MEDEO Privacy Impact Assessment Supporting Documentation

QHR Technologies Inc.

1 Table of Contents

2 Section A: Project Overview

2.1 Project Background

Medeo by QHR Technologies is a secure virtual care platform that enables healthcare providers to conduct online patient appointments through a secure video and messaging system. With devices that connect online, healthcare providers can offer alternatives to traditional office visits for patients who have barriers to their care. The scope of this document is limited to QHR's Medeo product.

Medeo delivers three major pieces of functionality via web applications and mobile applications, and this is described below.

2.1.1 Secure Messaging

Medeo enables patients and providers to communicate securely through text based messaging. Message threads support conversations with multiple individuals and when complete, can be closed by clinic users to ensure that no communication goes unmonitored.

Medeo Secure Messaging supports attachments as part of the conversation which allows for patients to share relevant diagnostic documents, such as an image or other media. Providers can use the attachments to share relevant educational material, results, or anything else which may be helpful for the patient to have.

Secure Messaging enables simple, non-urgent consults to be performed at the convenience of the patient and provider.

Patients and providers who are part of the message thread can view the messages, though organizations can be set up so information can be shared amongst other providers within the same organization. When a message is added to a message thread, participants will receive an email to inform them that there is a new message. The email will not contain the content of the message.

Patients and providers will need to launch to Medeo and authenticate, or be using an API Client which has integrated to Medeo and has authenticated as them to view the message.

2.1.2 Video Visits

Many areas of Canada do not have enough health care providers to service their local populations, and patients end up having to travel large distances. Medeo enables health care providers to perform a consult with a patient remotely using a secure video stream. Through use of a video consult, neither the patient nor provider are tied to the typical need to be in a physical clinic which drastically improves access to care for the patient.

Patients can connect using mobile devices, laptop computers, or desktop computers with a camera. Providers can connect using laptop computers or desktop computers with a camera.

Providers can take snapshots of the video stream to create health records of relevant visuals, such as a skin lesion or injury.

2.1.3 Online Booking

Online Booking enables patients to book an appointment at a time that is convenient without needing to call the clinic. Online Booking also keeps the patient informed of any changes to the appointment, such as if it is accepted, cancelled, moved, or if it will be with a different health care provider than originally booked with.

In addition to the ease of scheduling an appointment to the patient, this creates significant administrative savings for clinic staff as each booking or booking adjustment would have been one or more phone calls to coordinate with the patient.

2.1.4 Health Information Storage and Access

2.1.4.1 Storage

Personal Information about the patient is required to facilitate identification of the individual and communication via email or SMS.

Health Information is required on an as needed basis for the facilitation of a booking, or consult with a health care provider to provide their services to the patient.

Health Information is securely stored in QHR data centers located in:

- Kelowna, British Columbia
- Calgary, Alberta
- Toronto, Ontario

Medeo does not store any health information on the device which is accessing the web application.

All data for Medeo is retained indefinitely for backup and Custodial requirements.

Access to health information by Provider Users within Medeo is logged and the audit log can be viewed by Provider Users on a patient by patient basis.

2.1.4.2 Datacenter Access

QHR Technologies follows the ISO 27002 Framework for Information Security and all Medeo systems are stored within datacenter facilities which feature:

- Non-descript buildings, within a monitored security envelope.
- Multi-factor authentication to enter the facilities, including mantraps and other means to prevent unauthorized access.
- Video monitoring within the facilities.
- Secure space / racks for holding the equipment provisioned for the ASP.
- Restricted access to cabling and power equipment.
- Redundant power, with separate 'A' and 'B' power circuits.
- UPS and generator power backup.
- Redundant cooling with capacity to power cooling systems and building systems through power outage.

- Datacenter safe fire suppression systems, which use dry-pipe water systems and are zoned such that if a fire were to occur only the very specific zone(s) impacted would have water extinguishing activated.
- Fire extinguishers marked and available within facilities.
- All access is logged and recorded.
- Only QHR Datacenter Administrators have access to the facilities.
- Visitors must be accompanied by QHR staff, and must present photo ID and check-in prior to admittance.
- Only the Director of Technology and Technical Services can authorize access for new staff.
- All Canadian customers exclusively use datacenters that are located in Canada.
- Networks protected by Firewalls with IPS (Intrusion Prevention Systems) and Edge monitoring.
- Managed Anti-virus with rigorous update and patch control.

2.1.4.3 Medeo Web Application Access

The Medeo platform is built in a secure fashion with an IDP (identity provider) for patients and healthcare providers, which uses OAuth2.0 for authentication. OAuth2.0 is a secure protocol designed to provide authorization flows for web applications, mobile phones and room devices (e.g. shared computer).

Patients will primarily access Medeo through invite by a Health Care Provider who they interact with that uses one or more of the features of Medeo to improve patient access. Best practice for inviting patients is to do so from an integrated platform, such as an EMR where the patient's identity has already been confirmed.

Patients do not have access to any personal health information other than what they provide directly until they begin to have interactions with health care providers at which point the patient's identity should be confirmed prior to delivery of services or sharing of any additional health information.

