cliniconex

Privacy Impact Assessment

Prepared By
Valencia IIP Advisors Limited

VALENCIA
INFORMATION & INFRASTRUCTURE PROTECTION

July 2016

ABOUT THE ASSESSOR

Based in Ottawa and Toronto, **Valencia IIP Advisors Limited** ("Valencia") integrates three distinct yet related practices in the fields of privacy, information & infrastructure security and information technology strategy. Over the past 15 years, the principals of the company have carried out an extensive number of privacy, security and technology consulting engagements for public, private and health sector clients.

Valencia's philosophy is to provide our clients with the best possible strategic and operational advice based on thorough research and analysis. Further information about Valencia can be found at www.valencia.global.

This report was written by **Michael Power**, Valencia's Managing Director, Privacy. His practice involves providing strategic and operational advice to private and public sector clients on issues related to governance, technology, privacy and information security.

Michael Power has written extensively on privacy and information security issues. He is the author of *The Law of Privacy* (2013) as well as the Access to Information and Privacy Title of *Halsbury's Laws of Canada* (2005, 2011 and 2016 editions*)*. He is also the co-author of the American Bar Association's *Sailing in Dangerous Waters: A Director's Guide to Data Governance* (2004).

Michael Power is a member of the Law Society of Upper Canada and the Nova Scotia Barristers' Society. He is a member of the Canadian Bar Association, American Bar Association, Canadian Association of Management Consultants and the International Association of Privacy Professionals. He also serves an adjunct professor at Osgoode Hall Law School.

July 2016

Table of Contents

INDEX OF TABLES

INDEX OF FIGURES

TABLE OF ACRONYMS

The following acronyms appear in this document:

Acronym	Term
AES	Advanced Encryption Standard
API	Application Programming Interface
AWS	Amazon Web Services
EMR	Electronic Medical Record
HIC	Health Information Custodian
IMA	Information Manager Agreement
PaaS	Platform as a Service
PHIPA	Personal Health Information Protection Act, 2004 (Ontario)
PIA	Privacy Impact Assessment
PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
SaaS	Software-as-a-Service
TLS	Transport Layer Security

Table 1: Acronyms

EXECUTIVE SUMMARY

Cliniconex Inc. ("Cliniconex") provides solutions that focus on workflow related to communications for family and specialty clinics. One of the company's solutions is an automated appointment reminder service/patient communication service that uses voice, email and text to inform patients of upcoming medical appointments.

This report is a Privacy Impact Assessment ("PIA") and is intended to better inform potential clients, especially risk managers, of the privacy-related aspects of Cliniconex's automated patient communication service

It is to be noted that this report is not an audit of the privacy and security measures implemented by Cliniconex. Reliance is placed on the information, materials and responses provided by Cliniconex, which have not been verified as to the actual operation of the controls in place.

For the Family and Specialty clinics that use the Cliniconex patient reminder service, privacy risks generally revolve around:

- Unauthorized use of information by authorized users;
- Unauthorized collection/use or disclosure of information by external parties;
- Unauthorized or inappropriate collection/use or disclosure by a contractor, service provider or partner organization;
- Loss, destruction or loss of use of information;
- Loss of integrity of information;
- "Function creep" or changes in use and/or disclosure; or
- Non-compliance with legislative requirements (e.g. accuracy, access or correction).

In the use of any cloud-based service provider, while security and residency of personal information collected by the customer is entrusted to the service provider - in this instance Cliniconex - the majority of privacy-related responsibilities remain with the customer. Therefore, customers must ensure their information governance frameworks are mature enough to meet their own responsibilities with respect to personal information.

The nature of the personal information in question may not be considered by some to be particularly sensitive – name, mobile/home telephone number/email address/appointment information but the context of the appointment (with whom, for example, or where) could be sensitive personal information.

Clients concerned with data residency (the location where customer personal information will be processed) need to be expressly addressed. Whether processed by Cliniconex's hosted Cloud Controller, or sent via a third party service provider (e.g. Twilio), personal information will be processed outside of Canada. It is not problematic **if** express, informed consent is obtained from patients. This makes the issue more of a communications and business process issue.

Cliniconex does not have a mature privacy and security framework at this time. Beyond the security of the PaaS and SaaS service providers themselves, the security of Cliniconex's own code and application software is not fully known and a security assessment should be performed or, at a minimum, a security architect should be consulted as to the existence of vulnerabilities in design and deployment.

To their credit, the company's management recognizes these facts. As a first step, management is considering a series of privacy and security-related policies/procedures to better document and define its privacy and security posture. But even with the adoption of these policies, audit controls will need to be instituted to ensure adherence to them.

Furthermore, the corporate privacy policy should be revised and updated to address both access to personal information procedures as well as data residency. The audience for the document should be both customers and their patients and the full privacy policy should also be made generally available through the company website.

In terms of specific suggestions following review of the information provided, it is recommended that:

No.	Recommendation	Comment
1.	Arrange for a formal security assessment of the solution as well as review by a security architect.	No formal security assessment of the product has ever been conducted. The assessment should include penetration testing, security code review, and data loss prevention testing.
2.	Revise business processes so as to: • Contractually oblige customers to obtain an express consent; • Revise the Cliniconex Privacy Policy to meet notification requirements found in Canadian legislation; • Provide a written explanation as to how the personal information is processed outside of Canada	Personal information is processed outside of Canada. Legislation exists to prohibit such transfer of personal information unless legal exceptions apply. One exception is the express consent of the subject individual. To remove data residency as an issue, Cliniconex should facilitate customers obtaining express consent.

No.	Recommendation	Comment
	(e.g. the nature and extent) for use in seeking patient consent; and • Provide a patient consent form for use by customers.	
3.	Update the Cliniconex privacy policy to include information to both patients and clinics as to the company's information management practices (e.g. access to personal information, data residency) and provide a link to its Privacy Policy on its website. Publish a more fulsome public statement aimed at both customers and their patients as to the company's privacy and security measures as well as how it satisfies data residency requirements (i.e. through patient consent).	Organizations are expected to be open about their policies and practices with respect to the management of personal information. Generally, compliance with the openness principle is a client responsibility. In terms of Cliniconex providing such information to customers and patients, it does not do so except for one reference to an email address in its Privacy Policy. No further comment.
4.	Adopt a standard form information manager agreement or append a privacy/security annex to its service agreement. Revise company statements and agreements to indicate that personal information will not be disclosed unless the customer directs or "as required by law".	Cliniconex has entered into "information manager agreements" or "privacy/security" agreements on an *ad hoc* basis. It will need to do so if operating in Ontario and a number of other provinces. The company would be better served using its own template. Cliniconex indicates that will not disclose client data outside of the company or its affiliates except as the customer directs. This obligation is not technically correct and should be revised
5.	Establish controls to ensure adherence to policies and an audit procedure to ensure that controls are effective.	In seeking to mature its privacy and security management systems, the company is currently formalizing a number of information management and IT policies/procedures. The effectiveness of these efforts should be supported by specific control.
6.	Establish a simple access to personal information process and revise its privacy policy as to indicate the respective roles and responsibilities	The process can be simple given the current size of the company

No.	Recommendation	Comment
	of the company and customers vis-a-vis access to personal information.	
7.	Implement a privacy training and awareness program for Cliniconex staff.	Queries as to the existence of a company training program will likely be raised by customers. The program should focus on company privacy, security and incident management procedures as well as an introduction to legal privacy requirements.
8.	Establish a formal record retention schedule.	While record retention for personal information is not extensive given the solution in question, no formal record retention schedule has been created. A draft record retention policy is under consideration.
9.	Making the Company's full Privacy Policy publicly available through its website.	A short statement on privacy is located in the "About" section of the company website. This should be replaced with a link to the full corporate privacy policy.
10.	Formally adopt an access control policy for employees.	Current practices reflect the size of the company. Practices should be documented

PART 1: CONTEXT OF ASSESSMENT

A. INTRODUCTION

Cliniconex Inc. ("Cliniconex") provides solutions that focus on workflow related to communications for family and specialty clinics. One of the company's solutions is an automated appointment reminder service/patient communication service that uses voice, email and text to inform patients of upcoming medical appointments. The company was founded in 2009 and is based in Ottawa, Canada.

This report is a Privacy Impact Assessment ("PIA") and is intended to better inform potential clients, especially risk managers, of the privacy-related aspects of Cliniconex's automated patient communication service

A privacy impact assessment is an tool to evaluate the impact on privacy that results from a change to a system, environment, or process. Such change might take the form of a revised policy, a software upgrade, or the introduction of new technology, such as cloud services. A PIA is conducted by considering the system, environment or process in the context of privacy principles, best practices, codes of conduct, legislation and directives. This type of assessment is intended to inform relevant stakeholders and decision-makers on privacy considerations pertaining to the system, environment, process or program in question.

The objectives of a PIA can be described as to:

- Describe the privacy and security measures and controls associated with a particular project or initiative; and
- Assess the potential privacy risks and provide recommendations so as to mitigate those risks.

Cliniconex's service offering under consideration here is essentially a cloud-based service. The use of cloud services does not release potential client organizations from accountability for their custodianship of business and personal information.

In completing this report, the following activities were undertaken:

- Information gathering from materials provided by Cliniconex,
- Interpretation and documentation of Cliniconex components and associated services, for subsequent analysis and assessment,
- Review with Cliniconex of the solution descriptions, for accuracy and completeness prior to conducting a privacy analysis,
- Analysis of the Cliniconex service components and associated services in the context of compliance with chosen statutory authorities, relevant policies, and public expectations,
- Identification of privacy considerations and proposed mitigation strategies, and
- Review of outcomes with Cliniconex and other stakeholders.

Unless otherwise stated, this PIA reflects a review of documents provided by, and information exchanges with, Cliniconex staff in June/July 2016.

This assessment report considers all information associated with a client to be either business confidential or personal information, and assigns a high confidentiality and integrity value. This value assumes that any compromise or unauthorized disclosure of the information in question could cause social hardship, loss of privacy or serious harm to business operations or relationships.

B. SCOPE OF ASSESSMENT

The scope of this PIA is centred on the Cliniconex Patient Communication Service

The following table encapsulates particular domains that are within the scope of this report or excluded.

Domain	Within Scope	Out of Scope
Data transactions	• Personal information data flows between client and the Cliniconex service components.	• Anonymized or de-identified information about individuals associated with client. • Any information that is not personal

Domain	Within Scope	Out of Scope
	• Personal information storage within service data centers.	information, excluding identifying information of client personnel (e.g. employees/contractors) required to access and use the service.
Relevant Legislation	• *Personal Information Protection and Electronic Documents Act* (Canada) and associated regulations • *Personal Health Information Protection Act, 2004 (Ontario)* • Legislation within Canada that specifically address data residency.	• Legislation that does not specifically address protection of personal information related to the family or specialty clinic use of the appointment reminder service.
Privacy Posture	• Cliniconex privacy posture as it relates to provision of cloud services, compliance with applicable legislation and compliance with service agreements.	• Family or specialty clinic privacy posture as it relates to compliance with the applicable personal information protection legislation (e.g. PIPEDA, PHIPA).
Security Posture	• Cliniconex security posture as it relates to data flows and services.	• Family or specialty clinic security posture as it relates to physical, procedural and technical security measures.
Technology and Environment	• Cliniconex appointment reminder service offering	• Infrastructure and back office services of any family or specialty clinic that uses the appointment reminder service.

Table 2: PIA Report Scope

This report is not an audit of the privacy and security measures described in this document and implemented by Cliniconex Inc. Reliance is placed on the information, materials and responses provided by Cliniconex, which have not been verified as to the actual operation of the controls in place. Unless otherwise indicated, the views and statements expressed in this assessment are those of Valencia IIP Advisors Limited and not Cliniconex.

[Remainder of page left intentionally blank]

PART 2: SOLUTION DESCRIPTION

A. SOLUTION OVERVIEW

Cliniconex is an automatic cloud-based service allowing healthcare providers the ability to communicate with patients. The principal purpose is to provide appointment reminders but the service can be used for other purposes. including booking notifications, reminders, cancellations, surveys, and preventative care reminders.

The appointment reminder service is offered as a software service ("SaaS") - the solution is 100% automated and operates in the background 24/7 with no manual involvement required.

It is important to note that Cliniconex accesses only information needed to remind the patient of their appointment. This information uses patient demographic information from the EMR chart of the Family or Specialty clinic (the "Clinic") using the information provided by the referring physician as well as the details of the appointment that has been scheduled and agreed to by the patient.

Cliniconex installs an **On Premise Controller** - locally installed application that runs at the Clinic site. A significant aspect of this controller is that it is "stateless"[1], and does not retain data. The On Premise Controller connects to the clinic's electronic medical record ("EMR") using the EMR's own application programming interface ("API"), and caches required information for processing and encrypted transmission to Cliniconex's **Contact Memory Cache Servers** and **Cloud Controller**.

Patient details are sent to a cloud-based **Contact Memory Cache** Server, located in a DigitalOcean data center located in Toronto and a random token is created that serves as the Reference ID for the contact details. The EMR API uses Transport Layer Security ("TLS") with 128-bit Advanced Encryption Standard ("AES") algorithm in sending the information to the Contact Memory Cache Server.

Contact Memory Cache servers are specialized servers with no persistent storage, storing data solely in volatile memory. The contact memory caches delete data older than 30 days daily, by default. (A configuration change can reduce this to a shorter interval.) Appointment information is rendered permanently de-identified. This non-identifiable data is kept for statistical, billing and evaluation purposes.

As the name suggests, the data elements in the Contact Memory Cache ("memcache servers") concern patient contact information:

- "guid" (unique id for mapping later on in the reminder)

[1] "Stateful" and "stateless" are concepts to describe whether a device or program is to remember events in interactions. "Stateful" means that the tracking of interactions, usually by setting values in a field designated for that purpose, occurs. Stateless means there is no record of previous interactions and each interaction request has to be processed based entirely on information that comes with that request.

