

Using Managed Services As A Software Delivery Model In Canadian Health Care

September 9, 2005

Authors:

Darren Jones
Darcy Matras

INTRODUCTION.....	3
MANAGED SERVICES DEFINED.....	4
MANAGED SERVICES OVERVIEW.....	4
A DIFFERENT WAY.....	4
IMPLEMENTATION RESOURCING COMPARISON.....	5
MANAGED SERVICES: CHALLENGES IN A HEALTH CARE SETTING	6
SECURITY.....	6
PATIENT PRIVACY	8
INTEGRATION.....	8
SUMMARY.....	9
MANAGED SERVICES BENEFITS	9
EXPERT DOMAIN KNOWLEDGE.....	9
FLEXIBILITY.....	9
SOFTWARE UPDATES.....	9
CONCLUSION.....	9
APPENDIX 1 - ARCHITECTURE STRATEGIES	10
APPENDIX 2 - STAND ALONE ARCHITECTURE.....	11
APPENDIX 3 - INTEGRATED ARCHITECTURE.....	12
APPENDIX 4 - NETWORK CONNECTION ARCHITECTURE	13
REFERENCES.....	14
STANDARDS ORGANIZATIONS.....	14
INTEGRATION VENDORS.....	14
MANAGED SERVICE SOFTWARE PROVIDERS IN THE HEALTH CARE INDUSTRY.....	14

Introduction

Successful IT initiatives in health regions provide measurable positives for client care, patient flow, and increases in capacity. However the results of a failed initiative can be disastrous, resulting not only in burned-out staff and a wasted investment in capital and change management, but also in a credibility deficit against future initiatives.

One way to potentially increase the odds of a successful IT project is to use a managed service solution. By definition, a managed service solution provides a turnkey approach to:

- Software
- Hardware
- Hosting
- Implementation
- Change management
- Support

This white paper is meant as a reference tool for using a managed service model for software applications in the Canadian health industry. This is intended to be a high level overview and does not pursue specifics of particular software, hardware, or operating systems.

This paper will:

- Explain the benefits of a managed service solution
- Review the challenges that are intrinsic to a managed service solution
- Explore the Security and Architecture models available for managed services within the health industry

Managed Services Defined

Managed Services Overview

In the past, when a requirement for software was identified, a health region typically had three options:

- Buy existing software
- Buy existing software and have it customized
- Build new software in-house

All of these options typically require the health region to host the applications on internally managed servers and infrastructure, or in a hosting environment that has been contracted out for 3rd party support; in either case the applications are accessible only within the region's network. If access outside a region's network is required, a virtual private network (VPN) would typically be used.

Costs associated with a typical software deployment include:

- Software costs
- Software support costs
- Hardware costs
- Hardware support costs
- Technical project planning and implementation
- Change management project planning and implementation

A Different Way

A new and proven option exists for the health care industry to purchase software in the form of a **managed service provider (MSP)** solution. The MSP model includes the servers, hardware, and hosting as well as the software as part of the overall solution.

This type of solution means that instead of purchasing servers, software, and third party software licenses for report writers and database management services, a Health Region can purchase software as a service that essentially operates as a black box.

Furthermore, this type of service allows a health region's operations and planning departments to drive the purchase and implementation of clinical software without requiring their IT department to re-allocate technical resources. This can be a boon to an implementation when technical resources are already focused on core imperatives such as the framework for the EHR system and compliance with new health standard requirements.

Moreover, conventional software and support contracts only define the software components and support response being delivered. In contrast, MSP contracts are defined in terms of outcomes, and implicitly create a Service Level Agreement (SLA) that goes beyond the measurement of application availability for a defined period of time and at a defined level of performance. A managed service implementation allows the evaluation of success to be focused on how the software is actually helping the health region perform, rather than purely evaluating software installation or performance. Because the managed service provider is responsible for the complete product, including delivery, both parties are working towards a successful outcome, and the roles in terms of technical performance are clearly defined.

Implementation Resourcing Comparison

The implementation of a managed service application requires far less involvement of IT staff than a typical software implementation. Outlined below is a high level comparison of the typical implementation tasks for a shrink-wrapped software implementation in health care versus a managed service implementation.

