the cloud's service aspect, where consumers dictate their needs on the cloud and purchase accordingly. The essential characteristics of the cloud are illustrated in Figure 1 on the next page.

Cloud computing in healthcare can support a more collaborative, open, and shared healthcare delivery model, with information available across departments, hospitals, and geographic locations. The flexibility of the cloud allows the healthcare system to adapt to increases in the amount of data, and to participate fully in the Information Age as more and more industries adopt an information-centric approach to delivery of services. However, the inclusion of a third-party in the computing environment leads to additional security risks associated with keeping servers off-site, such as the physical safety of the server. Nonetheless, adoption of cloud computing and the feasibility of movement to this paradigm has been much discussed in the healthcare setting.

In this brief, we define the essential characteristics of cloud computing and the applications in a Canadian healthcare context. The security and privacy challenges, of particular importance to health information management professionals, and the end benefits of adopting a cloud computing model are also highlighted.
Figure 1. Cloud computing overview incorporating the essential characteristics of the cloud, the deployment models, and the service models available.

Defining Cloud Computing

The National Institute of Standards and Technology (NIST) has defined cloud computing as a model for enabling ubiquitous, convenient, on-demand access to a shared pool of configurable computing resources. The NIST model is composed of five key characteristics that define cloud-computing. We can use these characteristics to help create a standard for what is considered cloud-computing. The key characteristics are summarized as follows and in Figure 1:

- **On-demand self-service**: Consumers can access and use the resources provided without human interaction.
- **Broad Network Access**: Resources are accessible over the network and can be used by all client based platforms (mobile, tablet, laptop, desktop)
- **Resource Pooling**: Resources are pooled to serve multiple clients at the same time, and they are dynamically assigned to consumers based on demand.
- **Rapid Elasticity**: Capabilities can be scaled quickly and automatically as needed by the client.
- **Measured Service**: All usage of resources is metered and can be monitored, controlled, and reported.
Applications in Canadian Healthcare

Cloud services provide access to large-scale information technology (IT) infrastructure without the large financial investments and cost of space and maintenance of traditional IT environments. Currently existing cloud services can be classified from two dimensions: how computer resources are provisioned, and the method of implementation.

Cloud computing services can be used to provision computer resources by way of three distinct service models.

- **Software as a Service (SaaS):** The client uses applications in the cloud which are set up by the provider. Cloud-based EMR is one example of software offered through this model.
- **Platform as a Service (PaaS):** The client can choose which applications run on the cloud platform. Processes such as databases, libraries, and other tools supported on the platform can be run.
- **Infrastructure as a Service (IaaS):** The client has access to the fundamental computer components of the cloud, including storage, processing, and some networking settings. With this freedom, the client can run different operating systems and software as needed.

Services will often include components from more than one of the above-mentioned models. For example, a service can provide some application-level access, while also allowing manipulation of more fundamental computing components, such as infrastructure in IaaS.

Cloud computing services can also be categorized by their method of deployment: private, public, community, and hybrid.

- **Private Cloud:** This type of cloud provides exclusive access to services to a single organization, offered over a firewall protected connection. Private clouds may be owned by the organization itself or by a third-party: for example, a healthcare network making data available to its own facilities.
- **Public Cloud:** is a type that provides access to services to the general public. May offer a generalized service such as simple data storage or email.
- **Community Cloud:** This type of cloud provides service for a limited number of organizations with shared concerns, governed commonly by all the participating organizations or a third-party managed service provider. For example, healthcare organizations within a region may share a cloud service to manage patient data.
- **Hybrid Cloud:** This type of cloud is integrated and provides services in a way that is a mixture of public and private.
The four deployment models above allow organizations to tailor the service to meet their own IT needs. For example, smaller hospitals, medical practices, and laboratories may not have IT staff to maintain and service in-house infrastructure for applications such as electronic health records (EHRs). SaaS may provide a suitable way to eliminate the infrastructure cost and allow EHR adoption. The same organization may also use a public cloud for non-sensitive data for content collaboration or document storage. However, public cloud based services are considered to have greater security risk, and so may not be suitable for e-mail coming from healthcare organizations - which may be considered sensitive information. A larger healthcare institution such as a hospital may opt for a service with more intricate control in order to be adaptable to its future business strategies. The IaaS model has the most potential scalability, flexibility, and security, but also requires the most investment in IT personnel for the purchasing organization.

