Emerging Technology Series

Cloud Computing in Health

White Paper

Canada Health Infoway
Inforoute Santé du Canada

September 2012

Disclaimer

This white paper represents solely the views of *Infoway*. It is based on *Infoway's* research and analysis as well as information from various sources. *Infoway's* views are based on information and analysis which *Infoway* believes is sound and reliable, as of the publication date of this white paper. *Infoway's* views contained in this white paper may be amended or updated at any time by *Infoway*, without notice.

This white paper is informative only and cannot be interpreted as providing any indication of *Infoway's* present or future strategies or investment criteria.

This white paper is provided as is. No representation or warranty of any kind whatsoever is made by *Infoway* as to the accuracy, infringement of third party intellectual property, completeness, fitness for any reader's purpose, or correctness of any information or other contents contained in the white paper, and *Infoway* assumes no responsibility or liability if there is any inaccuracy, infringement of third party intellectual property, incompleteness, failure to meet any reader's purpose or incorrectness with respect to any of the information or other contents contained in the white paper.

Infoway does not assume any responsibility or liability related directly or indirectly to the white paper, including without limitation with respect to any person who seeks to implement or implements or relies or complies with any part or all of the ideas, recommendations or suggestions set forth in the white paper.

Infoway does not implicitly or explicitly endorse any particular technology or solution of any vendor or any other person, it does not guarantee the reliability or any proposed results related to the use of such technology or solution and this notwithstanding that reference may be made directly or indirectly to any such technology or solution in the white paper.

Infoway does not make any implicit or explicit commitment of any kind or nature whatsoever to make any investment in any particular technology or solution, and this notwithstanding that reference may be made directly or indirectly to any such technology or solution in the white paper.

Anyone using the enclosed material should rely on his/her/its own judgment as appropriate and seek the advice of competent professionals and experts.

Contents

1 Introduction

This document is a white paper on the subject of cloud computing and its potential relevance for the e-health community in Canada. The document defines the subject of cloud computing and describes possible applications of the technology from a Canadian health care perspective.

The phrase "cloud computing" (or even just the word "cloud") has become very visible in popular news and advertising media to businesses and consumers as a technology concept. However, for most people, its substance and shape are as vague and changing as its namesake.

While the capabilities underlying this technology paradigm have been in existence for more than a decade, they have matured in terms of definition, substance and demonstrated value. This has occurred to the point where cloud computing is rapidly being seen no longer as a novel innovation, but as an information technology (IT) framework that is for mainstream use.

One of the problems with the emergence and popularization of this framework is that the term "cloud" is now so pervasively used that the term "cloud washing" has been coined to refer to the tendency of industry to label everything it does as some form of cloud computing. This has the unfortunate effect of diluting the meaning and potentially the value of using cloud computing. It also complicates the evaluation of vendor offerings, thus a caution to those in that role.

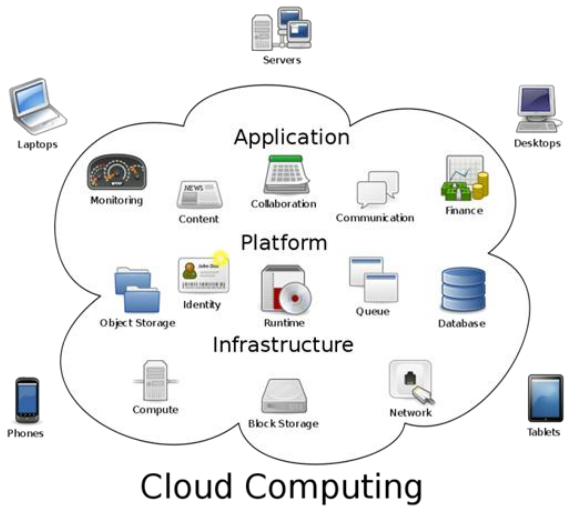
2 Executive Summary

The time is right for the health care community in Canada to consider the use of cloud computing as a strategic enabler and tactical vehicle for delivering timely and effective IT-enabled health services for Canadians. Cloud computing offers the health care system some very attractive economic advantages over traditional computing deployment models, thus the cost avoidance and savings can be redirected to the front lines of care delivery. Cloud computing has the potential to solve many pressing issues in the application of IT in health. It offers opportunities for innovative IT-enabled approaches to improving the health and wellbeing of Canadians by leveraging distributed health resources in organized ways. The cloud allows providers and more importantly health care delivery organizations the opportunity to focus less on managing IT and more on delivering care to their patients. However, one must utilize the appropriate cloud model for the application, ensure the service level agreement with their vendor(s) is appropriate, and the right privacy and security controls are in place.

The health care sector in Canada should give serious consideration to the use of cloud technologies and deployment models for the delivery of their health IT systems.

Cloud Computing Defined

The National Institute for Standards and Technology (NIST) in the United States is the source of the authoritative definition for cloud computing:



Cloud Computing

"Cloud computing 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."

Cloud has three models that provide computing resources for software (applications), platforms (middleware), and infrastructure (storage, CPU and networking) as services.

The three types of services can be deployed in four ways: private services dedicated to one organization; community services for organizations with a shared purpose or business domain; public services made available openly to a range of customers; or as

hybrid implementations that use a combination of the three deployments in an integrated fashion to meet a spectrum of needs.

The Economics of Cloud Computing

A 2010 Booz Allen Hamilton (BAH) study generally points to meaningful cost savings for operating a government services data centre in the cloud – as much as two-thirds lower than maintaining a traditional in-house data centre. Once cloud migrations are complete, the BAH cost model suggests annual operating savings in the 65-85 per cent range with the lower end attributable to the private cloud scenario and the upper end associated with the public cloud scenario.

Cloud Computing Opportunities in Canadian Health Care

There are many opportunities for the application of cloud computing in health care in Canada, ranging from: virtualization of infrastructures for individual organizations into a private cloud; establishing public clouds for health promotion or decision support; or development of community clouds to support integrated care delivery models for chronically ill patients or to rapidly implement IT solutions for health care and health promotion programs.

The EHRS infostructure and the EHR can be thought of as Software as a Service to clinical point of service systems deployed in a private cloud.

The EHR infostructures being implemented across the country are good candidates for virtualization as private or community clouds. The original vision for *Infoway's* EHRS Blueprint is very well suited to the cloud computing model. Like cloud, the Blueprint is a service oriented architecture (SOA) designed to provide interoperability and information sharing services to a broad spectrum of applications, in a highly scalable manner. Much of the e-health infostructure, such as: the Health Information Access Layer (HIAL), clinical domain systems, registry services and dedicated shared services (like consent or clinical decision support), can be considered Software as a Service (SaaS) that is offered by a ministry, health region or health care delivery organization. Providing EHR services from the cloud is just another type of implementation of the Blueprint that virtualizes the technology infrastructure.

However, like many other IT innovations, the entry point for cloud computing into the health care enterprise may be more readily accomplished via greenfield opportunities such as EMRs, e-referral, clinical decision support, PHRs, chronic disease management and remote monitoring.

Before health care delivery organizations embrace cloud computing, especially for mission-critical applications, several issues need to be addressed, including legitimate concerns about privacy and security. As well, organizations must fully assess the scope of affect, migration complexity and time requirements, cost of porting and cost of operations.

The approach to cloud deployment can and should be stepwise. It does not need to be an all or nothing approach. Organizations wishing to provide specific services for their clinicians and clients could implement private clouds to support more agile and dynamically scalable IT implementations. Cloud should be used to solve the growing demand to incorporate mobile devices and "apps" into the health care enterprise.

Cautious First Steps

Governments and health care organizations are taking a cautious attitude to cloud computing because of concerns about compliance with their own security and privacy policies and respecting regulatory obligations, but also over concerns about the potential for complex joint governance arrangements. Notwithstanding these concerns, the pace of cloud adoption in health care is likely to quicken in the mid-term out of the necessity to provide more service with relatively fewer resources.

...the pace of cloud adoption in health care is likely to quicken out of necessity.

While much work remains, the cloud computing industry is gradually addressing generic privacy and IT security risks. For example, safeguards such as virus protection and firewalls especially tailored to virtualization are coming into the market in addition to best practice tools, to assist cloud clients in assessing the wide range of risks. Security concerns and obligations associated with cloud computing rest with providers and customers.

Conclusion

The health care sector in Canada should give serious consideration to the use of cloud technologies and deployment models for the delivery of their health IT systems. Some industry observers look to the future and argue that individual hospitals and other health service delivery organizations do not need their own infrastructure. In fact, some predict that these organizations will be driven to adopt alternative models because they will not be able to attract and retain the necessary skilled human capacity or possess the financial resources needed to support in-house IT infrastructure.

Cloud computing is not the antidote for all financial pressures being experienced, but the purported benefits are difficult to ignore. To imagine a future where IT resources are unshackled from day-to-day tasks such as system maintenance, introduces the very real possibilities of focusing scarce staff on more important, challenging and rewarding initiatives like improving services and increasing innovation.

This white paper provides insight into the nature of cloud computing, opportunities for its effective application in the Canadian e-health and health care context, and identifies the risks and challenges associated with its use.

3 Cloud Computing Defined

A simplistic description of cloud computing is the provision of computing capability over a network (often the Internet) as a service that can be purchased by a person or organization.

The National Institute for Standards and Technology (NIST) provides this more detailed and authoritative definition for cloud computing[1]:

"Cloud computing 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models."

This cloud model promotes availability and is composed of:

1. Five essential characteristics
    1. On-demand self-service
    2. Broad network access
    3. Resource pooling
    4. Rapid elasticity
    5. Measured service
2. Three service models
    a. Cloud Software as a Service (SaaS)
    b. Cloud Platform as a Service (PaaS)
    c. Cloud Infrastructure as a Service (IaaS)
3. Four deployment models
    - Private cloud
    - Community cloud
    - Public cloud
    - Hybrid cloud

Key enabling technologies include:

- Fast wide-area networks
- Powerful, inexpensive server computers
- High-performance virtualization for commodity hardware.

[1] All of the definitional content here is derived from "NIST Special Publication 800-145, The NIST Definition of Cloud Computing", Peter Mell and Timothy Grance.

"The Cloud Computing model offers the promise of massive cost savings combined with increased IT agility. It is considered critical that government and industry begin adoption of this technology in response to difficult economic constraints. However, Cloud computing technology challenges many traditional approaches to datacenter and enterprise application design and management. Cloud computing is currently being used; however, privacy, security, interoperability, and portability are cited as major barriers to broader adoption."

3.1 Cloud's Five Essential Characteristics

Any true implementation of cloud computing must have the five essential characteristics. If any technology purporting to be cloud does not have these, then it is NOT a cloud-based technology.

1. **On-demand self-service**

   A cloud customer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

2. **Broad network access**

   Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops and workstations).