Providers do not have access to a personal or health information provided by a patient within Medeo, until the patient has been associated to a provider's organization. Patients grant access by associating themselves to an organization in one of the following ways:

1. Accepting a secure message via email
2. Accepting an appointment invite via email
3. Booking an appointment themselves

3 Section C: Project Privacy Analysis

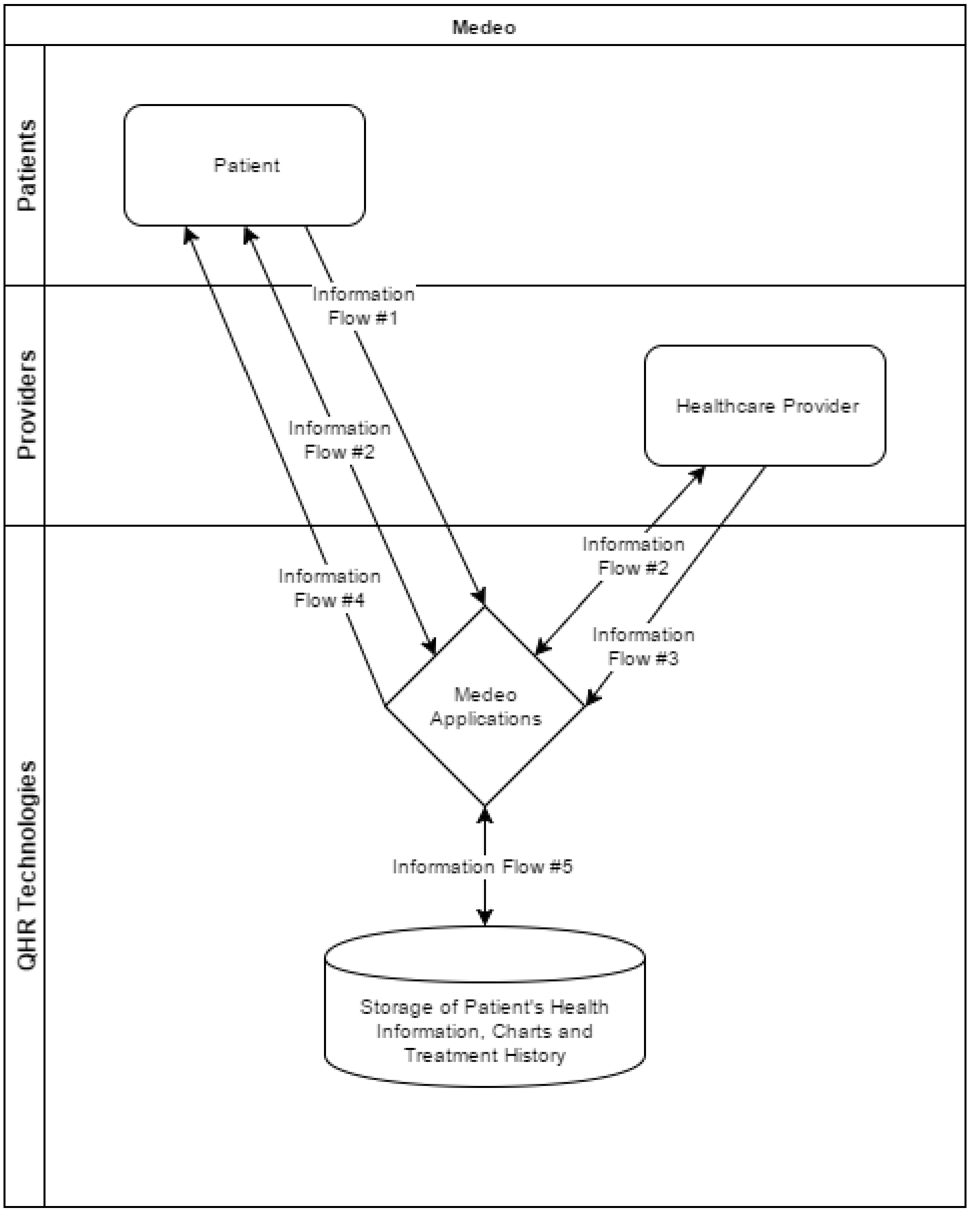
3.1 Health Information Listing

Category	Use	Data	Necessity
Patient	Profile	Picture	Optional
Patient	Profile	First Name	
Patient	Profile	Last Name	
Patient	Profile	Sex	
Patient	Profile	Phone #	For New e-booking sign ups, phone number is req.
Patient	Profile	Health Care #	Optional
Patient	Profile	Family Doctor Name	Optional
Patient	Profile	Time Zone	Only available through Medeo
Patient	Profile	Birthdate	
Patient	Profile	Country	Only available through Medeo
Patient	Profile	Province	Only available through Medeo
Patient	Profile	Email Address	
Patient	Profile	Preferred Pharmacy	Optional
Patient	Visit	Principle Reason	
Patient	Visit	Duration of Issue	
Patient	Visit	Medications	Optional
Patient	Visit	Allergies	Optional
Patient	Messaging	Message	
Patient	Messaging	Attachment	Optional
Provider	Profile	Profile Picture	Optional
Provider	Profile	Title	Optional
Provider	Profile	First Name	
Provider	Profile	Last Name	
Provider	Profile	Title Suffix	Optional
Provider	Profile	Time Zone	
Provider	Profile	Email Address	
Provider	Profile	Phone #	Optional
Provider	Directory Profile	Primary Contact Phone #	Optional
Provider	Directory Profile	Occupation / Specialization	Optional
Provider	Directory Profile	Description	Optional
Provider	Organization	Name	
Provider	Organization	Phone #	Optional
Provider	Organization	Fax #	Optional
Provider	Organization	Address	
Provider	Organization	City	

Provider	Organization	Country	
Provider	Organization	Province	
Provider	Organization	Postal Code	

3.2 Information Flow Analysis

3.2.1 Information Flow Diagram



3.2.2 Legal Authority and Purposes Table

Information Flow	Description	Type of Information	Purpose	Legal Authority
1	Collection of Personal Identification information directly from the Patient	Name, Email, Provincial Health Care Card number, Date of Birth, Phone number	Information is collected to provide access to the service.	Collection AB HIA Sections 18-24 NS PHIA Sections 30-31
2	Communication as needed between Patient and Provider through Medeo service	Medical History, Appointment, Visit, Treatment details	Information related to appointments and visits is collected, and all communication is channeled between the parties.	Collection AB HIA Sections 18-24 NS PHIA Sections 30
3	Collection of Health Information from the Provider	Patient's Name, Email, Medical History, Appointments, Visits, Treatments	Information is collected to review previous treatment and care.	Indirect Collection AB HIA Section 22 NS PHIA Section 31
4	Disclosure of health information back to the patient	Appointments, Diagnoses, Treatment Plans	Information is disclosed to provide ongoing treatment and care	Disclosure AB HIA Section 33 NS PHIA Section 37
5	Usage of collected health information by Medeo services	Name, Email, Appointments	Information is used to send appointment reminders and to assist in communication between patients and providers and scheduling of visits	Use AB HIA Sections 25-30 NS PHIA Sections 33,35

