Accuro Engage and Medeo
Privacy Impact Assessment Supporting Information

1 Purpose

The purpose of this document is to assist customers in the completion of their own privacy impact assessments (PIAs) specifically for Accuro Engage / Medeo, in accordance with regulatory requirements.

2 Project Description

QHR Technologies Inc. ("QHR") is a Canadian healthcare company founded in 2000. QHR provides software solutions as a service (SaaS) for healthcare professionals and patients.

QHR offers 'Accuro Engage' and 'Medeo,' which allow Providers and Patients to connect virtually in a secure way. Key functionalities include Patient Messaging, Video Visits, Online Booking and Appointment Notifications. Accuro Engage is an add-on tool accessed by Providers through the Accuro©EMR software. Medeo is a secure virtual care platform that is accessed by Patients using either the web application or by using the free mobile application.

Core features include:

2.1.1 Patient Messaging

- Accuro Engage and Medeo allow Providers and Patients to securely message each other without meeting in person. Secure Messaging supports attachments as part of the conversation which allows for Patients to share relevant diagnostic documents, including images. Providers can use the attachments to share relevant educational material, results, or other relevant information. Message threads support conversations with multiple individuals and when complete, can be closed by clinic users to ensure that no communication goes unmonitored.
- Patients and Providers who are part of the message thread can view their messages. When a message is added to a message thread, participants will be informed via email. However, the email will not contain the content of the message.
- Patient Messaging enables simple, non-urgent and follow-up consults to be performed at the convenience of the Patient and Provider.
- Providers can further send mass messages, clinic updates and information, to groups of Patients.

2.1.2 Video Visits

- Video visits allow Providers to launch a secure video visit with a Patient directly through Accuro Engage. This allows Patients to renew prescriptions, share test results and other documents, and conduct quick video follow-ups from anywhere with an internet connection.
- 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 (through Medeo) and Providers (through Accuro Engage) can connect to each other using mobile devices, 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 & Notifications

- Through Medeo, Patients can request a convenient appointment time from their device without having to sit on hold. Clinic staff can confirm all appointments directly through Accuro Engage.
- Patients will receive appointment reminder emails 24 hours before appointment times. Online Booking also keeps Patients informed of any changes to their appointments.
- Access to join virtual visits are found within the reminder email.
- In addition to ease of scheduling, this creates significant administrative savings for clinics as bookings usually would require multiple phone calls.

3 Project Privacy Analysis

3.1 Data Collection, Use, and Disclosure

- In the provisioning of Accuro Engage and Medeo, QHR manages personal information on behalf of healthcare Providers, who remain the custodians of that Personal Information. In the course of using QHR's solutions, healthcare providers will collect, use and/or disclose Personal Information about their Patients, including Personal Health Information.
- Types of information collected include name, email, phone number, demographics, medical history, appointment, visit, and treatment details.
- Instances where data may be shared with third parties and for what purposes is outlined in the Privacy Policy under the section 'Third Party Service Providers.'

3.1.1 Health Information Listing

Category	Use	Data	Necessity
Patient	Profile	Picture	Optional
Patient	Profile	First Name	Mandatory
Patient	Profile	Last Name	Mandatory
Patient	Profile	Phone #	Mandatory
Patient	Profile	Health Care #	Optional
Patient	Profile	Family Doctor Name	Optional
Patient	Profile	Local Time Zone	Only available through Medeo
Patient	Profile	Birthdate	Mandatory
Patient	Profile	Province	Mandatory
Patient	Profile	Email Address	Mandatory
Patient	Visit	Principle Reason	Mandatory
Patient	Visit	Appointment Start Time	Mandatory
Patient	Visit	Interaction Type	Mandatory

Patient	Visit	Appointment Type	Mandatory
Patient	Profile	Medications	Optional
Patient	Profile	Allergies	Optional
Patient	Messaging	Message	Mandatory
Patient	Messaging	Attachment	Optional
Provider	Profile	Profile Picture	Optional
Provider	Profile	Title	Optional
Provider	Profile	First Name	Mandatory
Provider	Profile	Last Name	Mandatory
Provider	Profile	Title Suffix	Optional
Provider	Profile	Time Zone	Mandatory
Provider	Profile	Email Address	Mandatory
Provider	Profile	Phone #	Optional
Provider	Organization	Name	Mandatory
Provider	Organization	Phone #	Optional
Provider	Organization	Fax #	Optional
Provider	Organization	Address	Optional
Provider	Organization	City	Optional
Provider	Organization	Country	Optional
Provider	Organization	Province	Optional
Provider	Organization	Postal Code	Optional

3.1.2 Data Flow Chart and Legal Authorities

Flow	Description	Feature	Source	Types of Info	Purpose/Rationale	Legal Authorities
1	Collection of Personal Identification Information directly from Patient	Sign-up for Medeo Application	Patient to Medeo Application	Name, Email, Phone Number	Information is collected from the Patient to provide access to the Medeo product for the Patient.	Collection PIPEDA 5(3), 6.1 AB HIA Sections 18-24 NS PHIA Sections 30-31
2	Collection of Personal Health Information by the Provider for	Online Booking/ Patient Messaging/Virtual Visit	Patient to Provider (via Accuro Engage)	Demographics, Contact Information, Medical History,	To validate the identity of the Patient, to provide Healthcare Services to the Patient and for accurate	Collection PHIPA ON 17, 18, 29, 34.