3. **Resource pooling**

   The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state or datacentre). Examples of resources include storage, processing, memory and network bandwidth.

4. **Rapid elasticity**

   Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

5. **Measured service**

   Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for the provider and consumer of the service.

3.2 Cloud Infrastructure

A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

3.3 Cloud Service Models

There are three service models for cloud:

Software as a Service (SaaS)

The capability provided to the cloud client is to 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. The cloud client does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

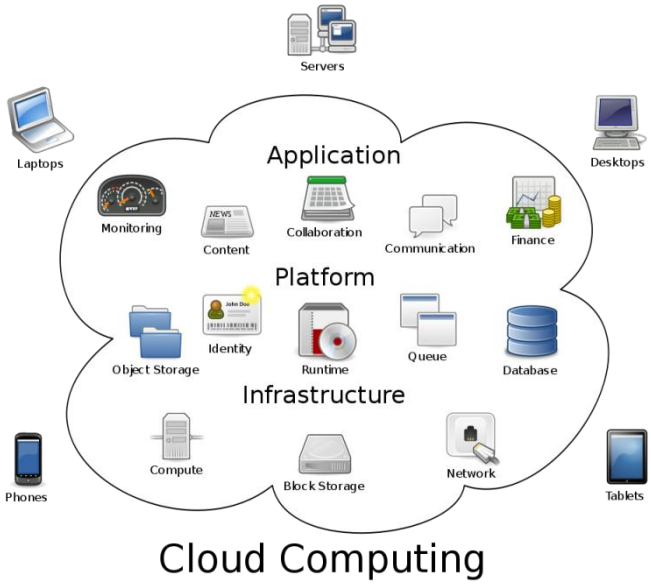


Figure 1: Cloud Service Models

Source: Wikipedia

Platform as a Service (PaaS)

The capability provided to the cloud client is to deploy onto the cloud infrastructure client-created or acquired applications created using programming languages, libraries, services and tools supported by the provider. The cloud client does not manage or control the underlying cloud infrastructure including network, servers, operating systems or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS)

The capability provided to the cloud client is to provision processing, storage, networks and other fundamental computing resources where the cloud client is able to deploy and run arbitrary software, which can include operating systems and applications. Depending on the cloud deployment model, the cloud client may not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Another representation that illustrates the layering of cloud service models is provided in Figure 2.

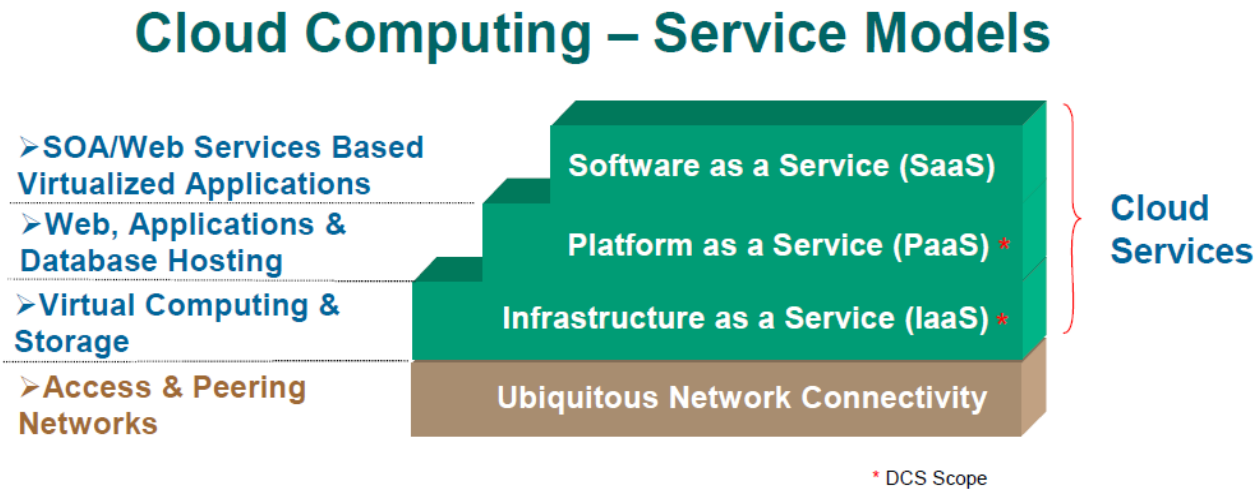


Figure 2: Layering of Cloud Service Models

Source: Danek, 2010

The layering of cloud service models helps define the dependencies of each model, one built upon the other, as well as the nature of the applications that each service model supports, for example whether that might be virtualized computing and storage, web hosting or SOA-enabled virtualized software applications.

3.4 Four Cloud Implementation Models

There are four recognized cloud implementation models. Each model comes with its own characteristics that must be considered when choosing to build or purchase cloud capabilities.

3.4.1 Private Cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

The emphasis here is that one organization governs and controls the use of the cloud for its own purposes. Accountability implementation, operation and use of the cloud is managed solely by that organization.

An example of a private cloud might be the conversion of all computing infrastructure (services, network and CPU) for a hospital to IaaS.

3.4.2 Community Cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

This implementation model is scoped by the user/customer base of the community of organizations served. The services provided are typically focused on the shared "business" of that community.

An example of a community cloud might be the implementation of a common e-referral and/or scheduling service for a Regional Health Authority (RHA) or an entire province. For additional examples please refer to section 3.4.4.

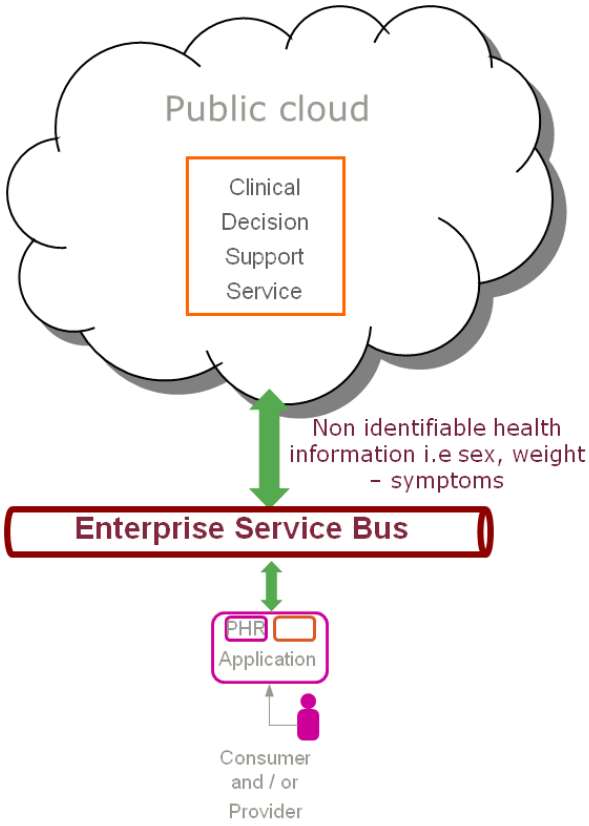
3.4.3 Public Cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by a business, academic or government organization, or some combination of them. It exists on the premises of the cloud provider.

This implementation model is well suited for generalized capabilities that are not specific to any one sector, community of users or organization.

An example of a public cloud implementation might be provisioning of email or office applications.

An example of the use of a public cloud might be the implementation of clinical decision support (CDS) service.



In this example we make the following assumptions and observations:

- The CDS service is used by public subscribers
- The CDS service is available as part of a consumer health solution such as a PHR, or is used by a health service provider
- Only non-identifiable health information is provided to the CDS service
- The underlying platform or infrastructure services may support multiple software services
- Because this application does not hold personally identifiable information, it can be operated anywhere in the world.

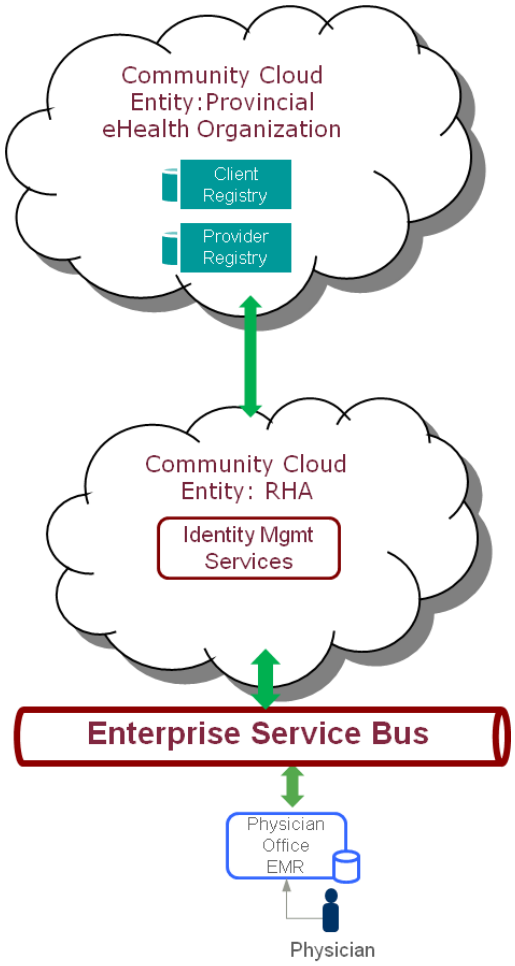
Infoway's rationale for suggesting this as a valid implementation includes several points:

- It may be the only feasible and cost effective way to deploy and scale an application that needs massive scale for deployment. A good example is IBM's Watson for differential diagnosis.
- The use of a single common public service centralizes the knowledge base of the CDS service's query logic.
- Using non-identifiable data as an input to the decision support service does not risk the privacy and confidentiality of any person, even though the service is provided in a public cloud.

- This model supports subscription and consumption-based business models either for individuals, application providers or organizations.

3.4.4 Hybrid Cloud

The hybrid cloud infrastructure is a composition of two or more distinct cloud infrastructures (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).



The hybrid implementation model is most often found in environments where the services provided cover a broad spectrum of the characteristics of privacy, governance and deployability. In a hybrid model, an organization may have some aspects of its technology deployed in a private model, other aspects of its business needs met by participating in one or more community models, and the most generic of its needs met by use of public cloud services.

An example of a hybrid cloud is one where an organization has implemented a private cloud for its mission-critical applications, it also participates in a community cloud for collaboration with business partners, and it has chosen to consume generic office services from a public cloud.

An example of a hybrid cloud implementation might be the integration of two community cloud service implementations to meet the needs of an RHA to provide a community service (such as e-referral) that utilizes Federated Identity Management (F/IDM) services provided by a community cloud run by a provincial e-health infostructure organization.