- patient first
- patient last
- patient cell/home/business
- patient email

The memcache servers are hosted separately from the Cloud Controller application (each using different cloud providers). Data in the memory cache does not include appointment information.

As noted, these cache servers are located in a data center operated by DigitalOcean and located in Toronto. The content memory cache servers in turn return to the local controller a random numeric identifier. This random identifier serves as the reference index for retrieval of contact details in future steps. The connection between all components of the system use SSL.

The patient contact information consists of either a telephone number for phone or SMS messages or an email address for mail messages.

Cliniconex pulls the patient contact information each day to send daily reminders (i.e. information is pulled today for only reminders to be sent today).

The appointment details and the Reference ID are sent to the Cliniconex Cloud Controller. The On-Premise Controller communicates with the Cloud Controller, but the reverse does not occur (i.e. the on-premises controller is not accessible from the cloud controller). The On Premise Controller only sends the reminders to the Cloud, and polls the cloud for updates to its configuration.

The following information is transmitted to the Cloud Controller:

- appointment type,
- appointment date,
- appointment status,
- appointment start and end time,

At this point the Toronto-based Memory Cache server contains personal information which is associated with a random identifier. This data is not stored on disk. It only resides in the memory of the running process. The Cloud Controller, located on servers in the United States has reminder information associated with the random identifier. With the exception of the appointment data - which is obfuscated (see below) and the random identifier, the data in the Cloud Controller is also not ‘stored’ on disk, rather it resides temporarily in volatile memcache for the purpose of constructing the eventual reminder.

The Reference ID index is deleted from the Cloud Controller after 30 days. The system can be configured to delete it from volatile memory right after the appointment reminder has been delivered to the patient.

If a patient requests the information used for reminders be updated or corrected, it is done directly in the EMR chart. If a patient does not want to be contacted by the appointment reminder system, they notify the clinic; the patient's record is then modified in the EMR (through the placement of a preference code in the patient's contact information) and the information is no longer provided to the Cliniconex.

Appointment details and the Reference ID for patient details are sent from the On Premises Controller to the **Cloud Controller**. The Cliniconex Cloud Controller begins the appointment reminder by assembling contact details from the Contact Memory Cache Server using the reference ID received from the local controller.

The information returned to the Cloud Controller is not stored on disk. It resides in memory in the process controller for the purposes of assembling the message and is deleted after the message is delivered successfully to the patient. These requests are transmitted over an encrypted SSL tunnel to the telecom or email service (Twilio or SendGrid). Patient details are permanently obfuscated when stored with the reminder in the cloud controller persistence, kept for the purposes of reporting to the clinic.

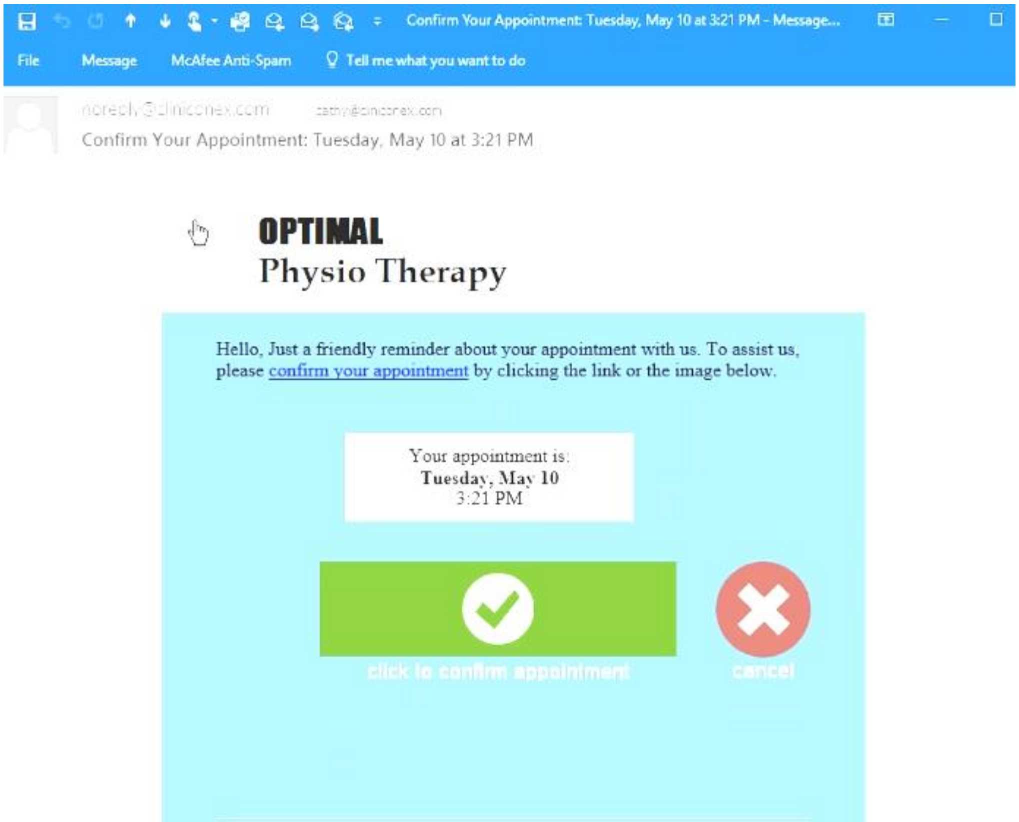
Aspects of the Cliniconex service uses third party service providers in the delivery of the communication service:

- The Cliniconex Cloud Controller uses Google's Cloud Platform.
- The Contact Memory Caches and Call Content Servers use Amazon Web Services and DigitalOcean platforms.
- Email Send Service is provided through Amazon Web Services and SendGrid
- Telephone/Text Service is provided through Twilio Inc., which using Amazon web services for telephony infrastructure and connectivity between HTTP and the public switched telephone network (PSTN) through Twilio's APIs.

Services are contracted for using the standard form service agreements provided by these suppliers.

The Reference ID index effectively de-identifies appointment details stored in the Cliniconex Cloud Controller. The reference index is deleted from the reminder application after 30 days. After no more than 180 days, the reference index data is permanently deleted or rendered unrecoverable (such as from backups).

In the case of an email reminder, the template is assembled, including all template customizations, such as the patient first or last name, if used. An email reminder is then sent via an email service provider (Sendgrid). Responses to the email reminder is registered by the Cloud Controller and ultimately updated to the EMR.



Confirm Your Appointment: Tuesday, May 10 at 3:21 PM - Message...

noreply@cliniconex.com cathy@cliniconex.com

Confirm Your Appointment: Tuesday, May 10 at 3:21 PM

OPTIMAL
Physio Therapy

Hello, Just a friendly reminder about your appointment with us. To assist us, please confirm your appointment by clicking the link or the image below.

Your appointment is:
Tuesday, May 10
3:21 PM

Figure 1: Mail Message Received by Patient

In the case of Voice or SMS reminders, the content of the reminder, including all template customizations is assembled. This compilation is sent to Call Content Servers but does not include the phone number. The Call Content server returns back to the Cloud Controller a unique message URL. This information is never 'stored' on disk. Rather it is stored temporarily in memory for the purpose of assembling and delivering the reminder.

The Cloud Controller initiates a voice or SMS reminder to a telephone number, via a telecom service provider (Twilio). It sends a secure message to Twilio referencing the message URL and the telephone number to call. Twilio then retrieves the message URL (which contains the MP3 with voice instructions) and delivers the call to the patient. Responses to the voice or SMS reminder are registered by the Cloud Controller and ultimately updated to the EMR.

The Cloud Controller runs on Google servers. The North American region of Google's Cloud Platform are physically located in the United States. No Google servers are located in Canada.

The Memory Cache and Call Content servers runs on Amazon Web Services ("AWS") servers. The AWS Cloud infrastructure is built around Regions and Availability Zones. A Region is a physical location in the world where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities. The AWS Cloud operates 35 Availability Zones within 13 geographic Regions around the world. None of these are in Canada although AWS has announced a future region based in Montreal within the next year.

The local controller pushes data to other parts of the Cliniconex system. There is never a case where other parts of the system push data into the local controller. In addition, the local Cliniconex system pulls data from the EMR and it only writes back to the EMR with appointment status.

Each day the Clinic's administrator receives an email report from Cliniconex that lists the previous day's calls made to patient for reference and auditing purposes. This table includes the following information:

- Provider's name
- Appointment identification (a six digit unique identifier)
- Result
- Phone number (with two of the digits blanked out)
- Date of appointment
- Reminder type
- Patient identifier (a five digit unique identifier)
- Attempts

Patient details are obfuscated when stored with the reminder in the Cloud Controller persistence. They are kept for the purposes of providing a report to the Clinic. Such reports will typically say a patient name was S#### J#####S, so that enough is there for a clinic to cross-reference with the appointment. The obfuscation level is customizable up to and including 100% (i.e. ##### #######). The obfuscation occurs at the database level (i.e. it is not just obfuscated for display; it is also stored in an obfuscated state in the database).

B. SECURITY

Effective security requires a holistic approach and this is accomplished through attention to the physical, logical, network and operational aspects of the service.

To support its business activities, Cliniconex proposes to adopt a "Security and Privacy Policy". The document is general in nature and would greatly benefit from being divided into two separate documents. Control activities to support the Security Policy should also be considered and governance workflows should be documented. For example, filing an exception when the policy cannot be met or creating and managing issues when gaps are identified between control activities and requirements.

1. Access

Only the Customer/Partner/Cliniconex admin can change the password only for a user. There is no current ability for users to change their own without talking to an admin.

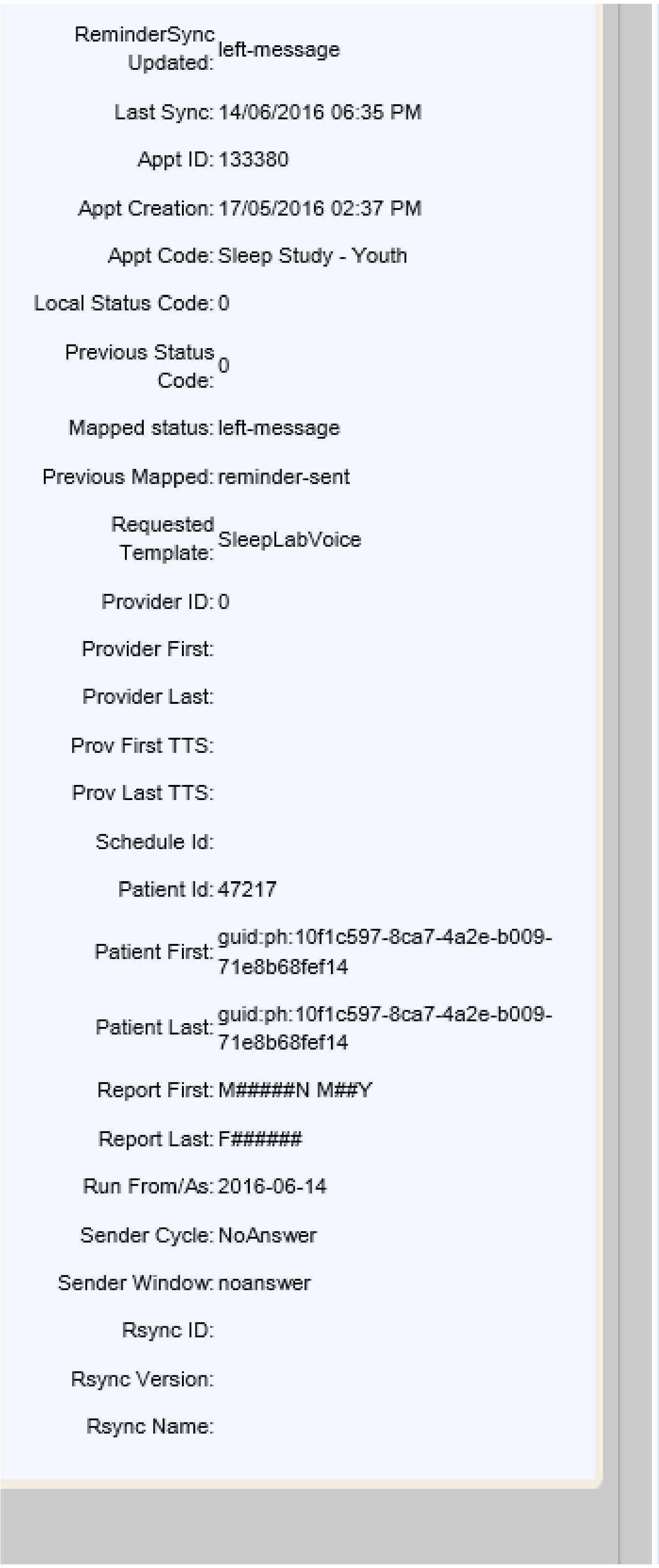
What does Cliniconex do with unnecessary accounts (e.g. when an employee leaves, changes groups, or does not use the account prior to its expiration).

The company's Chief Technology Officer currently monitors and manages accounts. The company has only 8 employees and has never had an employee leave or change positions. The company is currently preparing a policy concerning account management.

2. Support

Cliniconex personnel do not have access to personal information. Below is a screen shot of what a Cliniconex administrator would see in terms of personal information.