The cloud paradigm is increasingly used in an OMICS-context (the field of study in biology ending in omics: genomics, proteomics, etc.), and other healthcare applications are growing in use as well, such as EHRs. Patient data can be stored in an EHR or in a personal health record (PHR) supported by cloud services. The growing popularity of mobile devices means increasing access to these systems. Health service networks can be hosted on the cloud to connect providers with anytime and everywhere access to patient information. For example, Picture Archiving and Communication Systems (PACS) offered through the cloud can be used to create diagnostic imaging repositories. This alleviates the costs of on-site technology to store images and, if offered remotely, can offer the anytime, everywhere access options to health providers.

Telemedicine is another service that is well suited for cloud computing. The Ontario Telemedicine Network (OTN) is a good Canadian example of strategic planning for cloud computing adoption. The 2014-2015 annual privacy report released by OTN includes a cloud computing framework for the purposes of exploring and potentially adopting a cloud computing paradigm. Should OTN pursue the opportunity, it would be the first public sector organization to host personal health information in the cloud.

**Challenges Associated With Cloud Computing**

**Security**

Three primary goals of information security are to ensure confidentiality, integrity, and availability of data. Confidentiality is one of the biggest concerns in healthcare data transfer, and cloud computing requires an additional layer of security as data becomes assessable on the third-party provider side. Integrity and availability of data is generally
very good in the cloud environment as providers invest a great deal of effort in providing a high level of service, but unexpected outages must still be considered when implementing a cloud environment in healthcare.

Security issues with cloud computing can be two-fold: security issues faced by cloud providers and security issues faced by their customers. Cloud providers must physically protect their client's servers, in contrast to the traditional approach where the client takes on that role. Break-ins at the server facility, insider attacks by staff, and damage to servers by agents such as fire and flood constitute security risks which only the provider can mitigate. With reputable cloud providers, the cloud would provide superior security in that regard, as providers can specialize and afford high-grade security inaccessible to most organizations. Cloud computing clients, on the other hand, must adhere to standard security measures, including password protection and role-based access controls and, in addition, must also consider security of the data transaction between the cloud provider and the organization itself. However, cloud computing based solutions may lead to increased security over self-hosted computing infrastructure as long as a reputable cloud computing provider is chosen, as cloud providers can afford greater IT security expertise and technology with the cost spread out over multiple customers.

Due to outsourcing of architecture and software, cloud computing comes with unique digital security and physical security requirements. Traditional security measures must be reconsidered, since the unique and innovative cloud computing model is vastly different from traditional computing architecture where resources and allocation are typically fixed rather than being dynamically assigned, based on demand, to multiple agents. To improve efficiency, save space, and provide flexible service, cloud providers may store data from two different parties on the same server, potentially leading to unintended access by one or the other of the parties. Nonetheless, with stringent security measures, the segmentation of different entities can be rigorously maintained in a cloud computing environment.
Figure 2. Cloud computing 12 top threats, as identified by the Cloud Security Alliance.

The Cloud Security Alliance Top Threats Working Group has identified 12 top threats to cloud security (Figure 2). With good security practices, as described below, these threats can be mitigated. In addition, the ISO/IEC 27018:2014 standard is designed to protect sensitive data in the cloud in terms of implementation, risks, controls, and associated guidelines/policy. This standard provides guidance to ensure cloud service providers offer suitable security controls to protect the privacy of their clients. Cloud providers adhering to this standard offer another security measure to protect sensitive healthcare data in the cloud.