In this example, we make the following assumptions and observations:

- F/IDM services are offered by an RHA community cloud as a SaaS.
- F/IDM is a greenfield service.
- Identities are issued and used for mobile, EMR, hospital information system (HIS) and EHR users.
- F/IDM cloud leverages Client and Provider Registry (CR and PR) services from a provincial community cloud.
- The community cloud SaaS operates on its own platform and infrastructure services.
- The e-health organization may provide a common F/IDM SaaS that runs on the platform and infrastructure services in the RHA community cloud.
- Operational and inter-operational cloud governance is required.
- The regional community cloud leverages provincial CR and PR services provided in its own community cloud implementation.

3.5 Cloud 2.0

The phrase "Cloud 2.0" has been seen in the literature since about 2008. There are mixed interpretations of the use of this phrase. Some attribute it to the intersection of cloud capabilities and Web 2.0 as an enabler of social computing. Others have characterized Cloud 2.0 as a refinement of the hybrid model, where private cloud and public or community implementations are engineered to integrate seamlessly, providing services dynamically across the models as appropriate for the nature of the content.

Regardless of the rationale behind the phrase, we see a logical and necessary fusion in the use of cloud to support mobile computing, social computing, analytics and consumer enablement. In the evolution of the use of cloud, there will always be a compelling value proposition for augmenting enterprise or organization-specific cloud services with support for community cloud interaction and the use of non-proprietary/generalized information resources that will exist in the public cloud implementations.

This will certainly be true in health care, where many information and service assets regarding professional practice, administrative and office applications, and public reference information can be integrated with private or community-based services that support workflow, transactional processes and protected personal health information sources.

4 The Economics of Cloud Computing

Cloud computing has the potential to offer some very attractive economic advantages over traditional computing deployment models. In general, it offers significant savings by reducing the initial investment in computing hardware and in the overall support, maintenance and operations of that infrastructure. In some deployment scenarios, cloud computing offers consumers the ability to forgo capital expenses (e.g., building internal computing centres) in exchange for variable service fees. In addition to avoiding up-front capital investment, consumers of cloud services can also achieve significant operational savings by including that capability as part of the service.

In 2010, the consulting company Booz Allen Hamilton (BAH) conducted an economic analysis to investigate the potential savings of cloud computing for infrastructure services (IaaS)[2]. Their analysis included three deployment scenarios: public, hybrid and private. The BAH model also took into consideration transition costs, migration schedules and a (13-year) life-cycle of operational expenses. Their basis was a non-virtualized 1,000-server date centre scenario that was migrated to the three cloud deployment options. (Note: The economic metrics cited here from that report are based on the 1,000-server data centre. Sensitivity analysis was done with as few as 100 and as many as 4,000 servers in the report).

The BAH economic analysis of cloud computing distinguishes itself from other studies by including in its model cost components that are often overlooked in other analyses which generally limit their focus to hardware replacement savings. As a result, other studies may overstate the economic benefits of cloud computing.

Nevertheless, the BAH model should be of interest to decision makers of all organizational sizes because of its realistic consideration of the cost components and migration schedule associated with large scale, multi-year transition of an enterprise to the cloud. This report is further evidence that jurisdictional health systems should consider consolidating computing resources to fully realize the economics of cloud.

The BAH study generally points to significant cost savings for operating a data centre in the cloud – as much as two-thirds lower than maintaining a traditional in-house data centre. Once cloud migrations are complete, the BAH model suggests annual operating savings in the 65-85 per cent range with the lower end attributable to the private cloud scenario and the upper end associated with the public cloud scenario. However, the potential benefits are dependent on key sensitivity variables, including:

- Size/economy of scale: larger data centre scenario yielded almost five times the benefit as the small data centre scenario
- Deployment model scenarios: life cycle costs are lowest for public clouds and highest for the private cloud scenario, with the hybrid cloud scenario falling in the middle.

[2] http://www.boozallen.com/media/file/Economics-of-Cloud-Computing.pdf

Using their cost model, BAH estimated that the benefit to cost ratio (net present value (NPV) net benefits divided by NPV of investment costs) was 15.4 for public cloud, 6.8 for hybrid cloud and 5.7 for private cloud. This means that every $1 invested in public cloud computing could return more than $15 in benefits. (In the hybrid model 75 per cent of server workload was private and 25 per cent public). Viewed from another economic metric, the BAH model estimated discounted payback periods of: 2.7 years for public cloud, 3.5 years for hybrid cloud and 3.7 years for private cloud computing scenario.

The economic benefits are obtained through more efficient server utilization. BAH's model estimates that traditional, in-house computing environments experience a 12 per cent server utilization rate whereas in a cloud model it rises to 60 per cent. The difference in server utilization enables a relative reduction in the number of servers required in the cloud computing environment to serve the consumer's needs versus an in-house model. It means lower comparative capital expenditure and operating costs between the two environments. However, consumers with currently high server utilization rates will experience lower savings from a virtualized cloud environment.

Given the likelihood that health ministries and health service providers will deploy to private and hybrid clouds, the lower end of the benefit ranges for BAH's key metrics are more realistic targets to consider. There is, of course, the issue of scale which is an important factor that could cause cloud consumers to realize lower economic benefits. To address this issue in the USA, an operating agency – the General Services Agency – has been tasked with focusing the government on cloud computing and to provide a "storefront" where other government agencies can obtain IT services. In Canada, the federal government announced a similar initiative in June 2011. Shared Services Canada will have a mandate to streamline and reduce duplication in the government's IT services. Consolidation of provincial government IT services has also been announced or is underway in Ontario and British Columbia. It is a model that could be adopted by all jurisdictional governments in Canada on behalf of their health service providers.

5 Opportunities for Cloud in Health Care

This section evaluates potential opportunities for the e-health sector in Canada, and specifically for *Infoway*, to exploit cloud computing as an emerging technology.

5.1 Key Cloud Value Propositions for Health

The benefits and value asserted by cloud proponents in other fields certainly also apply to health care, however this portion of the white paper will attempt to frame benefits considering the nature of e-health and health care delivery in Canada.

5.1.1 Reduced IT Costs

Certainly the reduction of IT costs through multi-tenancy models, the improved percentage utilization of resources, and the "green benefits" resulting from reduced duplication of power consumption for processors and cooling are all material benefits to organizations providing IT-enabled health care. In those sectors where cloud has seen some substantial implementations, typical claims for cost reductions from re-platforming existing applications are from 15 to 35 per cent.

These cost reductions are likely to be more immediate and readily measured for applications and resources that can be acquired through public cloud offerings. However, given the privacy and security issues associated with the retention and transmission of personal health information, use of public cloud may be constrained to applications that do not manipulate personally identified health information or that are not mission-critical transactional applications.

For this reason, applications that leverage cloud to support internal organizational processes, intra and inter-organizational interoperability, clinical workflow and productivity, and broad spectrum deployment models such as chronic disease management or public health, may need to be delivered using private or community implementation models. While these models also benefit from multi-tenancy and other cost reductions operationally, there may still be some capital expenditures associated with establishing these capabilities before porting existing systems over.

Implementation of greenfield applications in health care may operate more economically, but addition of new cloud-based applications will still be a new additional cost.

5.1.2 Reduced Complexity/Increased Scalability and Extensibility

One of the core value propositions is derived from the service oriented architecture nature of cloud solutions, namely the layering of services and the establishing of standards-based interfaces between those layers. This allows the addition of, or swapping out of, components in each layer without necessarily introducing additional complexity in other layers. This permits greater scalability and extensibility of IT capabilities offered through cloud. *This may be a critical success factor for coping with the proliferation of mobile devices and "apps."*

However, the trade-off here is that these benefits are best achieved by solutions that have been engineered to take advantage of these approaches from the outset. Porting existing applications to a cloud model may actually require additional middleware or enablers to allow traditional applications to work effectively in a cloud model.

Fortunately, many cloud vendors or solution providers use the features of cloud itself to provide components or adapters to make this possible for traditional applications and cloud.

5.1.3 Increased Business Agility

One of the biggest benefits to e-health from the use of cloud is the ability to rapidly acquire and implement a cloud-based solution. This agility results from removing the time required to rationalize new capital costs, the time and capacity required to put necessary infrastructure in place, and procurement cycles (as mentioned in the next section).

In addition, the use of community cloud implementation models at regional or jurisdictional levels allows for the introduction of health service delivery programs across organizations, disciplines and geographies much more readily than when hosted by only one "owning" entity. In a community cloud implementation, the establishment of a governance model to manage the shared asset also supports the governance necessary to implement health service delivery programs that utilize resources that "belong" to various contributing organizations.

5.1.4 Reduced IT Sales and Acquisition Cycles

Some of the most difficult aspects of using IT to innovate and support operational aspects of health care delivery are the challenges of identifying, acquiring or building, and then operationalizing solutions that have their own costly infrastructures. Once baseline service level agreements (SLAs) are in place for foundational cloud capabilities, particularly in IaaS or PaaS, it becomes much simpler and less difficult to rationalize and then move from concept to implementation for IT solutions at the software or SaaS layer. This has the net effect of reducing sales cycles for solution vendors and acquisition cycles for purchasers. This lends itself to greater predictability of annual departmental and organizational budgets and an ability to more rapidly and effectively connect the expenditure with the benefits of the implementation of IT.

This will potentially increase the willingness of IT solution providers to invest in innovative and high-value-add solutions, while at the same time allow purchasers and implementers of solutions to plan strategically.

5.1.5 Increased Measurability/Accountability

The inherent nature of the service patterns and SLAs associated with implementing cloud-based IT requires that capacity planning be well done, and utilization accurately and consistently measured in a very timely fashion. This "feature" of cloud provides a degree of transparency, and to measure and rationalize the cost-benefit of solutions, that is something that is often difficult to achieve in conventional IT deployments. This could be a considerable boon to achieving sustainable health care through effective, measured use of IT.

5.2 Opportunities for Cloud in the Health Sector in Canada

There are many opportunities for the e-health sector in Canada to take advantage of cloud capabilities. This section elaborates on the main opportunities we see emerging.

Many of these opportunities take advantage of the ability of a cloud-based solution to allow organizations to deploy applications without constraining the footprint of the application to within their organization or physical facility.

In addition, cloud-based IT allows for collections of organizations, whether they are RHAs, Local Health Integration Networks (LHINs) or jurisdictional ministries, to deliver coherent health care services and programs to a population using the spectrum of health service providers that serve those citizens.

5.2.1 Consolidation/Virtualization of IT Services

The core value proposition of cloud-based IT is one of the early opportunities for e-health in Canada, whether that be for individual organizations wishing to virtualize their network, storage or processing capacity for existing applications in a private cloud implementation, or those who wish to take advantage of multi-tenancy cost savings for a shared cloud implementation, possibly as part of a community or a hybrid cloud.

This could include establishing cloud implementations to service common software application used by multiple facilities in a region or jurisdiction, provisioning EMR and CIS application capabilities through cloud. In addition, jurisdictions may wish to deploy multiple HIALs, or they may wish to improve scaling and extensibility of a single HIAL through virtualization of services. The SOA upon which the Blueprint for EHR solutions is based is well suited to transition to a cloud-based IT model.