Typical Shrink-wrapped Software Implementation vs. Managed Services Implementation:

Shrink-wrapped Implementation	Component	Managed Services Implementation
	RFI	
	RFP	
	Product Selection	
	Product Purchase	
	Hardware Purchase or Allocation	
	Software Installation And Upgrades	
	Scalability Testing	
	Acceptance Testing	
	Pilot	
	Deployment	
	Production	
	Server Support	
	1 st Tier Application Support	
	2 nd Tier Application Support	
	Software Update Installation	
	Disaster Recovery	

Legend

Health Region Responsibility - Software Vendor Responsibility - Shared Responsibility

Managed Services: Challenges In A Health Care Setting

There are some unique challenges to the managed services model in health care:

- **Security:** *The security requirements are the same as for internal implementations, but there is more of a technical challenge in addressing security requirements*
- **Patient Privacy:** *The privacy requirements are the same as for internal implementations, but there is more of a technical challenge in addressing these privacy requirements.*
- **Integration:** *Most health care applications must interact with an evolving EHR or EMPI system*

Security

Many health regions are currently outsourcing at least part of their hosting and support for servers. A secure co-location facility that is already hosting for a health region is a great candidate for hosting an MSP solution. Additional security concerns in a health region will include:

- User Access
- Data Security
- Communication Standards
- MSP Administrative Access

User Access

The challenge in any software that allows users to view confidential information is to ensure that users can and are accessing only that information which they need to see as integral to their duties. User access concerns can be mitigated if a managed service application supports the following functionality:

- Defining the physical locations where an application can be accessed
- Authenticating legitimate users
- Defining which areas in the software users have access to based on pre-defined roles
- Ensuring a viewable user and client view / change audit history is available

Additional considerations that may be applicable depending on the type of managed service application would include:

- Username / Password Standards
- Two-Factor Authentication
- LDAP Integration
- Single Sign On / Context Management (CCOW)
- User Notification

Data Security

Data encryption is a requirement for any managed service solution in the health industry. The only questions about data encryption are, what type of encryption should be used, and where should it be used. As the main focus of this paper is web based managed services, below is an overview of where encryption can fit into a web based managed service solution.

Web Browser – SSL

This should really be considered a requirement, as opposed to an option. A minimum of 128 bit SSL encryption with a valid certificate is the standard today, and should advance as encryption standards increase.

Using Managed Services As A Software Delivery Model In Canadian Health Care

Web Services – SSL

If web services are used in the application, all communication should use 128 bit SSL encryptions with a valid certificate.

Data Storage

It is possible to encrypt all data as it is written to the database, using either logic in the application, or functionality within the database. While this does provide an extra layer of security, it impacts both data integrity and the ability of support to update the database directly. New technology is making the encryption of database data a more attractive option, and most major databases will support encryption of a complete or partial data set.

Hosting

Each client in a managed service environment should have their own servers, network connection, and a physical separation from other clients. Reasons for physical separation include:

- Less chance of data corruption from other clients
- An increased flexibility in terms of scalability
- Protection from denial of service attacks
- An increased flexibility for maintenance windows

Firewall

Firewall configuration will need to work off the principle of closing all ports and opening only those required as opposed to opening all ports and closing only suspect ports. With a web based application, the only ports that are required to be open would be:

- SSH
- SSL
- VPN

Communication Standards

HL7 Communication

HL7 is a very useful standard for communication between health care focused software. When implementing HL7 integration in a managed service solution, all HL7 communication should be done within a VPN tunnel or secure dedicated network connection. Using a secure tunnel will provide a secure route for the data. Otherwise, the data in the communication could be compromised as it leaves the health region's secure internal network.

Data Warehousing

One of the challenges for a health region when using a managed service is the lack of an internal database in which data is stored, and thus not having that data available for ad-hoc reporting or comparison with other regional data. One solution to this dilemma is having database replication from the operational database to a data warehouse within the region's network. When providing the region with a database replication, it is necessary to either flatten the database into simplified logical reporting tables, or to educate regional data analysts in the business logic required to query the database.

MSP Administrative Access

Using Managed Services As A Software Delivery Model In Canadian Health Care

The MSP must be required to use similar levels of security when accessing the system to perform administrative and maintenance functions. A combination of SSH, SSL, and VPN will typically suffice.