Security Practice Considerations

The Canadian Standards Association’s (CSA) Model Code for the Protection of Personal Information describes ten fair information principles. Principle seven is Ensuring Safeguards and states, “Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.” As health information is deemed especially sensitive, security is of paramount importance. Tools to support meeting this principle include the development, implementation and maintenance of technical (transmission control, access
controls, and audits), administrative (policies and procedures, risk assessments), and physical safeguards (password controls, restricting printer and downloading capabilities to certain devices and/or individuals). Organizations should always keep in mind the security protocols of “IAAA” (i.e. identification, authentication, authorization and audit) for all transactions occurring over desktop and web based applications. In addition, some specific cloud-based security measures should be considered.

1. Cloud providers are responsible for the physical safety of the data, redundancy of systems, and disaster response; the healthcare organization is responsible for data backup and prevention of accidental deletion, though the provider also shares some of that role (i.e. prevention of accidental deletion or data loss on their end). Checks should be put in place to make sure data are deleted only when necessary and only by authorized personnel.

2. The use of encryption can thwart attacks – as encrypted data stolen by an attacker is rendered useless to them, and protects against unauthorized use of the data, even after data has been accessed. Cloud providers have an obligation to encrypt their data streams and access points on the provider side.

3. Multifactor authentication – the use of more than one authentication credential to verify a login (such as both password and smartcard). Rotating passwords, cryptographic keys, and certificates prevent unauthorized access and can greatly aid identity access management.

4. The organization should educate users to avoid repetitive password use and to identify phishing scams aimed at account hijacking. For example, users should be warned about clicking suspicious links. Also, users should be educated on strategies such as spear phishing (a phishing email that appears to belong to a trusted organization, such as the hospital itself but in reality is from a hacker) to prevent introducing Advanced Persistent Threats (APTs) into the system.

5. Reporting systems should be a part of the cloud provider’s services, and use should be monitored on the client side to detect if the cloud is being misused. Regular audits should be undertaken as well.

6. Lifecycle management and role-based access management of all users must occur for effective protection. Role-based access is important: a physician will see different data than a nurse or a clerk in health records. As well, these user types will not be able to delete data, but may need to read, write, or edit. Lifecycle management of users in practice requires granting access when necessary and revoking it when the period of involvement with the organization is finished (such as termination or the end of a contract).

7. Vulnerability scans, reporting for systems threats, and installation of security patches and upgrades as available are basic IT principles which can greatly aid in vulnerability management within the operating system.
8. In addition, there are numerous methods to implement if Denial of Service (DoS) or Distributed Denial of Service (DDoS) are threats for an institution. Research into the risk of these specific threats and the potential cost to the organization of a successful attack should be undertaken, and prevention and detection methods implemented accordingly.

9. On the provider side, use of a Trusted Third-Party (TTP) can potentially alleviate some security issues. In cloud computing, a TTP can serve to establish trust between providers and users by guaranteeing that access is both intended and secure through the exchange of private keys (an encryption/decryption key known only to the parties that exchange secret messages) between essential parties.

Privacy and Confidentiality

Confidentiality refers to restricting access of protected data to authorized parties only. A data breach occurs when unauthorized persons or parties gain access to confidential data. This is a major concern for the field of healthcare, where patient information is protected under confidentiality law. Data breaches may result from a targeted attack, but can also be due to human error, vulnerabilities in the system, or poor security practices. Up to 80% of data breaches come from within an organization, so while cloud computing provides more access points and additional parties are involved, the majority of security risk remains the same between paradigms and internal to the organization. The threat of a data breach is not unique to cloud computing. Additional security threats exist within the cloud computing environment by way of shared resources, cloud provider personnel and their devices, and third parties partnered with the cloud service provider. Preventing data breaches requires good defensive practices as described in detail above.

The Canadian Privacy Commissioner’s office provides a fact sheet on cloud computing, as well as a number of other guidelines for implementation and security of the cloud. The Office has released a comprehensive report on privacy issues related to cloud computing, and requires an organization to ensure a comparable level of protection in the cloud under Principle 4.1.3 of Schedule 1 of Personal Information Protection and Electronic Documents Act (PIPEDA). The organization is held responsible for meeting PIPEDA requirements. The Office has also released guidelines for trans-border data flow.