5.2.2 Collaborative Care/Care Continuity

There is an opportunity to use cloud-based services to support collaboration among departments, organizations and care settings to improve the ability of mixed care teams to deliver better health outcomes for individuals and populations of patients and persons with certain health conditions.

For example, University Health Network (UHN) in Toronto has been developing a prototype of a departmental collaboration service that has a great deal of potential to be virtualized and extended to provide information services to providers who deliver services to a shared group of patients, ensuring that patient-care transitions safely and appropriately across shift changes in the facility and through discharge.

This capability could be readily adapted to enable virtual teams anchored by family physicians. This cloud-based service could/should include the safe transition of patients out of one care setting and into another, for example from a long-term nursing facility to acute care and back again, or between ambulatory care settings and home care.

This capability would ideally be implemented in a community cloud model.

5.2.3 Support for Increased Use of Mobile Devices and Apps

One of the significant challenges facing health care delivery organizations is the exponentially growing demand for the use of various mobile devices, ranging from tablets and smart phones through intelligent peripherals that accumulate data for aggregation and incorporation into a person's EHR and/or consumer health application. This proliferation and the highly fluctuating demand for network and connectivity resources will place considerable strain on traditional IT operational and delivery models.

This demand will come equally from health service providers, administrators and clients and patients of the health care systems. In this sense, providers and patients will see this as a necessary and ubiquitous form of consumer enablement that they will be experiencing in other dimensions of their personal lives and occupations.

Cloud-based approaches to authentication, device management and access to a common backplane of data provide the ability to handle the rapid acquisition, connection, management and widely varying resource demands these devices will place on the systems and applications health care organizations will be compelled to provide.

5.2.4 Support for Social Networking and Consumer Enablement

Cloud-based implementations provide a flexible and readily scalable method for supporting the integration of social networking into e-health service delivery patterns and enabling consumers of health services to become active participants in their care. This could include participating in communities of people with the same condition, becoming part of their own virtual care team, or simply allowing people to participate in the scheduling of their own appointments or review of results.

Capabilities that do not rely on sensitive person-centric health information could readily be provided by public cloud implementations. Capabilities that require collaboration across organizations and that potentially involve disclosure of personal health information, would be better served through community cloud implementations, and some dedicated capabilities might be better served through private cloud implementations.

Regardless, the key to incorporating these concepts effectively in e-health-enabled service delivery will be in appropriately (and ideally seamlessly) incorporating these into hybrid cloud implementations, where capabilities are appropriately placed giving consideration to privacy/security requirements, the need to bridge service delivery across more than one organization, mission-criticality of applications, and the ability to govern the multiple varied SLAs that will be required.

5.2.5 Public Health

The highly distributed nature of public health services as well as the need for consistent, measurable and comparable service delivery across geographies and populations are all factors that make it well suited to a cloud-based implementation model. This capability could be provided in a private, community or hybrid cloud implementation model.

5.2.6 Chronic Disease Management

Many programs delivered at a jurisdictional level, such as those for chronic disease management (CDM), could benefit from cloud-based implementations as this would allow IT applications focused on addressing CDM to be made readily available to health care providers across the spectrum of care settings and disciplines, regardless of the organization they work for or their location. Cloud-based solutions would provide the ability to enlist existing service providers in these programs virtually, by providing them with tools, care plans and other resources to ensure that patients enrolled in a CDM program receive consistent, coherent and continuous care, regardless of where they receive service or from whom.

This also gives patients the ability to participate in a CDM program to receive educational information and relevant test results and to track their progress. Cloud-based social computing would also permit chronic disease patients to participate in social-support communities.

These capabilities would likely be delivered in a hybrid approach, with a mix of private, community and public cloud models.

5.2.7 Analytics

Cloud computing and big data analytics are both receiving quite a bit of attention lately across the IT industry. Regardless of the deployment models (public, private or hybrid), analytics and big data when combined with cloud computing are being seen as newfound capacity for better high-performance capabilities within companies. The agility of cloud platforms provides analytical applications with a scalable environment to leverage the large amount of data.

Cloud computing is opening up huge opportunities for companies with everything from cloud bursting to meet peak demand to hosting a scalable data analysis platform. Given the rise of big data and the various cloud computing models, companies are seeing and experiencing that collecting and using massive amounts of data isn't so hard any more. We are seeing a point in the improvement of performance and costs that companies can now afford to perform analytics and simulation for key business processes that improve and understand customer experiences and buying patterns.

Whether it's called "predictive analytics," "smart computing" or "analytics on cloud," cloud computing and analytics provides a comprehensive offering of a combination of products that enable enterprises to move their business intelligence, data warehousing and online analytical processing (OLAP) workload to a cloud platform. While the implementation of cloud analytics can take several forms at a high level, the following are parts of a cloud analytics platform that would be of interest to an enterprise:

- A virtualized infrastructure to support the basic cloud tenants to build a private/public/hybrid cloud
- PaaS in-line with the underlying cloud infrastructure that can support the analytical needs of reporting, analysis, dashboards, extraction, transformation and load (ETL) and predictive analytics
- Customized analytics applications in a PaaS/SaaS offering which are uniquely positioned for designing and developing customized analytics applications. The cloud provider is responsible for on-demand provisioning and the maintenance of software and hardware.

There are two trends that are driving this evolution:

- A convergence of enabling technologies like virtualization, inexpensive memory, powerful software middleware and others that make large-scale analysis practical for nearly any size data set, and for nearly any size business.
- The trend in the use of big data analytics in the ever-growing competitive pressure to accelerate and sharpen business decisions is seen as key to giving companies a competitive advantage in the marketplace.

The convergence of mobile, cloud, social and analytics continues to accelerate. Cloud apps that are not "socially aware," have no mobile support or support for analytics, are already being looked at as "legacy apps." Industry analytics see more and more application vendors bringing in feature parity in their apps for different mobile applications. Mobile web apps will dominate over native apps and analytics will be a key component of these applications. Companies will start to incorporate social media and collaboration with their business analytics. These will be embedded in strategies around unified communications, collaboration and social applications for customers, and will aid in determining trends and strategies that the business will need to focus on.

In health care, the interest is high in big data and predictive analytics to support the mining of this data (and therefore leveraging cloud computing architecture), however uptake still remains largely theoretical and untouched for many organizations. This is primarily due to patient privacy and security considerations.

Analytics and big data is gaining support mostly in financial, retail and insurance industries, where there is a focus on engaging with the customer and understanding social perspectives of customers. More and more Fortune 500 companies are diving into the cloud and using analytics against big data to perform complex calculations on very large data sets. Predictive analytics is emerging as a capability which allows companies to create models that can predict customer behaviour and other critical business information. The use of “big data” in predictive analytics is seen as a key enabler for companies in the creation of new services and new campaigns to reach existing and new customers.

Also, small to medium-sized businesses are a new targeted market for widespread cloud adoption and may find distinct new advantages in deploying certain analytics capabilities. As many of these types of organizations lack the IT infrastructure for an in-house cloud, the public cloud model offers lower upfront cost barriers for analytics or business intelligence (BI) and faster access to analysis options. As an example, for sales and marketing, companies will look to use the cloud to analyze customer data, gain visibility into the sales pipeline or understand the impact of social media on marketing initiatives. Customer engagement will become more and more important to companies.

5.2.8 Professional Practice and Continuing Education

Public cloud implementation models are well suited for applications that provide educational and professional practice content at a discipline level, whether those disciplines be in clinical, administrative or allied health fields. A good example of this is eHealth2Share, a web-based cloud for health care organizations to share information, created through a partnership between Toronto’s Baycrest Centre for Geriatric Care and Microsoft. Another opportunity might be the transitioning of products such as PatientOrderSets.com to a cloud model for consumption at the point-of-service based on clinician, care setting and patient condition context.

5.2.9 Appointment Brokering/Scheduling

There is a whole spectrum of logistics and process-oriented services that could be provided within organizations or shared across health regions or entire jurisdictions. The use of cloud approaches offers the flexibility and agility to allow the business side of health care to innovate and create a stronger sense of coherence and continuity of public health care to citizens. Appointment brokering/scheduling is one of those types of applications. This service could be provided in a private cloud for use within large health service delivery organizations, in a community cloud model for sharing across a number of organizations in a health region or jurisdiction, or in a public cloud model provided there is some degree of protection for the appointment reason information.

There is also tremendous potential to enable consumers to participate in this pattern and incorporate mobile application support for them as well as for health service providers, care planners and administrators.

5.2.10 E-referral

Like appointment scheduling (and potentially integrated with it), electronic referral processes could benefit from private or community cloud implementations. Because referral patterns typically require some disclosure of personal health information, and a picture of a person's conditions can be readily inferred from the pattern of appointments, there needs to be consideration given to protecting information used in this service.

5.2.11 Supply Chain Management

Supply chain management is a well-established capability in most sectors, and is seeing significant growth in health care as a means of driving down costs and improving efficiencies and timeliness in ordering and inventory management. This service is ideally suited to a public cloud implementation, readily supporting multi-tenancy customers on a broad scale.

For example, in January 2012, one HIS vendor announced a fully-integrated, cloud-based sourcing solution designed to completely automate the health care supply chain. The cloud-based application will give providers visibility and control over their medical-surgical supply spending. The solution is the first offering on the market that can support multiple materials management information systems (MMIS) and combine external and internal data for a single, comprehensive view of an organization's supply chain spend.

Another example is a U.S. based provider of comprehensive cloud based e-sourcing services to the health care sector. The company's solutions have been deployed to reduce the cost of products and services for all areas of the supply chain, purchased services, construction and capital. The cloud solutions services individual hospitals, medical schools and health systems throughout the United States.

5.2.12 Enterprise Resource Planning

Deployment of community cloud-based enterprise resource planning (ERP) could be used extensively in health care, not only to drive down costs, but potentially also to provide an ability for large facilities or health regions to more flexibly deploy and manage their human, fixed, movable and consumable assets.

5.2.13 Cloud-based Privacy and IT Security Solutions

The cloud computing industry is beginning to offer critical IT security services and infrastructures. These services are intended to improve the robustness of traditional enterprise IT security solutions or supplement the level of IT security with other cloud services.

Privacy and IT security features can be offered as SaaS, PaaS or IaaS. The following are examples of privacy and/or IT security offerings for each cloud computing service model:

IT Security Platform as a Service (PaaS) Opportunities

Web Services Security Functionality

Web Services Security (WS-Security) is a proposed IT industry standard that addresses security when data is exchanged as part of a web service. WS-Security is one of a series of specifications from an industry group that includes IBM, Microsoft and Verisign. Related specifications include the Business Process Execution Language (BPEL), WS-Coordination and WS-Transaction.