[Remainder of page left intentionally blank]



ReminderSync Updated:	left-message
Last Sync:	14/06/2016 06:35 PM
Appt ID:	133380
Appt Creation:	17/05/2016 02:37 PM
Appt Code:	Sleep Study - Youth
Local Status Code:	0
Previous Status Code:	0
Mapped status:	left-message
Previous Mapped:	reminder-sent
Requested Template:	SleepLabVoice
Provider ID:	0
Provider First:	
Provider Last:	
Prov First TTS:	
Prov Last TTS:	
Schedule Id:	
Patient Id:	47217
Patient First:	guid:ph:10f1c597-8ca7-4a2e-b009-71e8b68fef14
Patient Last:	guid:ph:10f1c597-8ca7-4a2e-b009-71e8b68fef14
Report First:	M#####N M##Y
Report Last:	F#######
Run From/As:	2016-06-14
Sender Cycle:	NoAnswer
Sender Window:	noanswer
Rsync ID:	
Rsync Version:	
Rsync Name:	

Figure 2: Data Elements Viewed by Cliniconex Admins

3. Safeguards

The safeguards described below reflect information provided by Cliniconex or publicly available information. No formal security assessments have been performed: no threat-risk assessment, no vulnerability assessments and no penetration testing.

I. Physical Security

Cliniconex uses DigitalOcean's Canadian data center located in Toronto for its memcashe servers. DigitalOcean's public statements concerning physical security indicate:

> *"Each site is staffed 24/7/365 with onsite security and to protect against unauthorized entry. Each site has security cameras that monitor both the facility premises as well as each area of the datacenter internally. There are biometric readers for access as well as at least two factor authentication to gain access to the building. Each facility is unmarked so as not to draw any additional attention from the outside and adheres to strict local and federal government standards."*

Google's Cloud Platform has extensive public statements concerning security, which can be found at: https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers.

As for physical security:

> *Google data centers feature a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. The data center floor features laser beam intrusion detection.*
>
> *Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are reviewed in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training.*

Amazon Web Services also provides a general public statement (white paper) about its security measures, which can be found at:
https://d0.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf
http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf

As for physical security, AWS states:

> "*AWS' data centers are state of the art, utilizing innovative architectural and engineering approaches. AWS has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional*

security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely."

II. Application Security

"Live" patient data is only used on the main application deployment. The company does not process patient data on any test/development/staging systems.

Cliniconex does not patch its applications but, instead installs new versions of the local or cloud applications as required. Updates to the clinic component (local controller) are relatively infrequent (in practice twice annually).

No specific application security development methodology nor are security requirements defined. The company indicates that it does some testing after patches to ensure tenant isolation. No information as to the testing was provided.

III. Encryption

When PHI/PI data is being transferred from EMR to Cliniconex and between the local controller and remote controller SLL (HTTPS) is being used to transport. The Cliniconex system uses standard based web encryption technologies and is currently compatible up to SSLv3 and TLS 2.o. The company indicates that it will phase out SSL as the end point client technology phases out (for example Internet Explorer 6 on Windows XP).

There is no encryption or obfuscation at rest. Data separation is used to protect the personal information processed within Cliniconex servers. Patient information and appointment details are separated until message assembly.

Cliniconex uses HTTPS protocol to secure client/server communication. Cryptographic keys are not managed, stored and distributed.

IV. Monitoring

The local controller has logs located within the clinic and the Cloud Controller has logs. Patient data is obfuscated in every log. In both the local agent and the Cloud Controller logging is done through standard java logging APIs (commons-logging and log4j). In the agent the logs are written to disk; in the Cloud Controller, the logs are written to the App Engine logging system and so are accessible through the Google cloud log viewer.

V. Network Security

At the interface with the public network, Cliniconex relies upon its PaaS and service providers for firewall, NAT, and IP filtering functions. Functions at this layer include denial of service blocking, intrusion detection systems, SSL, and initial access/certificate validation.

From publicly available information, the PaaS providers deploy a number of network security measures:

- Penetration testing;
- Network-level DDOS ("Distributed Denial-of-Service") detection and prevention;
- Network isolation;
- Virtual networks;
- Anti-virus and anti-malware protection;
- Anti-spam controls;
- Port scanning and remediation; and
- Perimeter vulnerability scanning.

VI. Backup & Recovery

The on-site local controller is stateless and therefore no local storage or backups are necessary. This system is merely used as a conduit to and from the Cloud Controller.

Data is not being backed up on different media types and it is not physically transported to remote locations.

Backups are not encrypted but any data stored (and backed up) does not contain any patient data (only appointment data).

VII. Change Management

Capacity planning relies on the ability and agility of the company's PaaS providers, in particular Google's Cloud platform.

There is no such change management plan at this time; nor is there any formal operational change control procedure. Change management is handled by and at the discretion of the Company's Chief Technology Officer ("CTO").

VIII. Incident Detection and Response

Customers are responsible for clinic activities. As for cloud-based components, the company relies upon the security measures of its' PaaS and SaaS providers.

4. Audit

There has been no formal audit (e.g. SOC 1, Type 1 or 2) of the application nor any certification (e.g. ISO/IEC 27001:2013; ISO/IEC 27001:2013) of the company's privacy and security postures.

C. AGREEMENTS

Introduction. A key component of the relationship between a service provider and clients is the service agreement. From a privacy perspective, such agreements should have provisions pertaining to the protection of personal information.

Ontario. In 2012, the Office of the Information and Privacy Commissioner of Ontario ("IPC") considered the use of service providers by government in a special investigation report, *"Reviewing the Licensing Automation System of the Ministry of Natural Resources"*[2]. The report was prepared in response to a complaint about the Ministry outsourcing the issuance of hunting and fishing licenses to an American company, with personal information being stored in the United States. The IPC considered that outsourcing was not problematic (especially with respect to the storage of personal information outside Canada) provided that reasonable contractual measures were taken to protect the data.

In this specific case, the IPC noted provisions in the agreement between the Ministry and the service provider/agent. This list of acceptable provisions is useful to consider since the IPC is responsible for enforcing PHIPA compliance. PIPEDA obligations also require reasonable contractual measures. The provisions pertained to:

- *Ownership* –The Ministry is to be the owner of all Ministry data.
- *Collection, Use and Disclosure* – Under the contract, the Agent cannot directly or indirectly use, collect or disclose any personal information for any purposes not authorized by the Ministry.
- *Confidential Information* –The Agent has specific contractual obligations to (i) keep the information confidential and secure; (ii) limit the disclosure of confidential information to only those who have a "need to know" and(iii) not to directly or indirectly disclose, destroy, exploit or use any confidential information (except for the purpose of the contract, or except if required by order of a court or tribunal), without the written consent of the Ministry.
- *Notice of Compelled Disclosure* – If legally compelled to disclose any of the Ministry's confidential information, the Agent must provide the Ministry with prompt notice to allow the Ministry to seek a protective order or other appropriate remedy to prevent or limit such disclosure.
- *Subcontracting* – The Agent is not permitted to subcontract the whole or any part of the contract without the prior written consent of the Ministry.
- *Security* – The Agent must ensure the security and integrity of all personal information and records in its possession and must implement, use and maintain the most appropriate products, tools, measures and procedures to do so.

[2] PC12-39 available at https://www.ipc.on.ca/images/Findings/2012-06-28-MNR_report.pdf

- *Retention and Destruction* – The Agent must return all confidential information to the Ministry before the end of the term of the contract, with no copy or portion kept by the Agent.
- *Audits* – The Agent is to comply with annual audits for privacy and security compliance for the duration of the contract.
- *Governing law* – The governing law of the contract is Ontario and the federal laws of Canada.

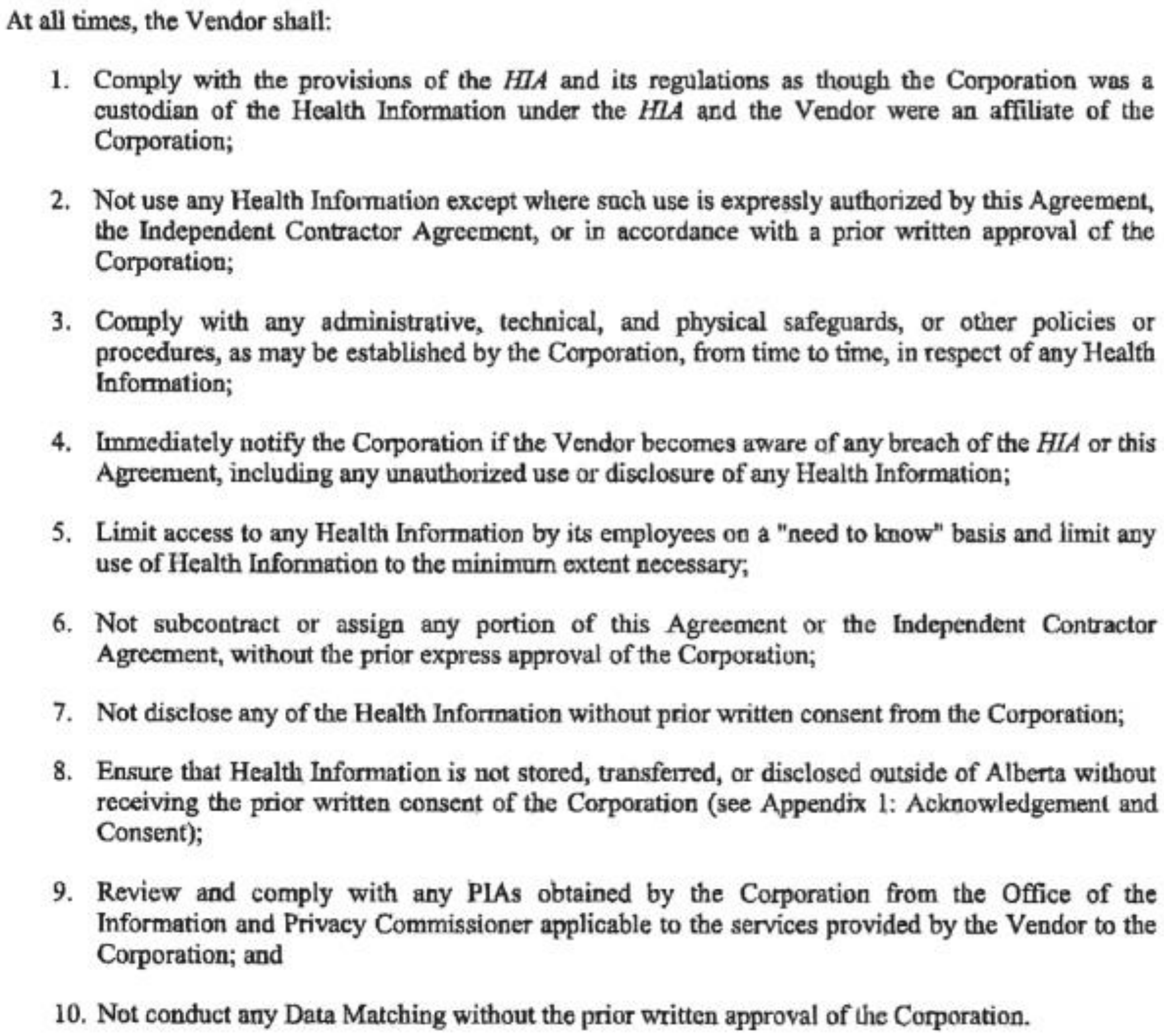
Cliniconex Agreement: General. "Customers" who purchase the service offering enter into a written agreement with Cliniconex. A copy of the "standard form" agreement was provided. The agreement is a license/subscription agreement containing terms one would normal expect in such agreements. Only one provision pertains to "account data":

> *4. Account Information and Data*
>
> *Cliniconex will abide by its Privacy Policy as published on its website; however Cliniconex does not own any Customer Data. Customer, not Cliniconex, shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, privacy protection, appropriateness, and intellectual property ownership or right to use of all Customer Data, and Cliniconex shall not be responsible or liable for the deletion, correction, destruction, damage, loss, misdirection, breach of privacy or failure to store any Customer Data. Cliniconex reserves the right to withhold, remove, and/or discard Customer Data, if any, without notice for any breach, including, without limitation, Customer's non-payment. Upon termination for cause, Cliniconex shall have no obligation to maintain or forward any Customer Data, if any.*

Cliniconex Agreement: Information Manager Agreement. Cliniconex does not have a standard form IMA or privacy/security-related agreement (or appendix to its service agreement). The company is prepared to enter them when requested to do so by clients but does not do so on a regular basis. The company has entered into at least at least one "Information Management Agreement" ("IMA") with a client in the Province of Alberta and one confidentiality agreement with a provider in Ontario. Cliniconex management indicates that this form of agreement is not generally used with all clients.