Patient Privacy

Most health regions will be subject to patient privacy legislation, and will require that a Privacy Impact Assessment or equivalent performed before any new software is implemented. This study must show that the proper care is being taken with respect to patient privacy, and that the benefits of the system will outweigh any risk that is introduced with the implementation of the application. Typically a health region must create and submit the Privacy Impact Assessment, but they will use technical information provided by the managed service provider to describe the system in the assessment.

Integration

There are currently huge gains being made in regards to integration strategies in the health care industry. Standards such as HL7 and Clinical Context Management Specification (CCOW) are almost becoming a default option for health care software. These standards work extremely well with the managed services approach, as it allows managed service software to have the same degree of plug and play functionality as an internally hosted application.

Summary

Managed Services Benefits

There are many advantages to a managed services model for software delivery in health care:

- The software can be deployed quickly, with an immediate focus on operational outcomes.
- The software can be acquired with a limited capital investment.
- The nature of the contract means that both parties are driven to meet the business needs rather than worry about the underlying enabling technology.
- Internal IT requirements are minimal, allowing critical technical resources to focus on core projects.

In particular, a web based managed service provides:

- A close collaboration between health regions and third party vendors
- Access to stakeholder workstations outside a region's internal network
- Access without any installation on existing workstations that have internet access
- Access for all workstations to one common version of the application

Expert Domain Knowledge

By using a managed service solution you have access to trainers that are focused on particular products, and who are experts in the application domain. In addition, the support staff for a managed service solution are not only well versed in support of the application, but are also experienced in working with users to determine the base problem of a user's issue. This results in filtered calls to a health region's support department, further reducing the resource requirements from the regional side.

Flexibility

Managed services is a "pay as you go" model, so when an application reaches the end of its useful life cycle, a health region simply stops paying and stops using the application.

Software Updates

Because the licensing is grouped in with a managed service solution, all upgrades, new versions, and bug fixes are included with the managed services fee; therefore, there should be no additional charges as an application evolves.

Conclusion

Managed services can be a powerful tool for a health region that wants to quickly implement a software product and deliver strong operational outcomes. It can reduce the risk associated with typical software projects, and can create an environment for collaboration among all stakeholders during the implementation, rather than a one-sided implementation being carried by health region resources. Although there are challenges associated with a managed service solution, they can be overcome by using a combination of technology and communication standards. After a managed service is implemented, the product can continue to evolve without further cost to the region, and once the application is no longer required, the region can end the subscription without the burden of legacy software.

Appendix 1 - Architecture Strategies

There are many different architecture strategies that can be used for a managed service solution. Below is a brief discussion of two main categories, and the following appendixes outline three possible architecture strategies.

Stand Alone Implementation

A stand-alone implementation is a simple MSP strategy that can be used when the application does not require input from any other application within the health region. Typically with this type of system the application can be accessed over the Internet with user authentication, but without location restrictions.

Examples of applications that lend themselves to this type of architecture would be:

- Decision support applications
- Wait list applications
- Safety report applications
- E-Referral systems
- Basic logistics systems

Integrated Implementation

If the application requires integration in order to be effective, then there are additional components required within the architecture to ensure the security of the application and data.