3.2.3 Notice

Every Medeo User whether a Patient or Provider will need to click through an end user agreement which also references the privacy policy. These documents inform individuals of the purposes for which their health information is collected, and how it is used.

Medeo User Agreement (https://ca.medeohealth.com/terms/user)

Medeo Provider Agreement (https://ca.medeohealth.com/terms/provider)

Medeo User Privacy Policy (https://ca.medeohealth.com/terms/privacy)

3.3 Use of Health Information Outside Alberta

QHR Technologies headquarters is in Kelowna BC, and additional offices exist in Vancouver, Toronto, Calgary, and Penticton.

QHR hosts its products and services out of data centers in BC, AB and ON. Medeo infrastructure is primarily hosted in ON.

QHR Customer Support Services Representatives are primarily split between offices in Kelowna, BC and Toronto, ON.

Medeo is a web application which can be accessed from anywhere in the world. Patients and Providers may access Medeo and use the services outside of Alberta or Canada. Providers will still be responsible for the privacy and security of patient data from whatever location they are using the application.

4 Section D: Project Privacy Risks and Mitigation

4.1 Access Controls

Role based Access to Health Information

Position & Job Title	User Role	Number of Staff in this Role	Type of Access (Read, Write, Edit)	Description of Information this User Can Access
Medeo Patient User	Healthcare Services	n/a	Read/Write	Their own information within Medeo for which they have provided or their provider has shared with them.
Medeo Provider User	Healthcare Services	<Clinic Details>	Read/Write	Medical History, Appointment, Visit, Treatment details which were contributed to the patient record by themselves or other Providers in their Organization.
Medeo Provider User	Healthcare Services	<Clinic Details>	Edit	Provider Users can delete their own messages along with attachments.
QHR Director of I.T. and Technology	Access Control, System Monitoring and Maintenance, Deployment	1	Full	All data via Direct Database Access
QHR DevOps	System Monitoring, Maintenance and Deployment	Varies based on team size and responsibilities	Full	All data via Direct Database Access
QHR Product Development	Support	Varies based on team size and responsibilities	Full	All data via Direct Database Access
QHR Product Management	Reporting, Analysis	Varies based on team size	Read	Provider, organization and aggregated

		and responsibilities		patient data via Reporting Systems
QHR Client Services	Support	Varies based on team size and responsibilities	Read	Provider, organization and aggregated patient data via Reporting Systems
QHR Finance	Reporting, Analysis	Varies based on team size and responsibilities	Read	Provider, organization and aggregated patient data via Reporting Systems
QHR Training	Reporting, Analysis	Varies based on team size and responsibilities	Read	Provider, organization and aggregated patient data via Reporting Systems
QHR Business Development	Reporting, Analysis	Varies based on team size and responsibilities	Read	Provider, organization and aggregated patient data via Reporting Systems