Article 2.2. of the Alberta agreement states:

[Remainder of page left intentionally blank]



At all times, the Vendor shall:

1. Comply with the provisions of the *HIA* and its regulations as though the Corporation was a custodian of the Health Information under the *HIA* and the Vendor were an affiliate of the Corporation;

2. Not use any Health Information except where such use is expressly authorized by this Agreement, the Independent Contractor Agreement, or in accordance with a prior written approval of the Corporation;

3. Comply with any administrative, technical, and physical safeguards, or other policies or procedures, as may be established by the Corporation, from time to time, in respect of any Health Information;

4. Immediately notify the Corporation if the Vendor becomes aware of any breach of the *HIA* or this Agreement, including any unauthorized use or disclosure of any Health Information;

5. Limit access to any Health Information by its employees on a "need to know" basis and limit any use of Health Information to the minimum extent necessary;

6. Not subcontract or assign any portion of this Agreement or the Independent Contractor Agreement, without the prior express approval of the Corporation;

7. Not disclose any of the Health Information without prior written consent from the Corporation;

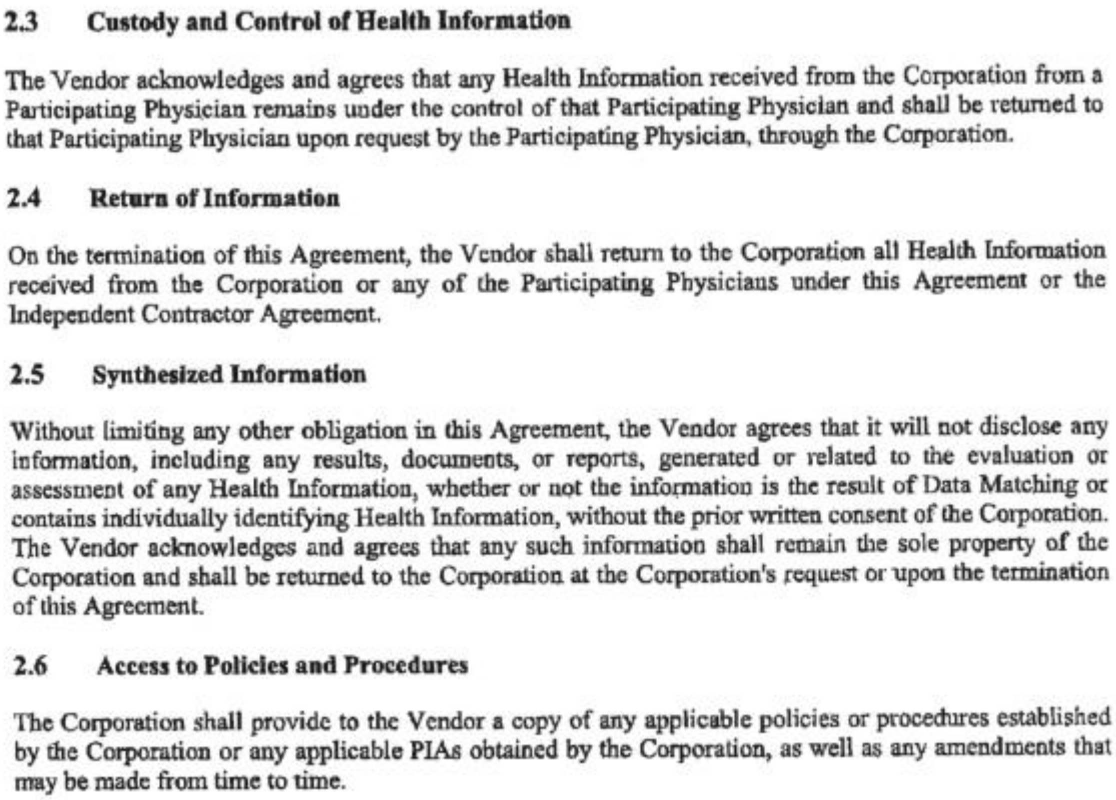
8. Ensure that Health Information is not stored, transferred, or disclosed outside of Alberta without receiving the prior written consent of the Corporation (see Appendix 1: Acknowledgement and Consent);

9. Review and comply with any PIAs obtained by the Corporation from the Office of the Information and Privacy Commissioner applicable to the services provided by the Vendor to the Corporation; and

10. Not conduct any Data Matching without the prior written approval of the Corporation.

Cliniconex as vendor further agrees to other personal information-related provisions:

[Remainder of page left intentionally blank]



2.3 Custody and Control of Health Information

The Vendor acknowledges and agrees that any Health Information received from the Corporation from a Participating Physician remains under the control of that Participating Physician and shall be returned to that Participating Physician upon request by the Participating Physician, through the Corporation.

2.4 Return of Information

On the termination of this Agreement, the Vendor shall return to the Corporation all Health Information received from the Corporation or any of the Participating Physicians under this Agreement or the Independent Contractor Agreement.

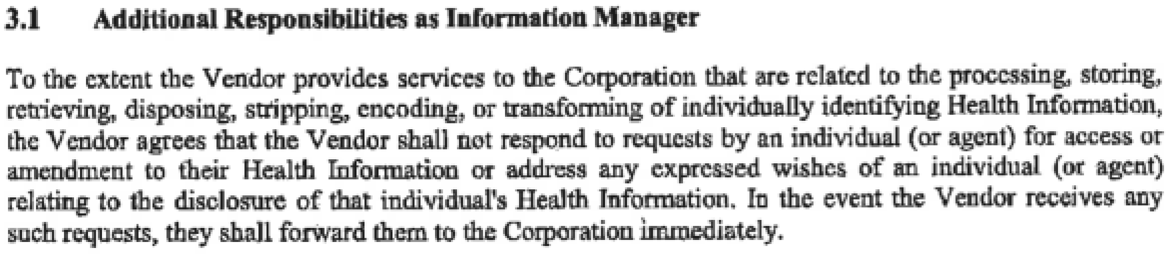
2.5 Synthesized Information

Without limiting any other obligation in this Agreement, the Vendor agrees that it will not disclose any information, including any results, documents, or reports, generated or related to the evaluation or assessment of any Health Information, whether or not the information is the result of Data Matching or contains individually identifying Health Information, without the prior written consent of the Corporation. The Vendor acknowledges and agrees that any such information shall remain the sole property of the Corporation and shall be returned to the Corporation at the Corporation's request or upon the termination of this Agreement.

2.6 Access to Policies and Procedures

The Corporation shall provide to the Vendor a copy of any applicable policies or procedures established by the Corporation or any applicable PIAs obtained by the Corporation, as well as any amendments that may be made from time to time.

Finally, Cliniconex agrees:

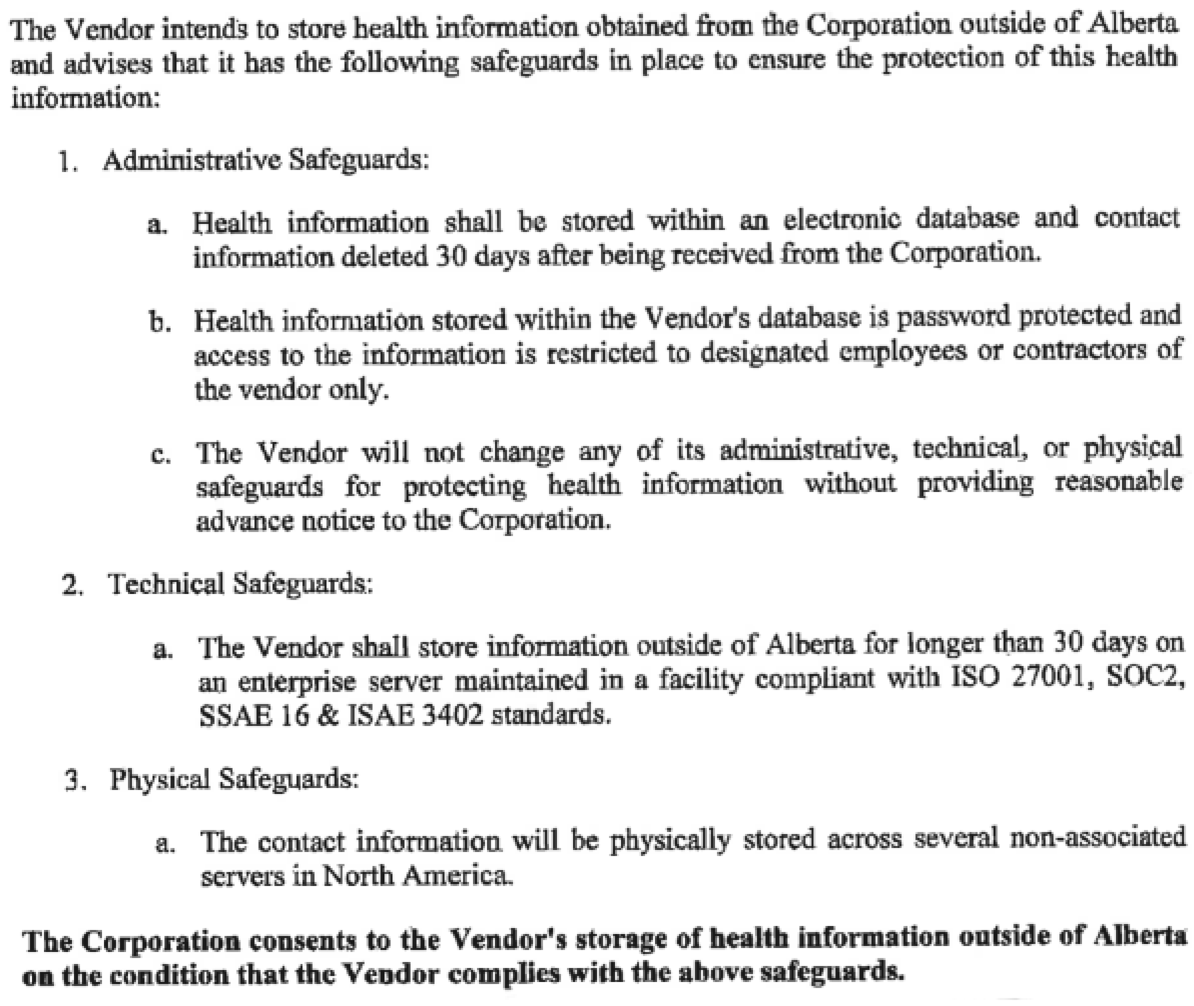


3.1 Additional Responsibilities as Information Manager

To the extent the Vendor provides services to the Corporation that are related to the processing, storing, retrieving, disposing, stripping, encoding, or transforming of individually identifying Health Information, the Vendor agrees that the Vendor shall not respond to requests by an individual (or agent) for access or amendment to their Health Information or address any expressed wishes of an individual (or agent) relating to the disclosure of that individual's Health Information. In the event the Vendor receives any such requests, they shall forward them to the Corporation immediately.

With respect to data residency, an Annex to the Agreement states:

[Remainder of page left intentionally blank]



The Vendor intends to store health information obtained from the Corporation outside of Alberta and advises that it has the following safeguards in place to ensure the protection of this health information:

1. Administrative Safeguards:

   a. Health information shall be stored within an electronic database and contact information deleted 30 days after being received from the Corporation.

   b. Health information stored within the Vendor's database is password protected and access to the information is restricted to designated employees or contractors of the vendor only.

   c. The Vendor will not change any of its administrative, technical, or physical safeguards for protecting health information without providing reasonable advance notice to the Corporation.

2. Technical Safeguards:

   a. The Vendor shall store information outside of Alberta for longer than 30 days on an enterprise server maintained in a facility compliant with ISO 27001, SOC2, SSAE 16 & ISAE 3402 standards.

3. Physical Safeguards:

   a. The contact information will be physically stored across several non-associated servers in North America.

The Corporation consents to the Vendor's storage of health information outside of Alberta on the condition that the Vendor complies with the above safeguards.

The Cliniconex service agreement does not fully address the subjects found in the IPC report. While the architecture of the Cliniconex solution may minimize the possibility of a data breach, compete “contracting out” of security measures is inconsistent with the accountability obligations of clients. The IMA does address many of the points that the IPC suggests be dealt with contractually between a custodian/owner and a service provider. Cliniconex should consider using a standard form information manager agreement or appending a privacy/security annex to its standard form agreement to fully address the topics enumerated in the IPC report.

Compliance with Laws. Cliniconex should state it will comply with all laws and regulations applicable to its provision of the appointment reminder service and that are applicable to information technology service providers, including security breach notification laws.

Conversely, customers should be required to comply with all laws and regulations applicable to its use of the appointment reminder service, including laws related to privacy, data protection and confidentiality of communications. ***Customers should responsible for implementing and maintaining privacy protections and security measures for components that the customer provides or controls***, and for determining whether the service are appropriate for storage and processing of information subject to any specific law or regulation. This is somewhat stated in clause 4 (general agreement) referred to above but it should be more clearly stated. Customers should also responsible for responding to any request from a third party regarding Customer's use of the service. The IMA does address this aspect in clause 3.1.

Use. Cliniconex's agreement should state that Customer Data (which should be defined) will be used only to provide the customer with the service, including purposes compatible with providing those services. This is done in Article 2(2) – 2 of the IMA. Cliniconex should further state that personnel will not process customer data without authorization from the customer. Finally, Cliniconex should indicate that it will not use customer data or derive information from it for any advertising or similar commercial purposes.

Ownership. Cliniconex does state that it acquires no rights in customer data (other than, implicitly, the rights granted to provide the Service. As between the parties, all right, title and interest in and to Customer Data should remain with the customer.

Law Enforcement Disclosure. Cliniconex, to the extent applicable, should state that it will disclose customer data to law enforcement unless required by law; it will attempt to redirect any law enforcement requests to the customer and, in doing so, may provide client's basic contact information to the law enforcement agency. If compelled to disclose customer data to law enforcement, Cliniconex should agree to use commercially reasonable efforts to notify the customer in advance of a disclosure and provide a copy of the demand, unless legally prohibited from doing so.

Other Disclosure. Cliniconex should also state that it will not disclose customer Data outside of the company, it's service providers or its controlled subsidiaries and affiliates except (1) as customer directs, or (2) as required by law. Upon receipt of any other third party request for Customer Data, Cliniconex should promptly notify Customer unless prohibited by law and reject the request unless required by law to comply. If the request is valid, Cliniconex should attempt to redirect the third party to request the data directly from Customer. The IMA does have a broad provision that prohibits disclosure without the clinic's consent but that will not be possible in law enforcement scenarios (should they ever occur) and Cliniconex may wish to replace the provision with one that is more accurate and descriptive.

Cliniconex should also state that it will not provide any third party: (a) direct, indirect, blanket or unfettered access to customer data other than customer's basic contact information to the third party.

Data Retention. Cliniconex does state in its promotional materials and in the IMA that customer information will be deleted after 30 days.

Data Residency. Cliniconex should state that data may be stored and/or processed outside of Canada and that the customer expressly agrees to such storage/processing and where consent is required, it is the express responsibility of the customer to obtain such consent**.**

Use of Subcontractors. The IMA does state that Cliniconex cannot subcontract without the consent of the clinic. Cliniconex should state may hire subcontractors to provide certain services on its behalf. The issue is not necessarily the use of subcontractors but rather their ability to access data and their location.