The protocol specifies how integrity, privacy and confidentiality can be enforced on messages and allows the communication of various security token formats, such as Secure Access Markup Language (SAML), Kerberos and X.509 Digital Certificates. Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security. The WS-Security protocol provides a model for many levels of security needed for web services.

WS-Security specifies enhancements to Simple Object Access Protocol (SOAP) messaging aimed at protecting the integrity and confidentiality of a message and authenticating the sender. WS-Security also specifies how to associate a security token with a message, without specifying what kind of token is to be used. It does describe how to encode X.509 certificates and Kerberos tickets. In general, WS-Security is intended to be extensible so that new security mechanisms can be used in the future.

These security tokens allow for single sign-on capability that allows for the verification of end user credentials across multiple applications in addition to interoperable authorization permissions.

WS-Security requires the implementation of various hardware and software components as a platform for development of web services and sites.

Functionality for the Web Services platform could be offered similar to capabilities defined in *Infoway's* HIAL. This could entail a secure look-up feature for available and authorized e-health applications/services.

IT Security Infrastructure as a Service (IaaS) Opportunities

IaaS could be the security features of a series of firewalls, anti-virus functionality or virtual private network (VPN) access for a community cloud network. This offers the potential of reducing software acquisition and management costs for integrating HIS or EMR applications to a regional e-health hub.

The market for cloud-based privacy and security services will primarily be for greenfield deployments requiring increased and uniform levels of privacy protection and IT security at reduced deployment costs.

While much work remains, the cloud computing industry is demonstrating that processes, techniques and best practices are evolving to meet privacy and IT security concerns.

IT Privacy and Security Software as a Service (SaaS) Opportunities

One of the principal privacy challenges in health care is the management and enforcement of patient information wishes, commonly known as informational consent. Many EMR and HIS solutions do not offer this capability and would require potentially costly retrofits to support this legislative requirement. By offering this software capability as a service in a community or private cloud, EMRs and HIS solutions operating in a cloud context could leverage this feature at reduced costs and implementation timeframes. This would also have the benefit of ensuring a uniform implementation, interoperability of consent directives and reduced overall consent solution management costs.

Consent Management Solutions

As indicated earlier, cloud security offerings would mostly be in the areas of greenfield services and/or functionality. One of the potential areas of new applications and/or services would be consent management solutions.

Consent management solutions are a critical privacy function in the health care sector. The management of an individual's informational consent directives with regard to the use and collection of personal health information (PHI) is a legislative requirement in several jurisdictions.

A business and technological solution to the management of consent directives would need to be interoperable across provincially managed health data banks, physician EMRs and mobile devices. Rather than developing and integrating consent management solutions for each EMR and e-health mobile computing app, which would reach into the thousands, a more cost effective deployment approach would be to develop and deploy a consent management service as part of a cloud offering. This would have several benefits such as a central point to manage consent management rules, simplified end point computing integration, reduced speed of deployment and a uniform and consistent application of a person's consent wishes.

IDM and Federated IDM

Identity and access management services, which offer one-stop shopping for the issuance and management of digital identities, and single sign-on functionality for cloud-based applications, are SaaS opportunities.

These types of solutions have the potential to manage all digital identities for a wide range of users, from citizens in a consumer health application to EMRs and HIS, as they integrate into jurisdictional iEHR solutions. This would have the benefit of standardizing authentication mechanisms and increasing levels of trust in the EHR eco-system at reduced cost and quicker time to market.

Mobile Device Management

Another example is cloud-based mobile device management (MDM) solutions. These are used to manage security and privacy features of tablets and smart phones deployed in the enterprise (e.g. hospital). This cloud-based service allows the management, use and inventory of mobile devices without the expense of implementing new hardware and software to manage the mobile infrastructure. This cloud-based service permits the uniform and consistent implementation of IT security and privacy policies across all mobile devices.

Secure Email

The federal government's "Community Cloud" offers secure email as a service to all participants in the cloud. E-health community clouds could offer a similar service to EMR and HIS applications not offering this capability.

6 Business Considerations for Cloud in Health

There are many things that need to be considered by any individual or organization when determining whether to build or subscribe to a cloud-based service. This section presents some of these considerations organized by their business impact, the impact of choosing a particular implementation model, and the general privacy/security issues that operating in the cloud may present.

6.1 Business Impact Considerations

6.1.1 Consumerization as a Driver

The visibility of cloud-based capabilities to consumers will become a significant driver for organizations to consider cloud-based solutions. Product offerings such as NetFlix and Apple's iCloud make the features and capabilities of cloud very visible to the average person. The fact that cloud is being used to allow consumers' data (music, files, photos, video, documents and apps) to be portable and ubiquitously available to them will generate a demand for similar capabilities across the organizational workplace, or for the customers of those organizations.

Increasingly, consumers will expect that their consumer-centric information be readily accessible by more than one device, more than one application, and in more than one location. This requirement is difficult to solve without considering cloud-based solutions.

This driver is amplified by the fact that cloud-based capabilities often can be purchased with a credit card without requiring any capital costs. This means, one way or another, cloud solutions are likely to be very visible in health care soon.

6.1.2 Considerations for Individuals

Clients of the health care system need to be made aware of the privacy and security implications of acquiring or participating in a cloud-based environment.

Individuals need to be aware of and agree with where their data is held, how it may be used, and ideally have some transparent means of monitoring its access and use. The ease of acquisition of a cloud-based technology, particularly for mobile apps, may hide or obscure this fact for the end-user.

6.1.3 Considerations for Health Service Providers

Health service providers are consumers and generators of information and services. Pervasive networking and mobile computing are causing service providers to expect to be able to do their jobs and service their clients in different care settings and contexts, and to be able to use a spectrum of applications that are function specific and also operating against a consistent backplane of data that ranges across customer-centric and provider-centric information.

Health service providers need to consider the reliability of any cloud-based technology they employ, their rights and obligations in its use, and what happens to data they collect using this technology. This includes the data related to what they do, as well as the data of the clients/patients they treat. Privacy and security issues similar to those raised in considerations for individuals are applicable to health care providers using cloud services.

They also need to consider that any cloud-based technology they acquire individually may require unique login assertions and that, unless their organization or jurisdiction enables the capability, the data they access and collect through that technology may be completely siloed and segregated from other relevant information they may need or expect in order to fulfill their professional responsibilities as a provider of health services.

6.2 Cloud Implementation Considerations

6.2.1 Considering Implementation Models

Infoway considers these four implementation models as characterized primarily by their scope of use and control. Determining what cloud implementation model is appropriate for a given situation is a matter of balancing these considerations. The characteristics of each cloud implementation model have a direct correlation to:

a) Privacy and Security

Each cloud implementation model has varying degrees of control and assurance regarding the relative privacy and/or security of information and services provided. As a generalization, the spectrum runs from private cloud providing the highest degree of potential control and accountability, to public cloud providing the least degree of control and accountability.

This does not necessarily mean that information in a public cloud may not be private and secure. It just means that the consumer of the service has little to no transparency as to what happens with that information.

b) Governance

Each cloud implementation model has a different relative degree of governance attached to it, with public cloud having the least governance, private cloud having the narrowest governance and community cloud requiring the broadest and most comprehensive governance, as it must meet the varied needs of the community it serves while providing corresponding transparency and accountability.

c) Deployability

Each cloud model has inherently differing degrees of deployability (or flexibility and scaling of capacity), with public cloud having the broadest possible utilization, and private cloud having the most controlled and constrained deployment footprint.

6.2.2 Incremental Adoption and Implementation of Cloud

It is important to remember that implementing a cloud-based solution does not necessarily require that an organization completely re-engineer all aspects of its computing environment and application base. Cloud capabilities can be introduced incrementally as appropriate for an organization's needs.

The least complex entry point to cloud is the use of an application or capability that is readily available from public cloud providers today. These applications tend to be generic, either non-sector specific (such as email services) or at least commonly used across the health sector without exposing personally identified information.

Implementing a private cloud is more impactful to an organization, as it must provide all of the baseline infrastructure services, however at least the scope of the implementation is entirely within the organization's control.

Implementation of community cloud is probably the next degree of complexity, simply due to the scope of effect on a broader community and the change management and governance issues that must be addressed to achieve an effective and sustainable implementation.

Certainly a hybrid cloud is probably the most complex model as there are many more moving parts and the different aspects of the hybrid environment need to be balanced and implemented in consideration of each other operationally. However, once a baseline pattern and infrastructure are in place, a hybrid implementation model may offer the greatest flexibility, extensibility and scalability for future needs.

Regardless of the approach chosen, any organization implementing or participating in a cloud-based capability should have a roadmap that establishes precedence, timelines and criteria for selecting, acquiring, implementing and extending the capabilities they obtain from cloud solutions.

6.2.3 Shift of Costs from Corporate Capital Expenditures to Departmental Operations

Administrators and purchasers of technology to support health service delivery need to carefully consider the transfer of costs associated with acquiring a cloud-based technology. Many of the IT system costs (and constraints) associated with traditional implementations "go away" when acquiring cloud-based technology. However, these capital expenditures and other costs become entirely replaced with operational costs for cloud services that may be allocated to their respective business units directly.

While cloud-based technology may be readily acquired, these costs become an expense item against the department's operational budget, and this needs to be taken into account.

6.2.4 A Cloud Provider's Obligation is to the Service Level Agreement

As many organizations discovered in the outsourcing trend of the 1990s, a provider of a cloud-based technology service is measured and compensated by its adherence to the SLA. If the SLA does not anticipate or consider exceptional circumstances that may affect the business obligations of the purchasing organization, that organization may find itself in a difficult spot as the technology service provider's loyalty is to the SLA, not necessarily the mission and goals of its customer organizations.

This means that for mission or time-critical applications provided by cloud technology, administrators must ensure the SLA reflects their nominal requirements and they must consider how exceptional circumstances will be addressed. In addition, administrators need to carefully consider their contingency strategies, particularly for mission-critical applications.

6.2.5 Speed of Acquisition does not Mean Speed of Deploy

Administrators need to recognize that the ease of acquisition of cloud-based technology does not replace the need to plan for and execute due diligence processes and change management aspects of the implementation of the technology. There is a need to ensure that workflow, business processes and end-user training are all appropriately in place to enable the technology to be effective.

6.2.6 Build or Buy?

Administrators need to be aware that it is possible to purchase cloud-based solutions outright as applications (typically in a public cloud model) as opposed to acquiring cloud technology services such as IaaS (e.g. storage or CPU capacity), and/or PaaS (such as DBMS, or middleware) to develop their own SaaS solutions. These decisions can be made as an individual organization, which would typically be delivered in a private cloud model, or as a group of organizations that share a common purpose or customer/patient base and wish to use a shared set of cloud services offered in a community or hybrid model. It is up to each organization to determine whether the capabilities it requires can be purchased from a public cloud, obtained by choosing to be a member of a community cloud implementation, or built by the organization itself in a private or hybrid cloud approach. This later choice essentially makes an organization a cloud provider and a cloud customer.