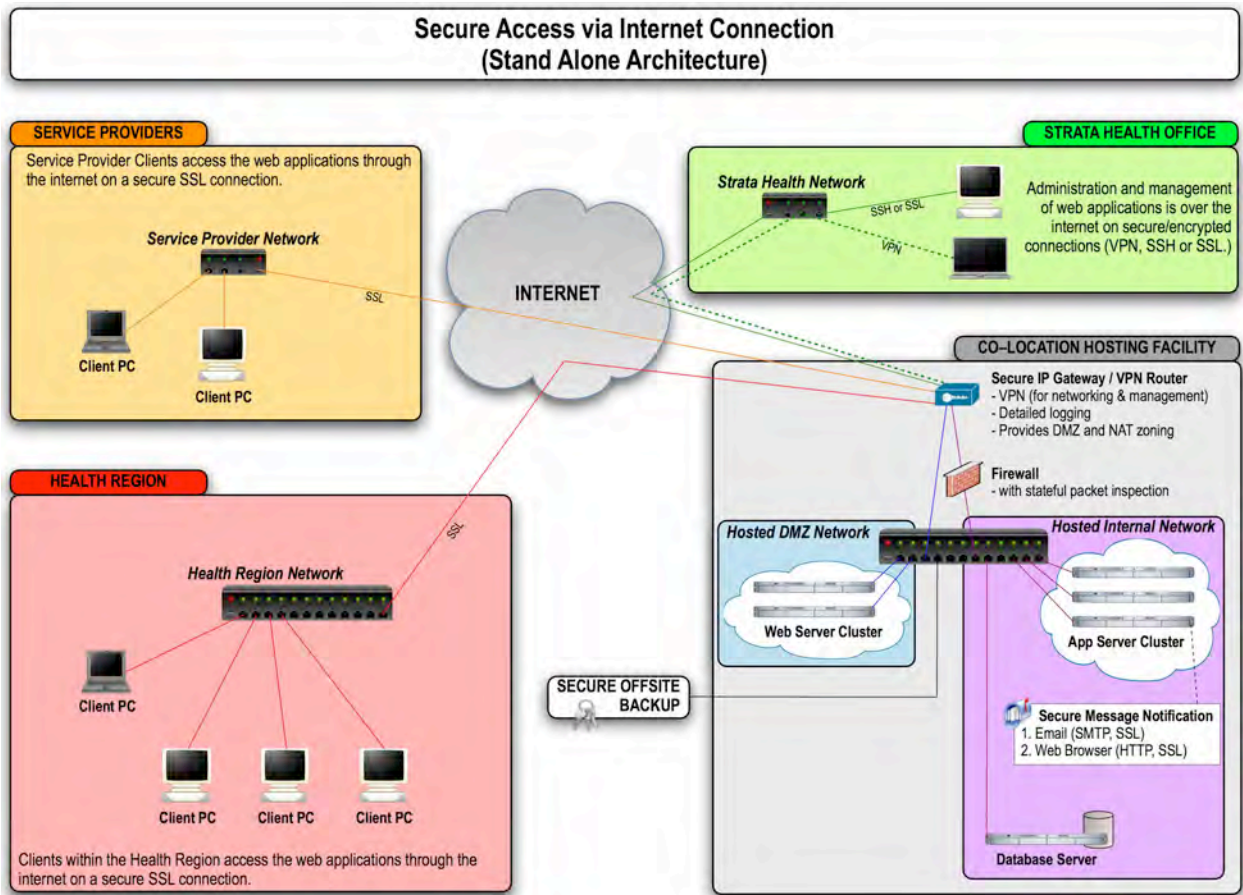
Examples of applications that lend themselves to this type of architecture would be:

- Work flow applications
- Simulation applications
- Contract management solutions
- Wait list applications
- Logistics systems

Appendices 2,3 and 4 outline three possible solutions for a managed service hosting strategy. Each solution has pros and cons. The optimal solution will differ depending on the requirements of the actual application and the health region.

Appendix 2 - Stand Alone Architecture

This is a suitable architecture if the application does not require integration for client demographics or medical information. There may be entry of patient information in this type of system, but typically any duplicate data entry would be limited. (Duplicate data entry refers to the entry of identical information into the managed service solution and an internal system) This type of architecture can be used as a stepping-stone if a project's timelines don't have integration scheduled until a second or third phase of the project.



These types of applications can still provide information for data warehousing by using a manual or automated data extraction and transformation. When performing the transformation, the following points should be kept in mind:

- Application performance
- Data analyst understanding
- Similarity with currently warehoused information