Appropriate Security. Cliniconex does state in the IMA it has implemented and will maintain and follow appropriate technical and organizational measures intended to protect customer data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.

Cliniconex Personnel. Cliniconex should expressly state that it's personnel are obligated to maintain the security and secrecy of any customer data and this obligation continues during and after their engagement ends. Cliniconex employees expressly sign Confidentiality and Non-Disclosure Undertakings.

Security Incident Notification. There is no express provision concerning security incident notification. Security incidents would be generally defined as unlawful access to any customer data stored on Cliniconex's equipment or in Google/AWS/DigitalOcean facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of client data).

Cliniconex should indicate that it will promptly:

(a) Notify the customer of the Security Incident,
(b) Investigate the security incident,
(c) Provide the customer with detailed information about the security incident, and
(d) Take reasonable steps to mitigate the effects and to minimize any damage resulting from the security incident.

[Remainder of page left intentionally blank.]

PART 3: PERSONAL INFORMATION

A. DATA FLOWS

Client access to the Cliniconex service begins at Internet-enabled locations and ends at a datacenter either operated by an "aggregation" PaaS provider to Cliniconex or a "delivery" SaaS service provider. The objective is to deliver healthcare-related appointment reminders to patients of the clinic's that subscribe to the service. The connections established between customers and datacenters are encrypted using Transport Layer Security (TLS) /Secure Sockets Layer (SSL).

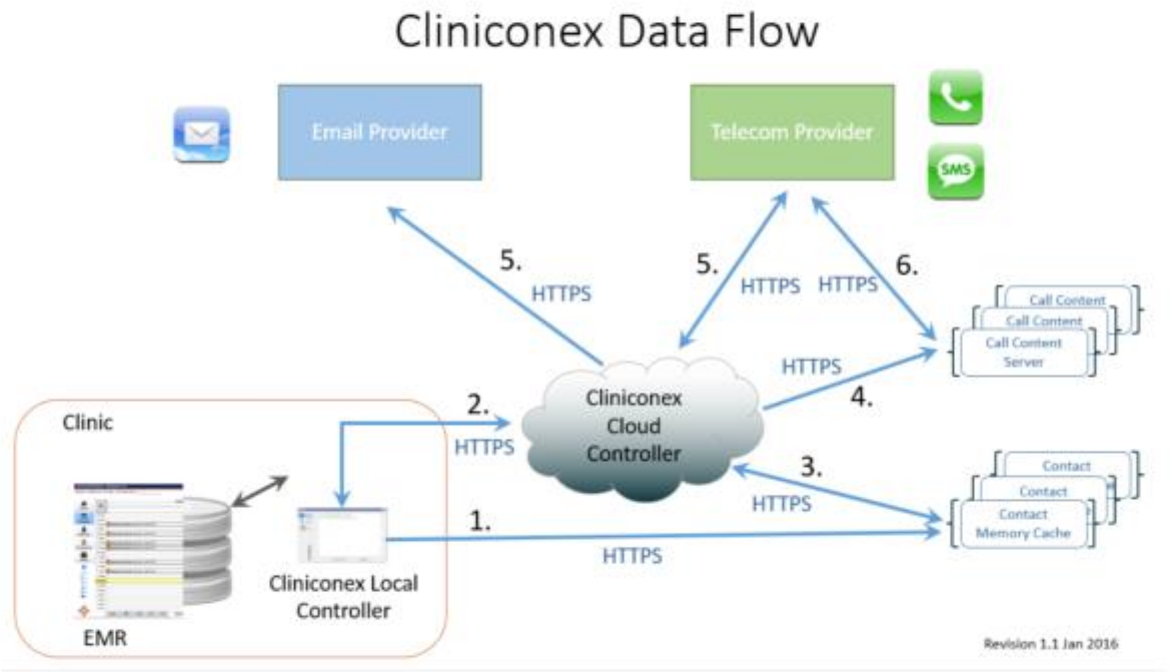


Figure 3: Cliniconex Data Flows

Overview of Data Flows

In Step 1, the patient information (e.g. name, phone, email …) are sent to the content memory cache. The content memory cache servers in turn return to the local controller random numeric identifier. This random identifier serves as the reference index for retrieval of contact details in future steps. The connection between all components of the system use SSL.

In Step 2, the appointment details (e.g. type, date, provider/clinic info…) and the random identifier (created in step 1) is sent to the Cliniconex Cloud Controller.

The Content cache server contains personal information which is associated with a random identifier. This data is not stored on disk. It only resides in the memory of the running process. The Cloud Controller (hosted on the Google Cloud platform) has reminder information associated with the random identifier. With the exception of the appointment data (which is obfuscated and the random identifier, the data in the cloud controller is also not 'stored' on disk, rather it resides temporarily in volatile "memcache" for the purpose of constructing the eventual reminder.

The reference index is deleted from the reminder application after 30 days and the system can be configured to delete it from volatile memory right after the appointment reminder has been delivered to the patient.

Reminder Message Assembly: Email and Text

In Step 3, the Cliniconex Cloud Controller begins assembling the appointment reminder by asking the content memory cache for the PI. It does this by requesting the PI associated with the Cliniconex random identifier. The content memory cache sends to the Cloud Controller the personal information for the appointment. That information is not stored on disk. It resides in memory in the process controller for the purposes of assembling the message and is deleted after the message is delivered successfully to the patient.

In the case of an email reminder (Step 5), the template is assembled, including all template customizations if used. In Step 5, an email reminder is initiated via Amazon Web Services (AWS). The same process applies for text message where the assembled message is sent to is Twilio's SMS service.

Responses to the email reminder is registered by the Cloud Controller

Reminder Message Assembly: Telephone

In Step 4, the content of the reminder is sent from the Cloud Controller to the call content server. The Call Content server returns back to the cloud controller a unique message URL. This information is not 'stored' on disk but is stored temporarily in memory for the purpose of assembling and delivering the reminder.

In Step 5, the Cloud Controller sends a secure message to Twilio referencing the message URL and the telephone number to call. Twilio retrieves the message URL (which contains the MP3) and delivers the call to the patient.

Responses to the voice or SMS reminder are registered by the Cloud Controller.

When this process is completed, the only details stored on disk are de-identified appointment details, not attached in any way to personal information. This is retained for billing and tracking purposes only. The retention period of this data is configurable but by default it is removed after each 30-day billing period.

The local controller, within the clinic’s EMR pushes data to other parts of the Cliniconex system. Other parts of the system do not push data into the local controller.

Data Flow Details

The appointment reminder service has the following information flows:

Data Flow 1

Description	Registration of Patient
Data Elements	2-3
Origin	Patient
Destination	Provider
Purpose	Initiate registration of patient in reminder service
Format and Protocol	Telephone call/e-mail/In-person
Safeguards	Unknown
Vulnerabilities	Unknown
Commentary	None

Data Flow 2

Description	Appointment Booking
Data Elements	1-6
Origin	Provider
Destination	Patient
Purpose	Communicate with Patient (e.g. appointment reminder)
Format and Protocol	Text message/telephone call/e-mail
Safeguards	SSL Encryption in Transit
Vulnerabilities	Unknown
Commentary	None

Data Flow 3

Description	Appointment Reminder Information/Other Communication
Data Elements	1-7
Origin	Provider
Destination	Cliniconex
Purpose	Facilitate sending of reminder or other information to Patient (e.g. appointment reminder)
Format and Protocol	HTTP over SSL
Safeguards	SSL Encryption in Transit
Vulnerabilities	Unknown
Commentary	None

Data Flow 4

Description	Appointment Reminder /Other Communication
Data Elements	1-7
Origin	Cliniconex
Destination	Patient
Purpose	Transmission of reminder or other information patient (e.g. appointment reminder)
Format and Protocol	Text message/telephone call/e-mail
Safeguards	Unknown
Vulnerabilities	Unknown
Commentary	None

[Remainder of page left intentionally blank]

B. DATA ELEMENTS WITHIN FLOWS

A significant component of a privacy assessment involves the identification of possible (or specific, where known) data elements, and their application to data flows between one place/system/person and another. Cliniconex holds 3 basic categories of data.

Data Category	Description
Service or System Data	"System or Service Data" is information about, and generated by, an information system or cloud service. System data is distinct from client-created content and is used solely for the purpose of providing, operating and maintaining the service, or diagnosing and/or troubleshooting in the event of problems or system outages. System data is stored both inside and outside of Canada and is accessible by authenticated Cliniconex administrators both inside and outside of Canada. Its use is controlled and limited to the provisioning, maintenance, support and ongoing operation of the Cliniconex service. System administrators and support service providers access this data.
Customer Contact Data	"Customer Contact Data" is information to identify and differentiate users of the service. This includes User ID, Organizational ID and basic user

	contact information (e.g. phone number or email address). This information is used to by Cliniconex staff in order to maintain customer relations, troubleshoot service issues. See Section C below for the attributes of this type of data.
Customer-Generated Content	Customer content consists of data/information used to assemble appointment reminders. Specific content will range in type, volume and sensitivity according to the client activities in using Cliniconex service.

Table 3: Personal Information Data Categories

As for specific data elements within the Cliniconex data flows, the following have been identified:

No.	Data Element	Details/Comments
1.	Appointment Date and Time	NA
2.	Patient Name (optional)	At provider's option, reading the patient's name can be disabled.
3.	Patient Contact	Home, work or mobile telephone number or email address
4.	Appointment Type	NA
5.	Provider name (optional)	At provider's option, reading the provider's name can be disabled.
6.	Office Identifier	Office identifier is a code indicating in which office the appointment is scheduled (used in multi-site clinics). This is not the clinic address.
7.	Appointment Status	Typical appointment statuses: Reminder Sent, Confirmed, Cancelled, Left Message, No Answer, Picked-up No-answer, Please Call. At the option of the clinic, writing the appointments status can be disabled.

Table 4: Personal Information Data Elements

[Remainder of page left intentionally blank]

PART 4: PRIVACY ANALYSIS

A. INTRODUCTION

Framework. A reasonable framework for a privacy analysis involves consideration of legal requirements for the protection of personal information together with a "principles" analysis based on general concepts of privacy. These legal requirements are enacted in legislation and are relevant because a clinic that proposes to use the Cliniconex service either operates in, or collects personal information from, one or more of jurisdictions, in which such legislation has been enacted.

Personal information protection laws in Canada may be considered as providing:

- Rules for the collection, use, disclosure and security of personal information;
- A general right of access to one's own personal information, subject to specified exceptions;
- A right to request correction or amendment of erroneous personal information;
- A process for the independent review of the decisions of personal information custodians; and
- Enforcement for contraventions of the legislation.

A number of different perspectives are considered in this Part. Data residency requirements in Canada will be examined as well as Privacy Commissioner guidance with respect to the use of service providers. This is followed by a mapping of how the potential use of the Cliniconex service meets the legislative requirements:

- Using Ontario's *Personal Health Information Protection Act* as illustrations; and
- Meeting private sector requirements under the federal *Personal Information Protection and Electronic Document Act*[3] ("PIPEDA").

B. DATA RESIDENCY

1. Introduction

Potential clients will invariably will ask Cliniconex about data residency of the personal information used in connection with the appointment reminder service. The reason for this is that several Canadian jurisdictions have enacted legislation that include provisions concerning the "location" or "residency" of personal information and its movement across international borders and provincial or territorial boundaries. These provisions generally concern security, storage, or access from, outside Canada are discussed below.

I. British Columbia

[3] SC 2000, c 5.

Legislation. British Columbia's *Freedom of Information and Protection of Privacy Act*[4], which covers public bodies including hospitals requires,

- Personal information, including information that is disclosed to service providers, in the custody or control of a public body must be stored and accessed only in Canada, unless specifically stated otherwise, and
- Public bodies and service providers to report to the Minister any non-Canadian demand for the disclosure of personal information not authorized under the statute.

The legislation also:

- Limited the purposes for which a public body may disclose personal information outside of Canada,
- Implemented new "whistle-blower" protection for individuals who report a foreign demand for disclosure of personal information, and
- Created offences in connection with violation of the provisions (e.g. fines of up to $500,000 for a corporation, up to $25,000 for a partnership or individual service provider, and up to $2,000 for an employee).

Other than these provisions, there are no health sector specific data residency requirements.

II. Alberta

Legislation. Alberta amended its *Health Information Act*[5] in 2006 by inserting three specific PATRIOT Act provisions[6] to:

- Prohibit compelling a witness to testify or compelling the production of documents except only in response to the direction of a court or tribunal in Canada,
- Require that health information can only be disclosed under an order, warrant or subpoena issued by a court person or body that has jurisdiction in Alberta, and
- Increase the penalties for acting in contravention of the new provisions.

Alberta's *Personal Information Protection Act*[7] was amended in 2009[8] to require an organization - using a service provider outside Canada to collect, use, disclose or store personal information for or on its behalf - to publish, in its policy or practice statement, information as to which countries outside Canada this activity occurs and what purposes the service provider is allowed to use the information.[9]

Notice must be made before or at the time of collection or transfer, in writing or orally, and

[4] RSBC 1996 c 165.
[5] RSA 2000, c H-5
[6] See *Health Information Amendment Act, 2006,* SA 2006, c. 18.
[7] SA 2003 c P-6.5.
[8] *See Personal Information Protection Amendment Act, 2009,* S.A, 2009 c. 50.
[9] S. 6(2).

indicate how an individual may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada and who within the organization can answer questions about the service provider's activities.[10] This requirements concern only those situations where the subject individual has provided consent for the initial collection and use of his or her personal information.