In addition to security concerns, cloud computing offers another unique challenge for healthcare. Laws regarding confidentiality in healthcare vary from country to country and province to province. Because cloud computing data and applications may be stored remotely on servers located outside of the originating country, the possibility for data to
fall under laws incompatible with that of the healthcare facilities home base is a possibility. For Canadian organizations, servers located in the United States are subject to the Patriot Act. A solution would be to make sure the location of servers physically remain within Canada, and no data will be stored or processed elsewhere. In Alberta, British Columbia, and Nova Scotia, this provision is required by law.

**Privacy and Confidentiality Practice Considerations**

1. Providers should be asked to stipulate where they are keeping their servers and to agree to keep the server facility within Canada as required by provincial law.

2. Providers should agree to sign a privacy agreement and data sharing agreement regarding access, use of, and disposal of the data stored at their facility in accordance with privacy law.

3. The availability and reliability of the system must be maintained within acceptable limits by the provider.

4. Transparency must be demanded from the cloud service provider and a Privacy Impact Assessment (PIA) should be undertaken. (Please see PPB 0038.15 entitled, Privacy Impact Assessments).

5. Organizations must understand what security options are available through the cloud service provider to promote privacy and confidentiality, including processes, infrastructure, and segmentation between customers. Tracking activity within the cloud and prohibiting shared accounts can also help identify potential misuse by insiders within the healthcare organization.

6. Security best practices must be followed (as described in the prior section), and audits must occur periodically to detect unauthorized access.

7. The law of the land, federal and provincial, must be adhered to on both the client and provider side.
Benefits of Adoption

Reliability Cloud computing services tend to be reliable. AppNeta, an application performance monitoring company, compiled data on the uptime reliability of 40 of the largest providers for cloud computing. Their data found the overall industry average to be 99.948% uptime. The overall trend revealed a low outage risk from cloud providers.

Technological Adaptation Cloud computing allows for self-service provisioning, a self-service option whereby end users can set up and utilize services and applications without direct intervention from service providers or the IT vendor. Furthermore, health information managers and healthcare professionals with system access can utilize computing resources for most types of workload on demand and in an independent manner. This allows for greater adaptability for information coming into the healthcare system from sources other than traditional computers, including medical devices and mobile computing technologies. (Please see PPB 0035.14 entitled, Mobile Computing).

Public Health and Chronic Disease Management An organization may simplify collection of data for a comprehensive view on population health by moving to a cloud-based infrastructure. The use of cloud computing to store applications focused on public health or chronic disease management can support healthcare organizations in coordinating outbreak responses and track statistics across disease categories. Chronic disease management can be improved via the transfer of information through the cloud to allow healthcare providers the opportunity of care coordination.

Inexpensive Infrastructure On a whole, the benefit of switching to cloud computing over local hardware storage of health information is a reduction in the initial investment in hardware and reduction of costs associated with on-site operation, IT support, and maintenance of infrastructure.

Potential Cost Benefit According to a study conducted by the Booz Allen Hamilton (BAH) consulting company, after implementation of cloud computing services healthcare organizations opting for private cloud services have annual operating savings of 65%. The net present value was 6.8 for private clouds, meaning—for every dollar invested in the private cloud computing model, the average return was 6.8 dollars. In terms of estimated payback, an average of 3.7 years was found to be the return on investment period. Cloud computing allows organizations to shift from capital expenses to operating expenses, allowing for low up-front costs and greater flexibility in use.
Conclusions