6.2.7 Establishing a Business Case

While the value proposition of using cloud-based technology can seem very appealing, there does not seem to be a body of practical knowledge on the business case and rationale for moving from traditional IT to cloud. However, things that should be considered in making such a case include the need for:

1. An enterprise approach to the use of cloud to avoid proliferation of departmental cloud products
2. Maximizing return on capital expenditures through better resource utilization
3. Improved responsiveness to technology needs, especially for organizations with limited IT capacity.

Section 5.1 provides additional information on the value aspects that can contribute to a business case.

6.3 Privacy and Security Considerations

All computing models must address the same set of privacy and IT security risks and requirements, such as authorized access to information and information resources, and cloud computing is no different. These common risks and requirements are not discussed below, as the focus will be on the potential additional risks associated with cloud computing. While not an exhaustive list, these risks and issues are a summary of the most prevalent challenges facing implementers. This section will describe the high level risks/issues and provide an assessment of how community and private clouds can reduce generic cloud computing risks.

6.3.1 Reduced Privacy and IT Security Governance and Control

The use of cloud may accelerate externalization of system user identities, security, infrastructure and services, especially in the context of public clouds. This externalization could mean the loss of direct control of this dynamic security perimeter. This also includes the overall governance of privacy and IT security within the cloud.

6.3.2 PHI Aggregation/Consolidation

Multi-tenancy applications, services and IT infrastructures in a public or multi-industry cloud means the natural aggregation of PHI in cloud silos and shared resources. The integrity of shared services must also ensure that users and applications of other cloud clients do not have unauthorized access to PHI. The sole reliance on contractual arrangements to ensure only authorized access to PHI may be insufficient. These risks are far more prevalent in public cloud offerings where privacy/security features and requirements are opaque to the cloud client.

6.3.3 Misalignment of Privacy and IT Security Requirements

Another area of generic concern with non-industry specific cloud services is the potential mismatch between the security requirements specific to the health care sector as compared to other industries. There is a risk that privacy and IT security mechanisms implemented for a wide range of industries may be insufficient for the protection of PHI. An example would be the level of robustness provided by authentication mechanisms.

Public and hybrid cloud offerings may not have sufficiently robust levels of system user authentication, exposing data custodians to additional risk of unauthorized access to PHI, in addition to exposing e-health enterprise solutions to security risks and vulnerabilities introduced by the interconnectivity between the cloud provider and proprietary regional and provincial e-health networks. It is imperative that cloud clients clearly articulate their privacy and IT security requirements prior to choosing to use cloud computing, a cloud computing deployment model or a cloud provider. They should ensure a cloud provider of services, infrastructure and applications meets and demonstrates compliance to health care requirements.

6.3.4 Reliance of Externalized Audit and Monitoring

The monitoring and auditing of information and communications technology (ICT) infrastructures, services and applications is a core construct of secure and privacy-enhanced EHR solutions. The ability to monitor and audit is key to investigating and resolving potential and real privacy and security breaches. Public cloud offerings that render auditing and monitoring mechanism opaque to cloud clients may expose data custodians and information managers to additional business risk if they cannot detect potential breaches and monitor appropriate access to PHI.

6.3.5 Data Loss and Reliability

As PHI is moved to the cloud it increases inherent risk of data loss and reliability. The loss or lack of availability of PHI is a serious concern and is a potential patient safety issue that must be appropriately managed. A typical public cloud provider’s contractual provisions and insurance may be insufficient in the context of e-health.

6.3.6 Confidentiality and Integrity of Data

End-to-end confidentiality and integrity of PHI is a basic tenet of all EHR solutions. However, in a shared, multi-tenant cloud environment it is critical that PHI is encrypted from the point of service (POS), whether citizen, physician EMR or iEHR connecting into a cloud infrastructure. Achieving this objective is more complex in a shared tenant environment/infrastructure typically found in public clouds. Cloud clients must ensure they are satisfied with the IT security mechanisms, policies and procedures offered by the cloud provider.

7 Considerations for Cloud in Health Care

The following sections highlight two key considerations for decision makers. The first topic covers a set of considerations for the development of a roadmap for the introduction and use of cloud in an e-health infostructure.

The second is *Infoway's* assessment of the evolution of cloud in the near terms (< two years), medium term (two-five years), and the long term (five-10 years). It is derived from a variety of sources and our own perspective on the current state of health care IT in Canada.

7.1 Considerations for the Introduction of Cloud in Health Care

At the time of this document, we see some adoption of cloud in health care, however it is very limited in terms of scope and the scale of the projects attempted to date. Implementations are typically related to greenfield opportunities rather than porting of existing environments to cloud-based services.

For cloud to be successfully introduced to health care:

- Misperceptions need to be corrected
- Legitimate concerns about privacy/security need to be addressed
- Better information needs to be provided to allow organizations to assess the scope of affect, migration complexity and time requirements, cost of porting and costs of operations.

The ability to introduce cloud capabilities will also be dependent on a clear understanding of the relative pros and cons of the public, private, community and hybrid implementation models and the ways in which each model can be used to greatest advantage.

7.2 Considerations for Cloud Deployment

This section's considerations are predicated on the concept that much of the e-health infostructure can be considered SaaS. When looking at the HIAL, domain systems, registry services and dedicated advanced services (like consent or clinical decision support) these can all be viewed as software services to a set of clients or users. The difference here from traditional definitions in the context of this discussion is that the offering party of the SaaS is a ministry, health region or health care delivery organization.

Given that context, what would be the considerations for deployment or re-deployment of these software services or components by those parties into a cloud infrastructure?

The suggested considerations are presented below, in no particular order. They should be analyzed against criteria suitable to the context of the software service they need to be applied to, such as use cases, software service function, privacy and security requirements, service level requirements, existing agreements, and anticipated evolution of the software service.

The fact that the EHRS Blueprint is based on a SOA pattern makes it possible to port all or portions of the EHRS infostructure to cloud-based delivery models. However, definitional work is needed (such as application architecture, best practices, cloud provider due-diligence checklists, SLA frameworks, cloud standards, etc.) to allow stakeholders to refactor their EHR infostructures as cloud-based solutions.

This discussion is independent of the type of cloud offering, but given the nature of the offering party the most likely is the use of a private or community cloud. The physical cloud infrastructure, its design and its operations may or may not be outsourced.

7.2.1 Current Solutions

The redeployment of current solutions, or parts thereof, into the cloud is largely an infrastructure decision. The aspects to consider are:

1. Suitability of the software solution's design to a cloud infrastructure.
2. Issues on resource utilization. Either too much is underutilized and future growth is best handled via cloud virtualization. Or, not enough computing capacity is available during peak times, warranting an increased investment and virtualization of existing resources to handle that load.
3. Capacity requirements over the next three years should be evaluated. Basic metrics like transaction volume and load should be factored into the decision.
4. Operational characteristics, such as quality of service and service reliability, should be factored into the decision. Persistent issues may be mitigated by use of cloud-based infrastructure.
5. The return on investment should be evaluated. Some vendors promote at least a 15 per cent savings in their offerings. Some organizations have claimed up to a 50 per cent reduction in their infrastructure costs. The return on investment (ROI) may be realized only if there is anticipated growth in the use of the computing infrastructure. One anticipates growth in the use of IT-enabled health care. Therefore, the task is to estimate the increase in capacity requirements and timelines for those against the return on the investment moving solutions to the cloud. One must also factor in the cost of re-deployment from the old to new infrastructure in the ROI calculation.
6. Assessment as to the appropriate cloud deployment model taking into consideration information governance and custodial responsibilities in the event PHI is collected or used.

7.2.2 New Deployments

New solution deployments should give very strong consideration to the use of a cloud-based deployment model. The initial opportunity for specification is at procurement. This is especially true when the procuring entity is responsible for the cost of the infrastructure, ongoing operations and SLAs with its users (in contrast to the respondent having those responsibilities). This deployment consideration needs to take into account the nature of the solution and whether it is suitable for cloud.

Moving to the cloud initially with a new deployment is advised for an organization with little or no experience with the technology (versus porting an existing solution to the cloud). This affords an opportunity to gain experience in specification, deployment and operations during pre-production phases of the project.

7.3 Cloud in Health Care Evolution Forecast

7.3.1 Cloud in the Near Term

Cloud Washing will Peak then Subside

In the near term, we expect the tendency to frame any form of web-enabled offering as cloud to peak and then rapidly diminish. This will be the result of the dilution of the meaning of the term through overuse, and through purchasers of systems becoming more aware of what cloud provisioning really means, which is:

- Virtualization of capacity (CPU, storage, or network bandwidth)
- Dynamic scaling of capacity as required
- Sharing of capacity across multiple applications and potentially multiple organizations (multi-tenancy)
- Costs indexed to variable consumption of resources
- SLAs based on predicted demands and measured against actual demand.

If a service does not provide these basic capabilities, then it is not truly a cloud service.

Greenfield Applications First

We expect greenfield implementations to dominate in the near term, with the exception that some productivity applications such as office software, email, ERP and supply chain management will be introduced in public cloud implementations. However, even in these cases, this will be less a porting of existing systems to cloud-based provisioning than replacement of these capabilities locally with cloud-based services.

Cloud and Mobile Computing Integrate

In the next two years we can expect to see a strong emergence of cloud-based services in support of mobile computing. Very rapidly we may see significant growth in the number of organizations acquiring cloud services to provision and manage mobile applications and devices.

Cloud and Social Networking will Experiment

Provisioning of social networking applications for health through cloud-based applications will emerge, although this will be done tentatively at first. There is always the possibility of a killer health care app emerging in this space, however it is unclear how organizations will manage/leverage the implementation of such capabilities in a hybrid environment.

Niche Middleware will Expand Rapidly

PaaS offerings acting as middleware between the consumer and health care provider organizations will gain adoption quickly. We expect to see mobile device management solutions increase their footprint rapidly in health care, as consumers (patients and health service providers) demand to be able to leverage their smart devices in their respective roles.

This will also extend to PaaS capabilities to manage user identity across devices and care settings.

Larger organizations that choose to create their own mobile app development capability may also purchase PaaS offerings that allow them to readily develop, test, and port mobile apps to their user-base.

7.3.2 Cloud in the Medium Term

Proliferation of Services and Providers

As the various aspects of cloud computing progress through Gartner's hype curve in the next two years, we expect to see a proliferation of different flavours of services across the spectrum, and in the number of companies providing these services.

This increased competition has the advantage of driving price points down, but comes with the disadvantages of confusion in the marketplace and the probability that, in the medium term, the market will rationalize itself and we will see some providers fail and others be assimilated.