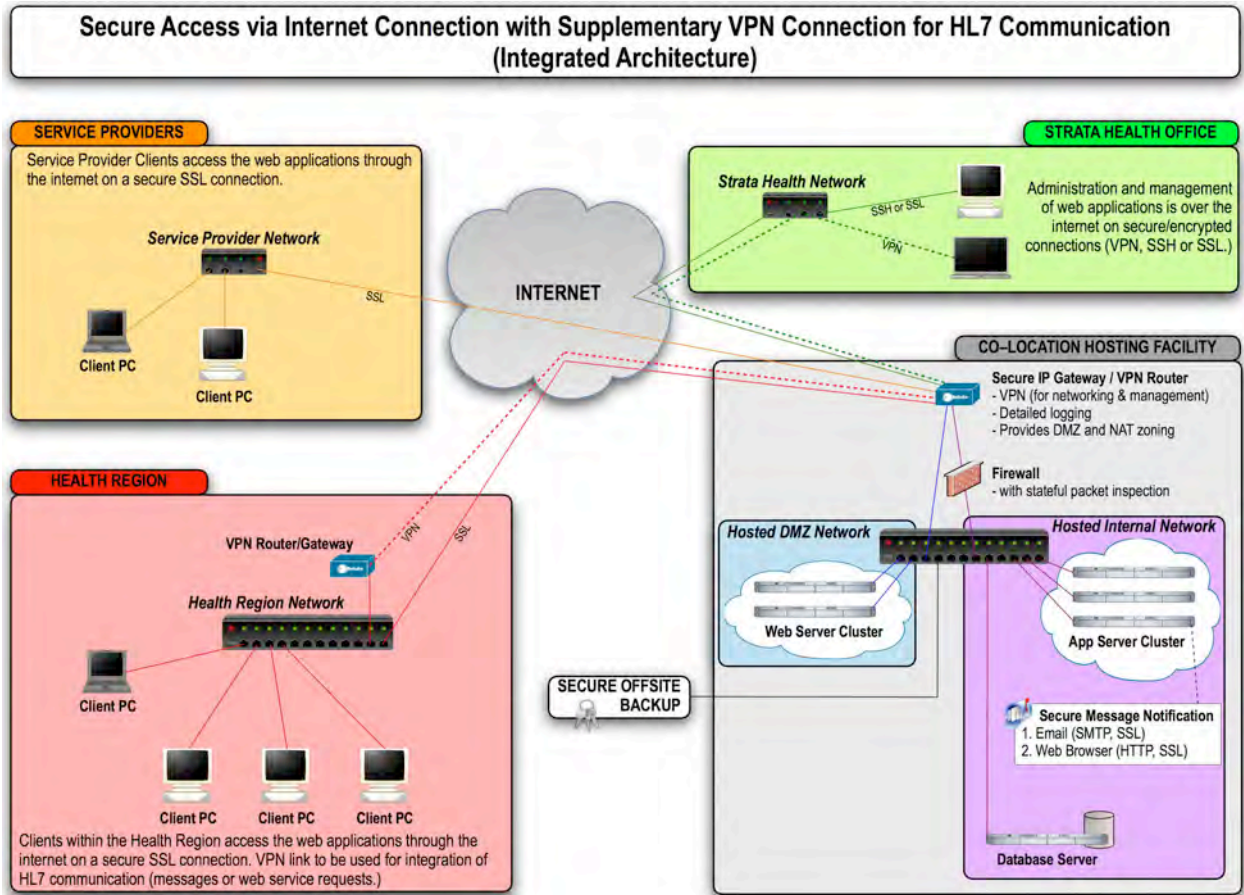
Usually this type of application can be accessed from anywhere on the Internet unless IP restrictions are placed on the firewall. The security risk for this type of application is minimal for the following reasons:

- Patient information in system is limited
- The application is not integrated with other systems

Appendix 3 - Integrated Architecture

This is the type of architecture is required if the application will be receiving an integration feed providing demographics or patient profile information from an internal system such as:

- EMPI (Electronic Master Patient Index)
- ADT (Admissions / Discharge Transfer System)
- CCIS (Community Computer Information System)