III. Manitoba

Legislation. Manitoba's *Personal Health Information Act*[11] authorizes the Lieutenant Governor-in-Council to make regulations governing the disclosure of personal health information to persons or bodies outside Manitoba. As of the writing of this assessment, no specific regulations have been promulgated and the *Personal Health Information Regulation*[12] contains no provisions concerning the subject of cross-border or cross-boundary transfers or disclosures.

Manitoba's *Personal Information Protection and Identity Theft Prevention Act*[13] does not contain any provisions concerning data residency.

IV. Ontario

Legislation. Ontario has no general personal information protection law (See Canada section below).

Ontario's *Personal Health Information Protection Act*[14] ("PHIPA") prohibits of "disclosures" outside of the province unless under certain circumstances. These circumstances are:

(a) The subject of the information consents to the disclosure;
(b) The disclosure is permitted by the PHIPA or the regulations under that statute;
(c) The recipient performs functions similar to the functions performed by a person within the province to whom this disclosure is permitted under subsection 40(2) of PHIPA;
(d) The following conditions are met:
  (i) the disclosure is for the purpose of health planning or health administration,
  (ii) the information relates to health care provided in the province to a person who is a resident of another province or territory of Canada, and
  (iii) the disclosure is made to the government of that other province or territory of Canada;
(e) The disclosure is reasonably necessary for the provision of health care to the individual and the individual has not expressly instructed the custodian not to make the disclosure in its entirety; or
(f) The disclosure is reasonably necessary for the payment for the provision of health care to the individual."

[10] S. 13.1.
[11] CCSM c P33.5, s. 66(1)(l).
[12] Man Reg 245/97.
[13] CCSM c P33.7. Not in force at the time of this assessment.
[14] SO 2004, c 3, Sch A.

Where a custodian discloses personal health information for healthcare purposes and the subject individual has instructed that not all the personal health information be disclosed, the recipient of the limited personal health information is to be apprised of the existence of the instruction and the limited disclosure.[15]

IPC Views. The IPC special investigation report, *"Reviewing the Licensing Automation System of the Ministry of Natural Resources"* has already been discussed (See Section 2.C above). The report concerned personal information being stored in the United States. The IPC considered that the storage of personal information outside Canada was permissible provided that reasonable contractual measures were taken to protect the data.

V. Québec

Legislation. Québec's approach to the subject of cross-border transfers of data was to focus on safeguards and access. These requirements apply whether or not the personal information crosses an international border or provincial boundary. Québec's Private Sector Law[16], requires, subject to certain exceptions, that those communicating or entrusting information outside of Québec:

> *"must first take all reasonable steps" to ensure that the information is not used for unauthorized purposes or disclosed to third parties without the consent of the subject individuals. If the person responsible for the personal information "considers that the information communicated outside Québec will not receive the requisite protection",*

If these steps are not taken then the communication or placement of the information outside Québec must not proceed[17].

Similarly, another provision of the Act specifying those situations in which consent is not required for the communication of personal information was amended to specify that it applies only to the communication of information required by an Act applicable in Québec (e.g. only a Québec subpoena).

Québec's public sector legislation, *An Act Respecting Access To Documents Held By Public Bodies And The Protection Of Personal Information*[18], contains a similar provision to that found in the Private Sector Law.

VI. New Brunswick

Legislation. New Brunswick has no general personal information protection law (See Canada section below).

[15] See PHIPA, s. 50(2).
[16] RSQ, c P-39.1
[17] RSQ, c P39.1, s. 17.
[18] RSQ, c A-2.1.

Under New Brunswick's *Personal Health Information Privacy and Access Act*[19] and unless otherwise indicated in the legislation, express consent of an individual is required in relation to the collection, use or disclosure of his or her personal health information by a custodian, including when the custodian discloses information to a person outside New Brunswick.

Section 47 the New Brunswick statute provides that a custodian may only disclose personal health information to a person outside New Brunswick in such circumstances described in section 37, 38, or 44 or in circumstances described in the regulations. Section 37 relates to disclosures for health-related purposes; s. 38 to disclosures to health care or other programs; s. 44 to disclosures of registration information pertaining to healthcare professionals.

Section 18 of the *General Regulation*[20] enacted under this statute also permits disclosure outside of the province in circumstances described in s. 43 (disclosure for research purposes). The Regulation also requires, where an information manager is retained, the written agreement between a custodian and information manager to describe the administrative, technical and physical safeguards employed to protect the confidentiality, security, accuracy and integrity of personal health information in the information manager's possession.

Cliniconex's management typically sends three (3) documents to clinics during the on-boarding process: a subscription agreement; the order; and the company privacy policy. Customers are required to acknowledge that they have read and accept the privacy policy.

VII. Nova Scotia

Legislation. Nova Scotia has no general personal information protection law applicable to the private sector (See Canada section below).

In November 2006, the *Personal Information International Disclosure Protection Act*[21] ("PIIDPA") was proclaimed in force in Nova Scotia. PIIDPA applies to a broadly stated range of organizations, defined to be any government department, (or government-appointed agency, board, or commission), school board, university, community college, hospital, district health authority, or children's aid society. It also applies to the directors, officers and employees of public bodies and all employees and associates of service providers.

Substantively, PIIDPA contains a number of provisions that are similar to those found in BC's amendments to its FOIPPA but also contains a number of exceptions to the prohibition of disclosure of personal information outside Canada (e.g. the head of the public body determines that it "meets the necessary requirements" of the organization's operation; if there is a law enforcement agreement or treaty in effect; to collect a debt; where the health or safety of individuals need to be protected, or for research purposes as outlined in the legislation).

Section 44 of Nova Scotia's *Personal Health Information Act*[22]also qualifies the ability of

[19] SNB 2009, c P-7.05, s. 19.
[20] NB Reg 2010-112
[21] SNS 2006, c. 3.
[22] SNS 2010, c 41

custodians to transfer personal health information. The requirements for any transfer are identical to those found in Ontario's PHIPA. (See Ontario section above).

VIII. Newfoundland and Labrador

Legislation. Newfoundland and Labrador has no general personal information protection law applicable to the private sector (See Canada section below).

Newfoundland and Labrador's *Personal Health Information Act*[23] requires a custodian to ensure compliance with the Act with respect to storage, transfer, copying, modification, use and disposition of personal information whether within or outside the province. Section 13(2) of the statute specifically imposes an obligation to protect the confidentiality of personal health information stored, used or disclosed outside the province and the privacy of the subject individual. The disclosure of personal health information to a person outside the province is expressly prohibited unless specific requirements are met.[24] These requirements are identical to those found in Ontario's PHIPA[25] (See Ontario section above).

IX. Canada

Legislation. PIPEDA applies to the "federal private sector" (i.e. works, understandings or businesses) as well as other private sector entities engaged in commercial activities but only in jurisdictions in Canada that do not have legislation that has been designated "substantially similar".

Substantially similar legislation has been enacted (and recognized as such by the federal government) in British Columbia, Alberta and Quebec, as have personal health information protection statutes in Ontario, New Brunswick and Newfoundland & Labrador. The statute does not contain any data residency provisions.

However, Schedule 1 of PIPEDA and in particular Principle 4.1.3 provides:

> *"An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party."*

OPC Views. In considering the interpretation and application of Principle 4.1.3 in the context of cross-border data flows, the Office of the Privacy Commissioner of Canada ("OPC") has issued three findings. While not binding precedents, they nonetheless reflect the Office's views on the subject and serve as useful illustrations.

[23] SNL 2008, c P-7.01.

[24] SNL 2008, c P-7.01, s. 47(1).

[25] SNL 2008, c P-7.01, s. 47(2).

Case 2005-313[26] concerned a bank sending a notification to its VISA customers amending the credit cardholder agreement. The notification referred to the use of a service provider located in the United States and the possibility that American law enforcement or regulatory agencies being able to obtain access to cardholders' personal information under U.S. law.

The OPC determined that PIPEDA does not prohibit the use of foreign-based third-party service providers and the bank, in keeping with its obligations under Principle 4.1.3, had imposed contractual requirements concerning confidentiality and security with its third-party service providers. Any transfer to a service provider is a management exercise requiring an assessment of security risks. The Privacy Commissioner's finding noted that the personal information of Canadians in the possession of a service provider outside of Canada is subject to the laws of the country in which it is located.

The Privacy Commissioner's position was that transparency was required: any organization having personal information processed outside of Canada should notify its customers that the information may be available to government authorities under a lawful order made in that country. Because the bank in question provided such notification, indicating to clients that their personal information might be accessed under the provisions of the PATRIOT Act while in the possession of a U.S.-based service provider, the bank was in compliance with PIPEDA.

Finding 2006-333[27] involved a security system provider, a Canadian subsidiary of a U.S. company, which had advised its Canadian customers that it intended to share customer contact information with its parent company by routing incoming home security alarm signals through another monitoring centre in North America. The only personal information shared would be information needed to provide monitoring and security services, such as the customers' home or business addresses, a phone number and an emergency contact list.

Since the company sent out a notification explaining what it was doing with customers' personal information, the OPC concluded that the obligation under PIPEDA Principle 4.8[28] was satisfied because the company readily made available specific information about its policies and practices relating to the management of personal information.

The third finding, Finding 2008-394[29], involved a website's e-mail operations that were outsourced to a U.S.-based firm. Existing subscribers were informed in advance that their new login to their account would be an opportunity for them to accept or reject the terms of the services. New e-mail subscribers were also informed, not only of information transfers to the U.S.-based provider but also the potential privacy implications.

The Privacy Commissioner rejected the complaints against the website owner insofar as the email provider had fulfilled its obligations to provide comparable protection under the Act by

[26] Available at: http://www.priv.gc.ca/cf-dc/2005/313_20051019_e.asp.
[27] Available at: http://www.priv.gc.ca/cf-dc/2006/333_20060511_e.asp.
[28] Principle 4.8 concerns Openness and states: *"An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information."*
[29] Available at: http://www.priv.gc.ca/cf-dc/2008/394_20080807_e.asp.

putting in place adequate contractual provisions. In this case, the Privacy Commissioner's position was re-iterated on two key points:

> *"Organizations must be transparent about their personal information handling practices. A company in Canada that outsources personal information processing to a company that operates in another country should notify its customers that the information may be available to the government of that country or its agencies under a lawful order made in that country.*
>
> *With regard to the issue of customer consent, the Office has taken the position that the sharing of information with a third-party service provider constitutes a "use" for the purposes of the Act. Organizations obtain customer consent for the use of personal information for the provision of services or products when individuals first apply for the service or product. Although service providers may change over time, if the purpose of the current provider's use of the personal information has remained the same, organizations are not required to obtain renewed customer consent for the information use."*

2. Analysis

The legislative provisions described above, IPC views and OPC Findings have to be taken into consideration by the initial collectors of the personal information in question (in the case of Cliniconex, potential or current clients).

Of particular significance is the fact that *client data*, including personal information collected used or disclosed by clients, is processed partly in Canada and partly in the United States.

When looking at data residency requirements, most legislation in Canada permits the transfer of health data outside of the province with the express consent of the subject individual. This is not a Cliniconex "issue" *per se* but rather a customer issue since they are the custodians of the personal health information in question. Having said that, Cliniconex has to satisfy the customer that this is not a problem. Since express consent removes any data residency obstacle, Cliniconex should revise its business process:

1. Contractually oblige customers to obtain an express consent;
2. Revise the Cliniconex Privacy Policy to meet notification requirements found in Canadian legislation;
3. Provide a written explanation as to how the personal information is processed outside of Canada (e.g. the nature and extent) for use in seeking patient consent; and
4. Provide a consent form for use by customers.

Cliniconex need not obtain the consents from patients – these can be left with customers but it should avoid potential legal liability by customers and Cliniconex by ensuring that such consents are obtained.

C. PHIPA (ONTARIO)

Ontario's *Personal Health Information Protection Act, 2004*[30] ("PHIPA"), in creating a statutory framework for the collection, use and disclosure of personal health information in Ontario, applies to the management and safeguarding of "personal health information" held by a "health information custodian" ("HIC"). A HIC is a person or organization that has custody or control of personal health information as a result of, or in connection with, the person's or organization's powers or duties and is listed in s. 3 of PHIPA. This concept of "custodian" is similarly used in other Canadian jurisdictions.

PHIPA also applies to a certain extent to "agents" of providers, and "health information network providers". This application to service providers is another concept found in Canadian health privacy legislation (in some provinces, an "information management service provider"). Such a provider is defined as an entity that processes the records of a HIC or that provides information technology services with respect to such records[31].

An important preliminary question: Is the information in question personal health information? It consists of identifying information (name, email, telephone number) and appointment information with a healthcare provider. PHIPA provides a broad definition of "personal health information". Of particular note is s. 4(1) of the legislation:

> *"personal health information", subject to subsections (3) and (4), means identifying information about an individual in oral or recorded form, if the information, ...*
>
> *(b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,*

The Cliniconex solution can be configured to remove both the patient and provider's names but that may not be possible or desirable in all instances. Therefore, for the purposes of this assessment, the information in question should be considered as personal health information. The existence of identifying information is self-evident although the term is defined in s.4(2):

> *"identifying information" means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.*

Cliniconex is not a HIC for the purposes of provincial legislation. In the other provinces in which it operates it can be classified as an "information manager". In Ontario, it could be viewed as a

[30] *Personal Health Information Protection Act, 2004*, SO 2004, c. 3, Sch A.

[31] See, for example, *Health Information Act*, RSA 2000, c H-5, s 66(1); *Personal Health Information Act*, CCSM, c. P33.5, s 1(1); *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05, s 1; *Personal Health Information Act*, SNL 2008, c P-7.01, s. 2(1)(l); *Health Information Protection Act*, SS 1999, c H-0.021, s. 2(j); and *Personal Health Information Act*, SNS 2010, c 41, ss. 24, 28; Health Information Act, SNWT 2014, c 2, s 13; and *Health Information Privacy And Management Act*, SY 2013, c 16, Part 6 (not yet in force).

service provider and, as a result of such status, is subject to s. 10(4) of PHIPA and the associated General Regulation.