In the medium term, it will become important that purchasing organizations be very diligent in assessing the applicability and viability of any cloud provider they seek to engage with.

Cloud Brokering

Organizations that embrace cloud computing will quickly discover that no one provider of cloud services can provide the capabilities they require to meet a particular need. In fact, there may be two or more SLAs in place with multiple cloud providers. As more organizational systems are provided through cloud, this proliferation of providers and associated agreements will require a broker to facilitate the definition, agreements and consumption of cloud services. For large organizations these brokers may be the internal IT department.

Migration of Organizational Computing to Cloud

In the medium term, a few organizations may shift their main computing capability to private or community cloud implementations. Community cloud implementations have the benefits of economies of scale and leveraging of skills in this technology.

Surviving the Trough of Disillusionment

It is inevitable that the elevated expectations for cloud in the early days will be countered by the challenges in implementation and benefits realization. Organizations need to understand this reality and, if they believe in the value proposition asserted by the cloud technologies they have embraced, be prepared to sustain their commitment to the course until their implementations stabilize and operational issues are addressed.

7.3.3 Cloud in the Long Term

Infoway will regularly monitor, review, validate and adapt evolving cloud migration strategies and best practices for the e-health community in Canada.

8 Privacy and Security Concerns and Considerations

Privacy and security concerns have consistently ranked as the most common reason for limiting the adoption of cloud computing. While cloud computing faces similar privacy and security risks and requirements as traditional computing models, it also presents several new privacy and IT security related challenges. Therefore only the privacy and IT security risks that are a direct consequence of cloud computing models will be discussed in this section.

The question then becomes: How do privacy and IT security issues and risks differ in a cloud computing context? The short answer is:

> When compared to traditional computing models, several cloud deployment models have the possibility of offering similar levels of privacy and IT security risks.

8.1 Context and Background

The key differentiator with regard to privacy and IT security concerns with specific cloud deployment models is the potential reduction in the amount of control by data custodians and information managers over privacy and security safeguards for PHI.

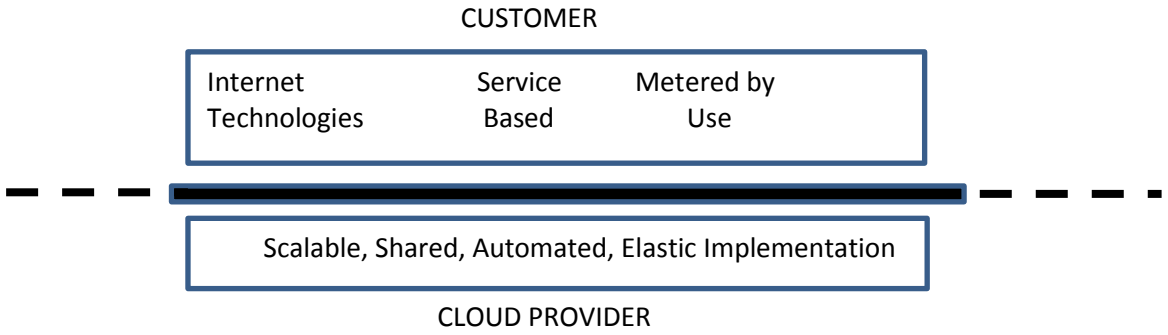
This section will begin with a discussion of the non-technical generic risks of cloud and provide a comparative analysis of these risks to specific cloud deployment models. This white paper also identifies several considerations and opportunities for managing privacy and IT security risks to assist implementers in choosing the appropriate cloud deployment model.

The industry has taken a very proactive approach to addressing the privacy and IT security risks associated with cloud computing. Several initiatives from the NIST, the Canadian Government and the CSA are promising. For example, the CSA has recently released Version 2.1 of its Cloud Controls Matrix (CCM), a baseline set of controls aligned to the CSA guidance and mapped to industry standards, regulations and frameworks to help organizations with cloud risk management. The CCM is part of the CSA's GRC Stack toolkit, which also includes the Consensus Assessments Initiative Questionnaire, a set of questions a cloud customer can ask a cloud provider to gauge its security.

8.2 Why is Privacy and IT Security a Concern for Cloud Computing?

Privacy and IT security risks and challenges in a cloud model are dependent to a large degree on the cloud deployment model. To better understand these issues, basic knowledge of the various cloud deployment models is necessary. The following definitions are taken from a Gartner blog.[3]

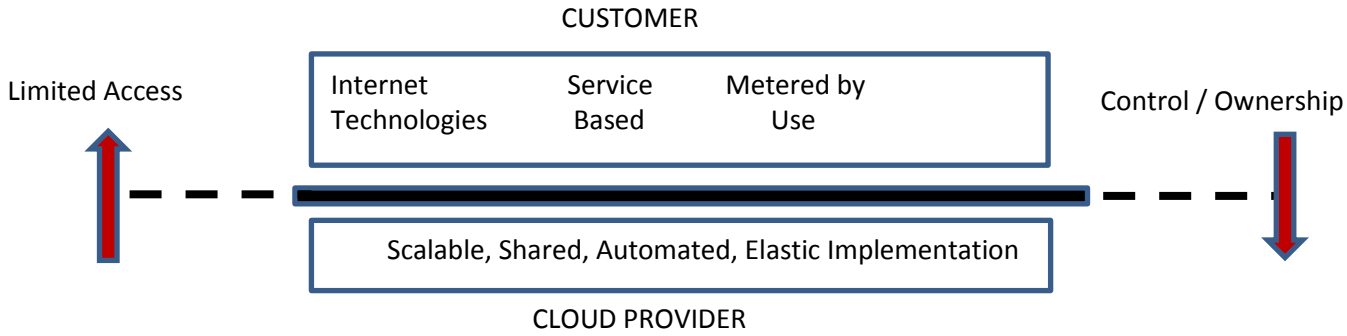
Gartner's official definition of cloud computing is: "A style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to customers using Internet technologies." We also describe five defining attributes of cloud computing: service-based, scalable and elastic, shared, metered by use, and uses Internet technologies. A key to cloud computing is an opaque boundary between the customer and the provider. Graphically, that looks like this:



When the customer does not see the implementation behind the boundary, and the provider doesn't care who the customer is, you have a public cloud service.

So what is private cloud?

Private cloud is "A form of Cloud computing where service access is limited or the customer has some control/ownership of the service implementation."



[3]Gartner Blog by Thomas Bittman, VP Distinguished Analyst. "Clarifying Private Cloud computing" May 18, 2010 http://blogs.gartner.com/thomas_bittman/2010/05/18/clarifying-private-Cloud-computing/

Graphically, that means that either the provider tunnels through that opaque boundary and limits service access (e.g., to a specific set of people, enterprise or enterprises), or the customer tunnels through that opaque boundary through ownership or control of the implementation (e.g., specifying implementation details, limiting hardware/software sharing). Note that control/ownership is not the same as setting service levels – these are specific to the implementation, and not even visible through the service.

The ultimate example would be enterprise IT, building a private cloud service used only by its enterprise. But there are many other examples, such as a virtual private cloud (the same as the example above, except replace "enterprise IT" with "third-party provider"), and community clouds (the same as a virtual private cloud, except opened up to a specific and limited set of different enterprises).

From a privacy and IT security perspective, ICT system managers and data owners typically have complete control of data safeguards and risk management processes within the dedicated health care enterprise perimeter. A public cloud model may eliminate or reduce traditional IT security solution control, reliability, risk management and monitoring capability. In many cases, public clouds offer little control over cloud provider ICT safeguards, yet cloud customers must maintain accountability and responsibility for the protection of PHI.

Public cloud replaces the traditional IT security perimeter with a virtual enterprise perimeter. The dynamic, unknown to client and outsourced nature of this traditional IT security perimeter has increased business risk. In a public cloud, virtual cloud IT security perimeters cut across multi-tenant, shared architectures utilized by nearly all cloud service clients, whether they are software, infrastructure or platforms.

Public cloud clients typically incur additional risks related to the reduced or complete lack of risk management transparency by cloud providers.

8.3 Mapping of Generic Cloud Risks and Issues to Community-based or Private Clouds

E-health specific community or private clouds have the potential to greatly reduce the generic cloud risks and issues identified above.

Private and or e-health community-based clouds have the potential to offer data custodians and information managers more control over governance, security mechanisms and infrastructures, thereby potentially reducing risk. Assurances as to whether privacy and IT security is appropriately governed, in addition to demonstrated compliance by the cloud provider, are facilitated in a community or private cloud. The risks associated with consolidation and aggregation of PHI may be reduced in infrastructures that support common data, application and infrastructure requirements.

E-health community specific and private clouds would allow for the establishment of data safeguards appropriate and standardized to the health care industry, thereby potentially reducing this risk. It is important to note that health care specific cloud requirements and standards have yet to be developed, but could potentially be leveraged from other industries.

E-health community or private clouds should also provide greater controls over data loss and availability, as cloud clients would play an important oversight role in the determination of data availability and recovery requirements and mechanisms.

Risk mitigation related to end-to-end confidentiality and integrity of PHI is potentially simplified in the context of an e-health community or private cloud. Common requirements, standards, policies, procedures, IT security and privacy mechanisms appropriate for PHI can be established and uniformly applied to manage risks.

The following table illustrates how the generic cloud risks can be managed when compared to the various cloud computing deployment models. This assessment is based on the above assumptions for e-health community and private clouds.

Computing model	High level generic cloud specific risks and issues					
	Governance/ control	PHI consolidation	Alignment of P&S require-ments	Auditing/ monitoring	Data loss/ reliability	Data confidentiality /integrity
Traditional computing	Low	Low	Low	Low	Low	Low
Public cloud	Increased	Increased	Increased	Increased	Increased	Increased
Community or private cloud	Equivalent to traditional computing models	Equivalent to traditional computing models	Equivalent to traditional computing models	Equivalent to traditional computing models	Equivalent to traditional computing models	Equivalent to traditional computing models

The major differentiators between the three cloud models are related to the levels of control, IT security, reliability and ownership of the cloud solution.

Public cloud offerings typically provide less control over choice and operations of IT security and privacy mechanisms.

Business risks decrease as we move from a public to community or private cloud. Governance of business solutions is simplified in a community or private cloud, as core business information systems support a common set of requirements for an industry.

Private or dedicated health care community cloud offerings can provide the opportunity for collaboration in determining the appropriate levels of data safeguards and processes necessary to manage risk.

Recognizing that the removal of barriers related to cloud risks is fundamental to successful adoption, the cloud computing industry is gradually attempting to address generic privacy and IT security risks. To assist cloud clients in assessing the wide range of risks, the CSA has created a "List of Top 10 Threats to Cloud Computing, v.1.0." We suggest reviewing this material for a more in-depth discussion of cloud-related privacy and IT security risks.