Ultimately, cloud computing is a multi-use resource which can be leveraged in a variety of different contexts to provide a vast array of benefits to the implementing organization. Choosing cloud providers, assessing the impact cloud services will have on the organization, and assessing security risks are important to consider prior to implementing cloud technologies. In healthcare, implementing information governance policies can mitigate security issues and protect against litigation surrounding privacy breaches. Motivation for this approach may come from concerns about litigation or fines resulting in data breaches from security threats, and in the long term, due diligence can save healthcare organizations more money and time than it may initially cost. If adequate security and privacy protocol is maintained, the benefits of cloud computing could allow cost-effective, flexible, and adaptable services within the Canadian healthcare system. With privacy as one of their four domains of practice, Health Information Management professionals have a role to play in both the acquisition and support of a cloud computing environment.
Special Thanks to the Authors and Reviewers

Authors:
Jathuson Jegatheeswaran, BSc, MHI
Elijah Joseph-Young, BSc (HI)
Michael Huang, BSc (HI)
Katherina Baranova, PhD, BSc (HI)

Reviewers:
Andy Igonor PhD, CISM, CRISC, CPHIMS
Thérèse Bernier, PMP, CPHIMS, MSc
Peter Madziak, MSc
Yuri Kagolovsky, MD, MSc, CHIM

Editor:
Paula Weisflock, BHA (HIM), MAEd, CHIM

For more information:
To learn more about this or any other Professional Practice Brief (PPB), including how to earn continuing professional education (CPE) credits from their use, please contact the Canadian Health Information Management Association (CHIMA) at:

Email: chima.education@echima.ca
Tel: 519-438-6700    Toll Free: 1-877-332-4462
Fax: 519-438-7001    Website: www.echima.ca

The publication of professional practice briefs (PPB) is a lengthy process due to the time it takes for authors to complete their research and write a draft of the brief. Subject matter expert reviewers are then called upon to review the PPB and provide feedback to the authors to consider incorporating into their work. Information within the PPB is deemed current at the time of writing; new information is always coming available and readers should take this into account. The content within this PPB reflects the opinions of the professionals who developed it. Scientific validation through research is not a part of the process. The links within this publication were current and valid as of the date of creation; however, webpage addresses and the information on them may change at any time.

©2016 by CHIMA. All rights reserved. This report or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of CHIMA.
Glossary

Access management: securing points of access against unauthorized users. Insufficient identity, credential, or key management can enable unauthorized access to data.

Advanced Persistent Threats (APTs): parasitical form of cyberattack to infiltrate systems and smuggle data and intellectual property.

Application Program Interfaces (APIs): APIs are a set of standardized protocols for making requests between programs. APIs allow programmers to call into cloud services through their applications.

Data Breaches: the loss, unauthorized access to, or disclosure of information by a party not privileged to view the data.

Denial of Service (DoS): attacks meant to prevent users of a service from being able to access their data or their applications.

Distributed Denial of Service (DDoS): a type of DoS attack where multiple compromised systems are used to target a single system.

Key Exchange: in cryptography, this refers to any method by which parties securely exchange information allowing encryption and decryption of messages between the parties. Public key cryptography is a common method of key exchange where the encryption key is freely available (the public key), while the decryption key (private key) is held solely by the owner (of the website, cloud application, etc.).

Malicious Insiders: a current or former employee, contractor, etc. who has or had authorized access and intentionally misused that access.

Multifactor Authentication: the use of more than one authentication credential to verify a login (such as both password and smartcard).

Shared Technology Issues: the shared infrastructure of the cloud may introduce vulnerabilities, which allow inappropriate access to another client's data if strong isolation capabilities are not integrated into the deployment model.
**Spear Phishing**: an e-mail spoofing fraud attempt (phishing scam) targeting a specific organization to access confidential data, retrieve personal information, or acquire passwords.

**System and Application Vulnerabilities**: exploitable bugs in programs which can enable attackers to infiltrate a computer system.

**Trusted Third-Party (TTP)**: a third-party organization which handles secure key exchanges for cryptographic access.
References


*Personal Information Protection Act*, SA 2003, c P-6.5.
Personal Information Protection and Electronic Documents Act  S.C. 2000, c. 5.


https://medium.com/@vrypan/explaining-public-key-cryptography-to-non-geeks-f0994b3c2d5#.tp9qfrijn