1. Service Provider Requirements

Service Provider Requirements – PHIPA s. 10(4)		
Citation	Requirement	Comment
General, O Reg. 329/04, s. 6(1) #1	"The person shall not use any personal health information to which it has access in the course of providing the services for the health information custodian except as necessary in the course of providing the services."	Aside from possible access for support purposes, Cliniconex does not use any client information.
General, O Reg. 329/04, s. 6(1) #2	"The person shall not disclose any personal health information to which it has access in the course of providing the services for the health information custodian."	Cliniconex does not disclose the data in question to third parties unless authorized or required by law. Requests for access, while technically possible, are referred back to the HIC.
General, O Reg. 329/04, s. 6(1) #3	"The person shall not permit its employees or any person acting on its behalf to be able to have access to the information unless the employee or person acting on its behalf agrees to comply with the restrictions that apply to the person who is subject to this subsection."	Access to personal information is restricted to supporting, and operating the Cliniconex service. Staff are required to sign confidentiality and non-disclosure undertakings.

The table below addresses questions raised in Parts A and B of the Ontario Information and Privacy Commissioner's *PHIPA Privacy Impact Assessment Questionnaire*.

[Remainder of page left intentionally blank]

2. Part A: Organizational Privacy Management

The questions in this section relate to privacy management.

No.	Question	Yes	No	Comment
A1	Is there an organizational strategic plan or business plan that addresses privacy protection?		X	Cliniconex does not currently have a mature privacy and security program, with an identified management and governance framework for both privacy and information security. It is noted that the company is in the process of implementing a series of policy documentation, including privacy and security policies.
A2	Does your organization have a written privacy policy or statement of information practices?	X		Generally, compliance with this requirement is a client responsibility. Cliniconex provides a copy of its privacy policy to customers and requests acceptance of the policy.
A3	Have privacy policies or procedures been developed for various aspects of the organization's operations?	X		See Response A2. An employee privacy policy is currently under development.
A4	Do the privacy policies or procedures that you identified in response to questions A2 and A3 ensure the following:			
A4a	Personal health information is collected in accordance with PHIPA and other applicable legislation.	X		The collection of personal health information is the responsibility of the health information custodian. Cliniconex is a service provider to Family and Specialty clinics.
A4b	Individual consent is obtained in accordance with section 18 of PHIPA where consent is required	X		Responsibility for obtaining consent rests with the HIC. Cliniconex serves as a service provider or information manager to those HICs. Cliniconex should consider giving appropriate guidance and text to customers to ensure that any consent is knowledgeable and informed.
A4c	A written public statement			The HIC, as collector of PHI, has the

No.	Question	Yes	No	Comment
	about the organization's information practices, who to contact with privacy questions or complaints, and how to obtain access or request correction of a record of personal health information is readily available to individuals, as outlined in section 16 of PHIPA.		X	obligation to inform the individual as to the provider's privacy practices. Requests for access or correction are referred to the HIC. In terms of Cliniconex providing notice to end users, it is noted that the company is in the process of implementing a series of policy documentation, including privacy and security policies. Cliniconex should consider the development and publication of a statement concerning data residency and how it assists customers obtain the direct consent of patients.
A4d	Individuals are entitled to request access to and correction of their own personal health information as provided for under sections 52-55 of PHIPA, subject to exceptions.	X		See Response A4c. Cliniconex is a service provider/information manager to the HIC. As such, it directs access requests to the HIC.
A4e	There is a record retention schedule for records of personal health information that outlines the minimum and maximum lengths of time personal health information may be retained as well as procedures outlining the manner by which personal health information will be securely destroyed		X	Record retention is the HIC's responsibility and subject to its own record retention policies. In terms of Cliniconex own record retention, it is noted that the company is in the process of implementing a series of policy documentation, including a record retention policy. No record retention schedule has been established though. It is also noted that the Reference ID index effectively de-identifies appointment details stored in the Cloud Controller. The reference index is deleted from the reminder application after 30

No.	Question	Yes	No	Comment
				days. After no more than 180 days, the reference index data is permanently deleted or rendered unrecoverable (such as from backups).
A5	Are administrative, technical and physical safeguards in place at the organization to protect personal health information against theft, loss, unauthorized use or disclosure and unauthorized copying, modification or disposal pursuant to section 12 of PHIPA?	X		See Part 2.B.3 above for a description of safeguard measures deployed by Cliniconex. Reliance is placed on the security measures in place for the PaaS and SaaS providers are used in connection with the appointment reminder service.
A6	Is there an appointed privacy contact person in the organization?	X		Compliance with this requirement is generally a client responsibility. Cliniconex's CTO serves as the company's Privacy Officer.
A7	Does a reporting process exist to ensure that the organization's management is informed of any privacy compliance issues?		X	No formal reporting process currently exists. It is noted that the company is in the process of implementing a series of policy documentation, including an incident management policy.
A8	Are senior executives actively involved in the development, implementation and/or promotion of your organization's privacy program?	X		Compliance with this requirement is generally a client responsibility. Cliniconex is a small organization and privacy issues are quickly brought to the attention of senior management
A9	Are employees or agents with access to personal health information in your organization provided training related to privacy protection?		X	No training process is currently in place. Cliniconex should implement a training and awareness program for Cliniconex staff.
A10	Have policies and			It is noted that the company is in the

No.	Question	Yes	No	Comment
	procedures been developed concerning the management of privacy breaches, including the notification of individuals when the confidentiality of their personal health information has been breached?	X		process of implementing a series of policy documentation, including an incident management policy.

3. Part B: Project Privacy Management

The questions in this section relate specifically to the Cliniconex appointment reminder service.

No.	Question	Yes	No	Comment
B1	Has a summary of the proposed or existing information system, technology or program been prepared, including a description of the requirements for the system, technology or program and a description of how the information system, technology or program will or does meet those needs?	X		This PIA report is intended to provide a summary of the existing solution.
B2	Has a listing of all Personal Health Information or data elements that will be or are collected, used or disclosed in the proposed or existing information system, technology or program been prepared?	X		See Part 3 above.
B3	Have diagrams been prepared depicting the flow of Personal Health Information in the proposed or existing information system, technology or program?	X		See Part 3 above.

No.	Question	Yes	No	Comment
B4	Have documents been prepared showing which persons, positions or employee categories will have access to which elements or records of Personal Health Information?	X		It is noted that the company is in the process of implementing a series of policy documentation, including an access control policies.
B5	Does consent from the individual or an authorized substitute decision-maker provide the primary basis for the collection, use and disclosure of Personal Health Information for the proposed or existing information system, technology or program?	X		Compliance with this requirement is a client responsibility. Cliniconex serves as either a "service provider" or an "information manager" to HICs.
B6	Have you documented the purposes for which Personal Health Information will be or is collected, used or disclosed in the information system, technology or program?	X		Compliance with this requirement is a client responsibility. This document is intended to satisfy this requirement. The company's privacy policy also formally addresses collection, use and disclosure of personal information.
B7	Is Personal Health Information collected, used, disclosed or retained exclusively for the identified purposes and for purposes that an individual would reasonably consider consistent with those purposes?	X		See Response B6.
B8	Will Personal Health Information in the proposed or existing information system, technology or program be linked or cross-referenced to other information in other information systems technologies or programs?		X	Compliance with this requirement is a client responsibility. Other than the combination of identifying information with appointment information, the nature of the Cliniconex appointment reminder service does not have interfaces with private and public information systems, which permit

No.	Question	Yes	No	Comment
				the exchange of information, including personal health information.
B9	Will Personal Health Information collected or used in the information system, technology or program be disclosed to any persons who are not employees or agents of the responsible organization?		X	The resources of PaaS and SaaS providers are used to assemble and deliver appointment reminders.
B10	Have you made arrangements to provide full disclosure of all purposes for which the information system, technology or program will collect Personal Health Information?	X		Compliance with this requirement is a client responsibility. As identified in the company's Privacy Policy, the only purpose for collection, use and disclosure by Cliniconex is to provide appointment reminders to patients. Cliniconex should consider making the Privacy Policy publicly available through its website.
B11	Have communications products and/or a communications plan been developed to fully explain the information system, technology or program to individuals and how their Personal Health Information will be protected?	X		Compliance with this requirement is a client responsibility. Cliniconex's website explains the nature of the service offering but the company should consider a more fulsome public statement as to its security measures and how it satisfies data residency requirements (i.e. through patient consent).
B12	Does the proposed or existing information system, technology or program involve the collection, use or disclosure of any Personal Health Information beyond Ontario's borders?	X		Some processing occurs outside of Ontario. PaaS and SaaS providers used to assemble and deliver appointment reminders. These providers agree under their own contract terms not to use client information (here Cliniconex) other than in connection with the provision of their services.
B13	Has an assessment been			Compliance with this requirement is

No.	Question	Yes	No	Comment
	completed to identify potential risks to the privacy of individuals whose Personal Health Information is collected, used, retained or disclosed by the proposed or existing information system, technology or program?	X		a client responsibility. This document is intended to support client privacy assessments.
B14	If potential risks to privacy have been identified, have means to avert or mitigate those risks been incorporated into the design and/or implementation of the proposed or existing information system, technology or program?		X	See Part 2.B.3 above for a description of safeguard measures deployed by Cliniconex. No formal security assessment of the product has ever been conducted.
B15	Has an assessment been completed to identify whether other health information custodians have implemented the same or a similar information system, technology or program, the risks to privacy experienced by other health information custodians and the means implemented by these other health information custodians to avert or mitigate these risks?		X	Compliance with this requirement is a client responsibility. It is noted that the company is in the process of implementing a series of policy documentation, including incident management.
B16	Have key stakeholders been provided with an opportunity to comment on the sufficiency of privacy protections and their implications on the proposed or existing information system, technology or program?		X	Compliance with this requirement is a client responsibility.

No.	Question	Yes	No	Comment
B17	Will users be trained in the requirements for protecting Personal Health Information and will they be made aware of the relevant notification procedures if Personal Health Information is stolen, lost or accessed by unauthorized persons?	X		Compliance with this requirement is a client responsibility. Cliniconex requires that all employees sign confidentiality agreements. Cliniconex should ensure employees undergo appropriate privacy training.
B18	Have security policies and procedures to protect Personal Health Information against theft, loss, unauthorized use or disclosure and unauthorized copying, modification or disposal been documented?	X		See Part 2.B.3 above for a description of safeguard measures deployed by Cliniconex. It is noted that the company is in the process of implementing a series of policy documentation, including information security policies. Draft policies have been prepared.
B19	Have privacy policies or procedures been developed for various aspects of the operations for the proposed or existing information system, technology or program?	X		Compliance with this requirement is a client responsibility. It is noted that the company is in the process of implementing a series of policy documentation, including information security policies. The company already has a privacy policy.
B20	Do the privacy policies or procedures that you identified in question B19 ensure the following:			
B20a	Personal Health Information in the proposed or existing information system, technology or program is collected in accordance with *PHIPA* and other applicable legislation;	X		Most compliance obligations fall on the HIC.
B20b	Individual consent is			Cliniconex does not directly obtain

No.	Question	Yes	No	Comment
	obtained in accordance with section 18 of *PHIPA* for the proposed or existing information system, technology or program where consent is required;		X	consent for the use of the service. Obtaining consent is the responsibility of the HIC.
B20c	A written public statement about the purposes for which the proposed or existing information system, technology or program collects, uses or discloses Personal Health Information is readily available to individuals as outlined in section 16 of *PHIPA;*		X	Compliance with this requirement is a client responsibility. Cliniconex should consider a communication statement aimed at patients.
B20d	Individuals are entitled to request access to and correction of their own Personal Health Information in the proposed or existing information system, technology or program as provided for under sections 52-55 of *PHIPA*, subject to certain exceptions;	X		In the event such a request is received, individuals are directed to the HIC for any access or correction requests.
B20e	There is a record retention schedule for records of Personal Health Information that outlines the minimum and maximum lengths of time Personal Health Information may be retained in the proposed or existing information system, technology or program, as well as procedures outlining the manner by which Personal		X	No record retention schedule has been established. It is also noted that the Reference ID index effectively de-identifies appointment details stored in the Cloud Controller. The reference index is deleted from the reminder application after 30 days. After no more than 180 days, the reference index data is permanently deleted or rendered unrecoverable (such as from

No.	Question	Yes	No	Comment
	Health Information in the proposed or existing information system, technology or program may be securely destroyed.			backups).
B21	Does the proposed or existing information system, technology or program provide functionality for the logging of the insertion, access, modification or disclosure of Personal Health Information as well as an interface to audit those logs for unauthorized activities?		X	The nature of the solution does not lend itself to logging activity.

D. CSA Code (PIPEDA)

A further layer of analysis, especially for private sector organizations can be conducted using the ten fair information practice principles of the Canadian Standards Association *Model Code for the Protection of Personal Information* ("CSA Model Code")[32].

The CSA Model Code principles are:

- Accountability
- Identifying Purpose
- Consent
- Limiting Collection
- Limiting Use, Disclosure and Retention
- Accuracy
- Safeguards
- Openness
- Access
- Challenging Compliance

1. Accountability

Under the CSA Code, an organization is responsible for personal information under its control. At a minimum, such responsibility requires the designation of one or more individuals to be accountable for the organization's compliance with the principles described in the Code. This accountability extends to information that has been transferred to a third party for processing and obliges the organization to use contractual or other means to provide a comparable level of protection while the information is being processed by that third party.

Meeting these expectations requires evidence of a mature administrative structure for privacy. This includes having privacy risks accepted at an appropriate senior level; documenting procedures; ensuring privacy training is conducted and refreshed regularly; including privacy protective language in all contracts with third parties handling personal information; and ensuring that that privacy compliance audits are undertaken on a regular basis.