8.4 Considerations for Privacy-enhanced and Secure Use of Cloud Computing

8.4.1 Governance Challenges in Cloud Computing

Public cloud offerings typically do not provide details concerning the governance of privacy and IT security, including policies, procedures and roles/responsibilities. The industry tendency is to provide this level of detail as part of community and/or private cloud offerings. Data custodians and information managers should give consideration to their privacy and IT security governance role in the context of cloud computing. In several jurisdictions data custodians have legislated obligations and may not wish to delegate all governance and operational aspects to a public cloud provider. An example would be the monitoring and investigation of unauthorized access and potential breaches.

8.4.2 Due Diligence of Cloud Providers

In the absence of clearly defined cloud privacy and IT security certification programs, it is recommended that cloud clients give consideration to a formal due diligence process. The onus is on cloud clients to ensure that cloud providers are compliant with applicable regulations and legislation. The use of third party audits for compliance is a valuable tool in the due diligence process. Cloud clients should consider structuring contractual agreements in a way that indicates the cloud provider comprehends and will respect regulatory issues and possibly share liabilities.

Consideration should be given to leveraging due diligence tools such as the CSA CCM version 2.1, which is a baseline set of controls aligned to the CSA guidance and mapped to industry standards, regulations and frameworks to help organizations with cloud risk management. The CCM is part of the CSA's GRC Stack toolkit, which also includes the Consensus Assessments Initiative Questionnaire, a set of questions a cloud customer can ask a cloud provider to gauge its security.

As privacy and IT security are based on technical solutions, policies and procedures, the due diligence process should include these dimensions. The following is a subset of the areas that should be considered in a due diligence process:

1. Physical, network and application security
2. Data confidentiality and integrity
3. Data retention, backup and infrastructure/services availability
4. Business continuity and disaster recovery
5. Identity management and access control
6. Authentication mechanisms levels
7. Liability and insurance.

8.4.3 Location of PHI and Information Resources

In a typical outsourced computing model the location of servers, networks, data centres and the physical resource where PHI is stored is well documented and accessible for audit purposes. In a public cloud environment there is no market expectation for cloud providers to demonstrate the above. In the case of PHI, several jurisdictions have restrictions on the location of PHI that may affect cloud usage decisions and cloud provider service implementations. E-health community or private clouds allow cloud clients to govern the location of PHI and information resources and should be considered as an alternative to public clouds when PHI is collected, used and stored.

8.4.4 Risk Management Frameworks and Transparency

Cloud clients should consider the development of a formal risk management framework (RMF) specific to cloud computing environments. This framework and its associated tools and methodologies can be used as part of the initial cloud provider due diligence process and subsequent monitoring and compliance process. The RMF should take into consideration industry best practices and leverage tools commonly used to manage privacy and security risks such as privacy impact assessments, threat risk assessments and vulnerability assessments.

The use of contractual instruments to encourage the use of RMFs by cloud providers will be important in demonstrating compliance to privacy and IT security requirements and regulatory obligations. Transparency of the RMF must also be given consideration as RMFs are predicated on transparency of privacy and IT security risks, risk mitigation strategies and compensating controls, therefore transparency should be included as part of contractual agreements. RMFs should also be considered as part of community or private clouds as they will play a key role in managing risks and demonstrating compliance for cloud clients.

8.5 Opportunities for Cloud-based Privacy/Security

8.5.1 Privacy in Public Clouds

Notwithstanding the IT security risks and associated privacy implications of public clouds, they can still play a privacy enhanced role in e-health applications.

The following use case illustrates how a public cloud can be used and not negatively affect an individual's privacy.

Privacy requirements are a direct result of the collection, use and disclosure of PHI. By reducing the privacy requirements a public cloud can be used in the context of e-health services.

The use of IBM's Watson as part of a public cloud offering to perform diagnosis is a prime example. Watson can be deployed in a public cloud available to a consumer health solution and providers. By providing non-identifiable information a user of this public cloud service can obtain diagnosis options without requiring the level of data safeguards and privacy normally associated with the use of PHI.

Other examples of public cloud clinical services would be anonymized drug utilization review and clinical decision support services.

8.5.2 Risk Management Best Practices

While cloud computing raises new privacy and IT security challenges, there are several efforts underway to assist cloud providers and clients in the management of risks. The CSA has representation from both communities and is creating artefacts that advance risk management in the cloud computing environment. Version 3 of "Security Guidance for Critical Areas of Focus in Cloud Computing" provides a framework for managing cloud-specific risks.

The NIST has also published SP 800-144; Guidelines on Security and Privacy in Public Cloud Computing. These documents provide a comprehensive set of best practices and should be leveraged when considering cloud computing.

While still in its infancy, there are industry initiatives underway to develop acceptable trust models and security evaluation criteria to be used in cloud computing security certifications.

9 Conclusion

As the technological and business understanding of how to implement cloud computing matures, there is a significant opportunity for the health care community in Canada to consider the use of cloud as a strategic enabler and tactical vehicle for delivering timely and effective health services for Canadians.

Cloud computing has the potential to solve many pressing issues in the application of IT in health:

- Cloud provides an opportunity for reduction of operational IT costs while at the same time increasing the scalability and flexibility of deployed IT solutions.
- Cloud can enable organizations to deploy information systems more rapidly, by reducing the time needed for acquisition and implementation of solutions, and reducing the approval and funding challenges for up-front capital costs associated with large IT projects.
- However, to take advantage of these capabilities, the health care sector in Canada needs to have a much better understanding of what it means to "operate in the cloud," and how to manage the transition from a capital expenditures model to a demand-based operational expenditures model.

Cloud computing offers opportunities for innovative approaches to improving the health and wellbeing of Canadians by leveraging distributed health resources in organized ways:

- Cloud provides an opportunity to rapidly implement program-level solutions over distributed geographies and across a spectrum of user communities.
- Cloud allows for varying degrees of organization control and governance, from private and purpose-specific infrastructure to computing and software capabilities shared by a community of organizations with a shared purpose and a shared governance model.
- Cloud can be a foundational enabler of mobile and social computing, permitting the dynamic deployment and scaling of these technologies and applications.

Concerns about privacy are not a valid reason to avoid cloud computing:

- Each of the deployment models (private, community, public or hybrid) can be leveraged as appropriate to the privacy needs of the application and the community.
- Regardless of the deployment model, there must be mature, transparent and well managed mechanisms to ensure secure implementations that appropriately meet the privacy and disclosure requirements of each jurisdiction in the country.

Finally, jurisdictions that are implementing EHR systems based on the EHRS Blueprint architecture are very well positioned to transition to cloud computing:

- The Blueprint and cloud implementations are based on a SOA
- In many cases existing EHR infostructures, or parts thereof, can be transitioned to the cloud model by virtualizing the underlying infrastructure, and by ensuring that information assets and EHR capabilities are provided using SaaS implementations.

It is the authors' hope that this white paper has provided enough context and meaningful information to result in a strategic discussion by the health care sector in Canada on approaches to the adoption and implementation of cloud computing.

10 Bibliography

The following sources have been consulted in the development of this white paper.

Top Ten Healthcare Game Changers, Accenture, 2011

Rippert, Don; Michael, Dr. Gavin; Swaminathan, Dr. Kishore: Technology Vision 2011: The technology waves that are reshaping the business landscape, Accenture, 2011

Top 10 Healthcare Game Changers: Canada's Emerging Health Innovations and Trends, Accenture, 2011

Plummer, Daryl C.; Middleton, Peter: Predicts 2012: Four Forces Combine to Transform the IT Landscape, Gartner, 2011

Smith, David Mitchell: Hype Cycle for Cloud Computing, 2011, Gartner, July 27, 2011 G00214915

Heiser, Jay; Clearley, David W.: Hype Cycle for Cloud Security, 2011, Gartner, July 28, 2011 G00214151

Desisto, Robert P.: Hype Cycle for Software as a Service, 2011, Gartner, July 28, 2011 G00214934

Smith, David Mitchell: Key Issues for Cloud Computing, 2011, Gartner, April 1, 2011 G00212080

Bittman, Thomas J.: Key issues for Private Cloud Computing, 2011, Gartner, April 1, 2011 G00212000

Haight, Cameron: The Cloud Is Less Important Than the Cloud Operating Model, Gartner, March 29, 2011 G00211464

Mell, Peter; Grance, Timothy: National Institute of Standards and Technology (NIST) "The NIST Definition of Cloud Computing – Recommendations, NIST Special Publication 800-145

Petri, Gregor: Shedding Light on Cloud Computing, Ca Primer, January 2010

Hugos, Michael; Hulitzky, Derek: Business in the Cloud – What Every Business Needs to Know About Cloud Computing, John Wiley & Sons Inc.

Armour, Quinton; Thizy, Didier: HIMSS Whitepaper "11 Disruptive Technologies That Will Change the Face of EHRs – and How Your Competition is Using Them", Macadamian, October 2010

11 List of Abbreviations

ASP	application service provider(s)
BAH	Booz Allen Hamilton
BI	business intelligence
BPEL	Business Process Execution Language
CCM	Cloud Controls Matrix (of the Cloud Security Alliance)
CDM	chronic disease management
CDS	clinical decision support
CIO	chief information officer(s)
CR	client registry
CSA	Cloud Security Alliance
EHR	electronic health record
EHRS	Electronic Health Record Solution (Blueprint)
EMR	electronic medical record(s)
ERP	enterprise resource planning
ETG	Emerging Technology Group (of *Infoway*)
ETL	extraction, transformation and load
F/IDM	Federated Identify Management
GDP	gross domestic product
HIAL	Health Information Access Layer
HIS	hospital information system
IaaS	Infrastructure as a Service
ICT	information and communications technology/technologies
IT	information technology
ITM	information technology management
LHIN	Local Health Integration Network(s)

MDM	mobile device management
MMIS	materials management information systems
NIST	National Institute for Standards and Technology (US)
OLAP	online analytical processing
NPV	net present value
PaaS	Platform as a Service
PHI	personal health information
PHR	personal health record
POS	point of service
PR	provider registry
RHA	Regional Health Authority
RMF	risk management framework
ROI	return on investment
SaaS	Software as a Service
SAML	Secure Access Markup Language
SLA	service level agreement(s)
SOA	service oriented architecture
SOAP	Simple Object Access Protocol
VPN	virtual private network
WS-Security	web services security

12 Contact

Infoway established an Emerging Technology Group (ETG) in 2011 to identify and guide the use of information and communications technologies (ICTs) in health care innovation. The ETG's role is to identify and evaluate emerging technologies, and mature technologies that haven't been fully applied, that look most likely to provide significant benefits to our health care system and the health of Canadians.

This white paper is the first in a series the ETG will be producing, with the aim of providing information and analysis that could benefit those who make decisions about technologies for health in Canada.

For more information about the ETG and its work, contact ETG@infoway-inforoute.ca