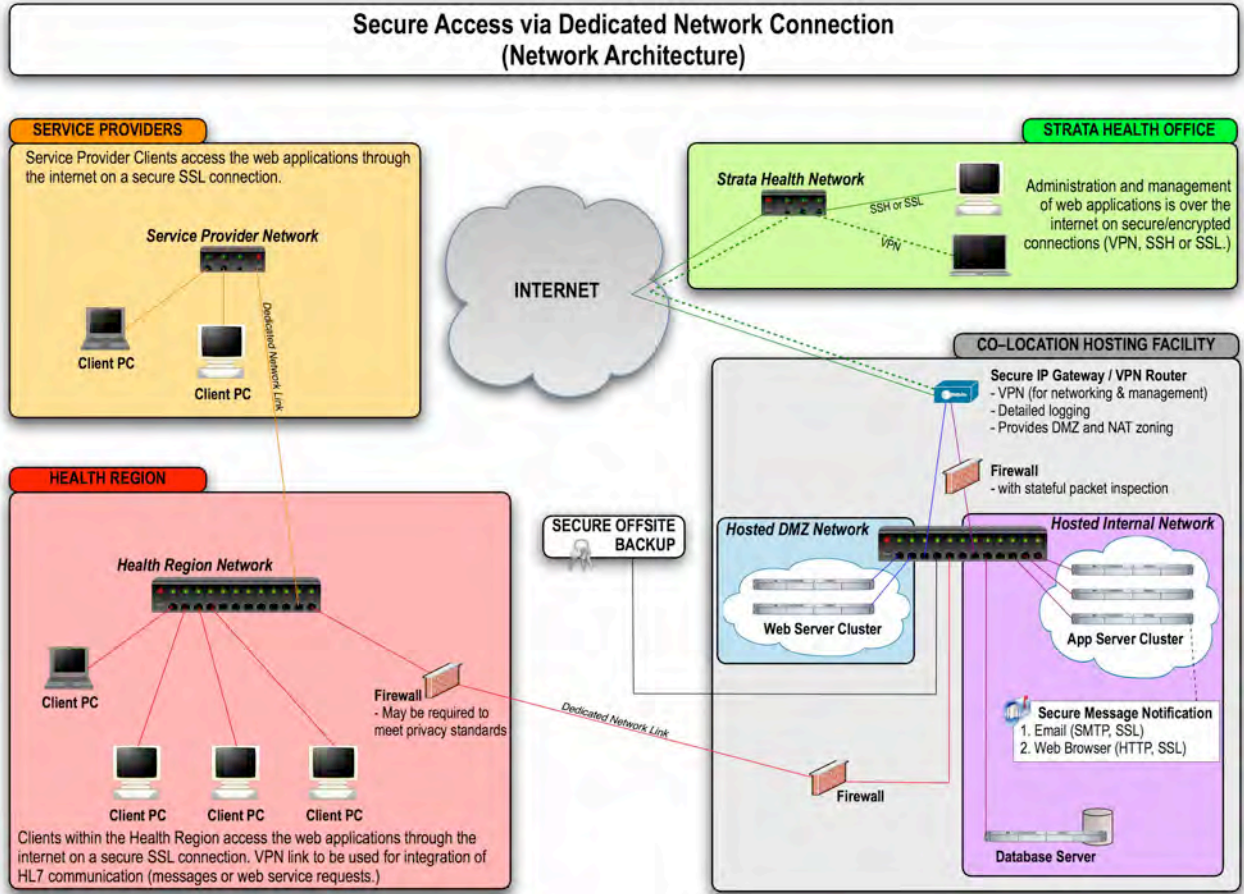


A secure VPN tunnel is created from the health region's internal network to the managed service environment. The integration messages can be sent using this secure tunnel as a secure delivery method.

Access to the application can be limited to users within the health region's internal network, or provided to vendors outside the region's internal network.

Appendix 4 - Network Connection Architecture

In this scenario, a physical connection from the health region's internal network to the managed service environment is created. This is most economical in situations where the health region's internal network has an existing connection in the physical location of the managed services hosting center. An example of this scenario is where a Tier 1 facility may be hosting a health region's network, while at the same time providing hosting space for private vendors. The integration messages can be sent to the MSP application on the health region's internal network.



Access to the application can be limited to users within the health region's internal network, or provided to vendors outside the regions internal network.

References

Standards Organizations

Health Level 7 (HL7)

www.hl7.org

Clinical Context Object Workgroup (CCOW)

<http://www.hl7.org.au/CCOW.htm>

Integrating the Health Care Enterprise (IHE)

<http://www.ihe.net>

<http://www.ihe-canada.com>

Canadian Institute For Health Information

<http://www.cihi.ca>

http://secure.cihi.ca/cihiweb/dispPage.jsp?cw_page=infostand_e

International Organization For Standardization (ISO)

<http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html>

Health Information Standards Committee For Alberta (HISCA)

<http://www.health.gov.ab.ca/about/hisca/index.htm>

Integration Vendors

Sentillion

<http://www.sentillion.com>

Interfaceware

<http://interfaceware.com/>

Orion

<http://www.orionhealth.com>

SeeBeyond

<http://www.seebeyond.com>

Managed Service Software Providers In the Health Care Industry

Strata Health Solutions Inc.

<http://www.stratahealth.com>