Generally, a client's privacy and access framework is (or should be) designed to provide internal policies, procedures and an administrative structure to comply with its legal requirements. Cliniconex is does not have a mature privacy and security framework although it is moving to implement a suite of privacy and security policies.

Usually, data residency is raised as an accountability issue in the use of service providers and, generally notice of location of data is expected in client privacy statements/policies. In this instance, the retention of client data within Canada eliminates the issue although clients may

[32] The text of the CSA Code forms Schedule 1 to PIPEDA and is available at: http://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/latest/sc-2000-c-5.html#SCHEDULE_1__121957

wish to provide a greater degree of assurance to their own customers by indicating that Office 365 services will be used and data processed within Office 365 services remains in Canada.

Cliniconex staff are required to sign confidentiality and non-disclosure undertakings.

Contractors are required to sign agreement to ensure compliance with Cliniconex policies on required engagements.

2. Identifying Purpose

To the extent personal information is collected, the purposes are to be identified by the organization at or before the time the information is collected. The collection of personal information for permitted purposes is a client responsibility since Cliniconex has no role in the direct collection of patient data.

Cliniconex's Privacy Policy does state the sole purpose of its use of personal information is in the provision of its appointment reminder service. However, a patient-oriented communication concerning privacy should be made publicly available.

3. Consent

The Consent Principle requires that the knowledge and consent of the individual are required for the collection, use, or disclosure of the data subject's personal information. A further qualification is that the reasonable expectations of the subject individual have to be met as well. It is expected that such consent will usually be obtained at the time of collection and that the purposes are stated in a manner where the individual can reasonably understand the proposed use and disclosure of personal information.

With the Cliniconex service, the responsibility for consent remains with the customer. Cliniconex, as a service provider, has no specific obligation here concerning consent. However, given the need for patients to understand the data residency issue, since express consent removes any data residency obstacle, Cliniconex should revise its business process to:

1. Contractually oblige customers to obtain an express consent;
2. Revise the Cliniconex Privacy Policy to meet notification requirements found in Canadian legislation;
3. Provide a written explanation as to how the personal information is processed outside of Canada (e.g. the nature and extent) for use in seeking patient consent; and
4. Provide a consent form for use by customers.

4. Limiting Collection

The collection of personal information is to be limited to that which is necessary for the identified purposes. This implies an obligation to ensure that the amount and the type of information collected are strictly necessary to fulfill the stated need. Another way to describe this concept is "data minimization".

Collection of patient data is the responsibility of the client. Cliniconex's collection of personal information is for user registration purposes; system management purposes and the actual delivery of appointment reminders to patients. The number and nature of the data elements collected by Cliniconex are reasonable and necessary in connection with the purposes of their collection.

5. Limiting Use, Disclosure and Retention

The general rule is that personal information is not to be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by, or allowed in, legislation. Once personal information is no longer required for the identified purposes it is to be securely destroyed, erased, or made anonymous.

Disclosure. Cliniconex indicates that will not disclose client data outside of the company or its affiliates except (1) as the client directs. It should consider slightly narrowing that obligation to also indicate "as required by law".

Cliniconex should indicate that it will not disclose client data to law enforcement authorities unless required by law. The company should also keep an accurate accounting of disclosures of information held in each system of records under its control, including date, nature, and purpose of each disclosure of a record.

Retention. Record retention is the HIC's responsibility and subject to its own record retention policies.

In terms of Cliniconex own record retention, it is noted that the company is in the process of implementing a record retention policy. No record retention schedule has been established though.

In terms of what the solution does, the Reference ID index effectively de-identifies appointment details stored in the Cloud Controller. The Reference ID index is deleted from the reminder application after 30 days. After no more than 180 days, the reference index data is permanently deleted or rendered unrecoverable (such as from backups).

6. Accuracy

The concept of "accuracy" as a principle is related to "use" in that if information is used to make a decision it should be as accurate and up-to-date as possible in order to ensure that inappropriate information will not be used to make a decision about an individual.

Amendment of patient information occurs at the EMR level within a customer's clinic.

7. Safeguards

Personal information is to be protected by security safeguards appropriate to the sensitivity of the information. This principle requires particular care to be used for data at rest and in transit, as well as the disposal or destruction of personal information.

See Part 2.B.3 above for a description of safeguard measures deployed. It is noted that there are no audit measures to support the deployed safeguards. In formalizing a number of information management and IT policies/procedures, the company should also establish controls to ensure adherence to the policies and an audit procedure to ensure that controls are effective.

Cliniconex should also provide appropriate role-based security training to personnel with assigned security roles and responsibilities as well as privacy training to all employees. Contract staff are required to take any training determined to be appropriate to the services being provided and the role they perform.

8. Openness

Organizations are expected to be open about their policies and practices with respect to the management of personal information. Descriptions of such policies and practices are to be made available in a form that is generally understandable.

The information made available shall include:

1. The name/title and address of the person who is accountable for the personal information policies and practices and to whom complaints or inquiries or requests for recourse can be forwarded,
2. The means of gaining access to personal information,
3. A description of the type of personal information held including an account of its use, and
4. Information that explain the policies and procedures surrounding the use of personal information.

Generally, compliance with the openness principle is a client responsibility.
In terms of Cliniconex providing such information to customers and patients, it does not do so except for one reference to an email address in its Privacy Policy. Cliniconex should update its privacy policy to include such information as well as information on data residency and provide a link to its Privacy Policy on its website.

9. Access

Under the CSA Code, individuals have a right to access their own personal information and to request that corrections be made.

Generally, this is an obligation for customers since Cliniconex is simply a service provider to the clinic.

While the prospect of access requests is likely minimal, it is noted that the company has a draft “Access Request” form but the context for its creation is unclear. The company has no publicly available access request process nor does the privacy policy indicate what the customer’s responsibility is or what patients are to do. Cliniconex should put in place a simple access process – given the current size of the company – and revise its privacy policy as to indicate the respective roles and responsibilities of the company and customers vis-a-vis access.

10. Challenging Compliance

Organizations are required to have procedures in place to address complaints or inquiries pertaining to the handling of personal information. The complaint process is to be easily accessible and simple to use. Where a complaint is justified, systemic problems are to be addressed through the amendment of applicable policies and practices.

Cliniconex should add language as to how to contact the company concerning complaints and/or inquiries. It may be that complaints are better addressed by customers (since it is there patients) but even a statement to that effect would avoid confusion by better defining roles and responsibilities.

[Remainder of page left intentionally blank.]

PART 5: CONCLUSION

The objective of a privacy impact assessment is to identify areas of non-compliance with applicable privacy legislative requirements and/or personal information protection principles. The focus of such an assessment is to determine how organizations avoid or minimize the loss, damage, misuse or abuse of personal information.

The consequences associated with a failure to address privacy risks are manifold. These include:

(a) Public expectations as to the protection of personal information are not met,
(b) Key stakeholders withdraw support because of perceived privacy threats,
(c) Regulators take action to respond to a failure in legislative compliance, or
(d) Legal claims (including class actions) are made for compensation from affected individuals.

For Cliniconex customers, privacy risks can manifest themselves in a variety of ways but generally revolve around:

- Unauthorized use of information by authorized users;
- Unauthorized collection/use or disclosure of information by external parties;
- Unauthorized or inappropriate collection/use or disclosure by a contractor, service provider or partner organization;
- Loss, destruction or loss of use of information;
- Loss of integrity of information;
- "Function creep" or changes in use and/or disclosure; or
- Non-compliance with legislative requirements (e.g. accuracy, access or correction).

In a "not unexpected" way, given the size of the company, Cliniconex does not have a mature privacy and security management framework and this framework needs to evolve over time. Beyond the security of the PaaS and SaaS service providers, the security of the solution is not fully known and a security assessment should be performed or, at a minimum, a security architect should be consulted as to the existence of vulnerabilities in design and deployment.

To their credit, the company's management recognizes this fact. As a first step, management is considering a series of privacy and security-related policies/procedures to better document and define its privacy and security posture. But even with the adoption of these policies, audit controls will need to be instituted to ensure adherence to them.

Furthermore, the corporate privacy policy should be revised and updated to address both access to personal information procedures as well as data residency. The audience for the document should be both customers and their patients and the full privacy policy should also be made generally available through the company website.

The nature of the personal information in question may not be considered by some to be particularly sensitive – name, mobile/home telephone number/email address/appointment information but the context of the appointment (with whom, for example, or where) could be sensitive personal information.

Clients concerned with data residency – the location where customer personal information will be processed needs to be expressly addressed. Whether in terms of being aggregated within the Cloud Controller or sent via a third party service provider (e.g. Twilio), the plain fact of the matter is that personal information will be processed outside of Canada. It is not problematic **if** express, informed consent is obtained from patients. This makes the issue more of a communications and business process issue.

In terms of specific suggestions following review of the information provided, it is recommended that:

No.	Recommendation	Comment
1.	Arrange for a formal security assessment of the solution as well as review by a security architect.	No formal security assessment of the product has ever been conducted. The assessment should include penetration testing, security code review, and data loss prevention testing.
2.	Revise business processes so as to: • Contractually oblige customers to obtain an express consent; • Revise the Cliniconex Privacy Policy to meet notification requirements found in Canadian legislation; • Provide a written explanation as to how the personal information is processed outside of Canada (e.g. the nature and extent) for use in seeking patient consent; and • Provide a patient consent form for use by customers.	Personal information is processed outside of Canada. Legislation exists to prohibit such transfer of personal information unless legal exceptions apply. One exception is the express consent of the subject individual. To remove data residency as an issue, Cliniconex should facilitate customers obtaining express consent.
3.	Update the Cliniconex privacy policy to include information to both patients and clinics as to the company's information management practices (e.g. access to personal information, data residency) and provide a link to its Privacy Policy on its website.	Organizations are expected to be open about their policies and practices with respect to the management of personal information. Generally, compliance with the openness principle is a client responsibility. In terms of Cliniconex providing such information to customers and patients, it does not do so except for one reference to an email address in its Privacy Policy.
4.	Adopt a standard form information manager agreement or append a privacy/security annex to its service	Cliniconex has entered into "information manager agreements" or "privacy/security" agreements on an *ad hoc* basis. It will need to

	agreement.	do so if operating in Ontario and a number of other provinces. The company would be better served using its own template.
5.	Establish controls to ensure adherence to policies and an audit procedure to ensure that controls are effective.	In seeking to mature its privacy and security management systems, the company is currently formalizing a number of information management and IT policies/procedures. The effectiveness of these efforts should be supported by specific control.
6.	Establish a simple access to personal information process and revise its privacy policy as to indicate the respective roles and responsibilities of the company and customers vis-a-vis access to personal information.	The process can be simple given the current size of the company
7.	Implement a privacy training and awareness program for Cliniconex staff.	Queries as to the existence of a company training program will likely be raised by customers. The program should focus on company privacy, security and incident management procedures as well as an introduction to legal privacy requirements.
8.	Publish a more fulsome public statement aimed at both customers and their patients as to the company's privacy and security measures as well as how it satisfies data residency requirements (i.e. through patient consent).	No further comment.
9.	Establish a formal record retention schedule.	While record retention for personal information is not extensive given the solution in question, no formal record retention schedule has been created. A draft record retention policy is under consideration.
10.	Revise company statements and agreements to indicate that personal information will not be disclosed unless the customer directs or "as required by law".	Cliniconex indicates that will not disclose client data outside of the company or its affiliates except as the customer directs. This obligation is not technically correct and should be revised
11.	Making the Company's full Privacy Policy publicly available through its website.	A short statement on privacy is located in the "About" section of the company website. This should be replaced with a link to the full corporate privacy policy.
12.	Formally adopt an access control policy for employees.	Current practices reflect the size of the company. Practices should be documented

APPENDIX A - LIST OF DOCUMENTS REVIEWED

1. Letter to Mr. C. Skinner, OIPC, Alberta from client organization (undated but in response to a 11 February 2015 letter). [Response Letter]
2. Commitment to Maintain Health Information Confidentiality, rev2.
3. Health Information Act Compliance Agreement between Cliniconex Inc. and 1267407 Alberta, Ltd., 23 January 2016. [Information Manager Agreement]
4. Privacy Impact Assessment submitted by 1267407 Alberta, Ltd to Alberta OIPC.
5. Cliniconex Privacy Policy, Revision, August 10, 2011.
6. "Cliniconex and Privacy", 30 March 2015, Rev 1 (Communications Add-ons for Medical Clinics).
7. "Cliniconex Data Flow", Jan 2016, Rev 1.1 (Communications Add-ons for Medical Clinics).
8. "Cliniconex and SLAs Jan 2016, Rev 1.0 (Communications Add-ons for Medical Clinics).
9. Cliniconex, Access Management Process Policy, v.1 [Draft]
10. Cliniconex, Back Up Policy, v.1 [Draft]
11. Cliniconex, Data Classification Policy, v.1 [Draft]
12. Cliniconex, Information Security Incident Management Procedure, v.1 [Draft]
13. Cliniconex, Information Security Risk Assessment Process, v.1 [Draft]
14. Cliniconex, Back Up Policy, v.1 [Draft]
15. Cliniconex, IT Security Policy, v.1 [Draft]
16. Cliniconex, Major Incident Management Process, v.1 [Draft]
17. Cliniconex, Major Incident Report template, v.1 [Draft]
18. Cliniconex, Mobile Computing Policy, v.1 [Draft]
19. Cliniconex, PII Access Form, v.1 [Draft]
20. Cliniconex, Principles for Engineering Secure Systems, v.1 [Draft]
21. Cliniconex, Records Retention and Protection Policy, v.1 [Draft]
22. Cliniconex, Secure Development Policy, v.1 [Draft]