	Professional Services			Appointment, Visit, Treatment details	data linking once the Personal Information is with the Provider.	AB HIA Sections 18-24 NS PHIA Sections 30-31
3	Disclosure of Personal Health Information from the Provider to the Patient	Patient Messaging/Virtual Visit	Provider to Patient (via Accuro Engage)	Appointments, Results, Treatment Plans	Information is disclosed to the Patient by the Provider for Patients' own purposes in managing the Patients' ongoing treatment and care.	Disclosure PHIPA ON 52-54 AB HIA Section 33 NS PHIA Section 37
4	Usage of collected Personal Health Information by Medeo	Appointment Reminders/Notifications	Medeo directly to Patients	Name, Email, Appointments	Information is used to send appointment reminders and to assist in communication between Patients and Providers and scheduling of visits.	Use PHIPA ON 17, 37 (2) AB HIA Sections 25-30 NS PHIA Sections 33,35

3.2 Safeguards

QHR uses various security safeguards to protect Personal Information, which include but are not limited to multi-factor authentication, proactive penetration tests, encryption of data in transit (TLS 1.2 or above) and at rest (TDE), active logging, intrusion detection and prevention systems, unique user accounts, role-based access based on need to know policies and ensuring that third parties have similar or better privacy practices than QHR. QHR applies a risk-based approach to determining which controls are required for each instance of Personal Information.

Vulnerability Management: QHR regularly monitors its systems for vulnerabilities and patching using an enterprise grade vulnerability management application. QHR maintains an active vulnerability management program that consists of weekly scanning and monthly meetings with various teams to ensure systems are patched and updated as prioritized by CVSS score.

Penetration Testing: QHR performs annual third-party penetration tests of our systems, and then tracks any important findings to remediation. QHR's penetration testing is performed by 3rd party companies following industry best practices and methodologies.

Data Residency/Hosting: Data is stored at one of the secure and professionally managed data centres in Canada. No PHI is stored outside of Canada. For additional details, please refer to the Privacy Policy at https://accuroemr.com/privacy-policy/.

Datacenter facilities feature the following measures:

- 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
- Networks protected by Firewalls with IPS (Intrusion Prevention Systems) and Edge monitoring
- Managed Anti-virus with rigorous update and patch control

Customer's data is also backed up within QHR's datacenters, with the following characteristics:

- Backups are done automatically (backups the SQL databases directly, no need to run a backup within application first)
- Transactional backups are done every 15 minutes Differential backups are done nightly Full backups are done every 2 weeks and stored for 30 days
- Backup of the customer's specific shared folder is also performed
- Backups are mirrored, meaning they are sent to a replication site for Disaster Recovery
- The data is encrypted with AES encryption and encrypted in transit At no time is a backup unencrypted in the process
- Only authorized Users within QHR have access to the backups, which are stored in a secure facility

Access Controls: QHR has taken steps to ensure that everyone who works for QHR, and the third parties with which we contract, understand the sensitivity of Personal Information and are required to adhere to the protection of Personal Information as set out in this Policy. QHR Staff are educated and trained on the importance of protecting Personal Information and ensure that access is provided only on a "need-to-know" basis. QHR uses roles-based access to ensure that only those who are authorized to access your Personal Information can access it.

Audit Logging: Accuro's audit log feature also allows searching for multiple parameters such as user, date, patient, comment, and activity. Logs can be viewed within Accuro and all database interactions are logged.

Continuous Improvement: QHR continually works to maintain appropriate physical, procedural and technical safeguards with respect to the offices, websites and information storage facilities to prevent loss, misuse, unauthorized access, disclosure, or modification of Personal Information.

3.3 Data Retention

Data retention schedule is up to the Provider. The EMR is a repository and the Provider is the responsible party for the data. Users of the systems can purge data and these actions are logged in the audit log for accountability. Under strict circumstances, QHR can purge data only after approval from an authorized legal authority. Those

purges are also logged. QHR does not store data indefinitely and will remove data thirty days after data destruction papers are signed.

3.4 Requests to Access or Update PHI

Customer users can access and change personal information by contacting Client Services, while patients requesting access or changes will be directed to the Custodian, as stated in Accuro's online Privacy Policy: https://accuroemr.com/privacy-policy/.

3.5 Certifications and Compliance

3.5.1 Certifications

Accuro Engage / Medeo is validated by Ontario Health, as meeting their privacy, security, technology and functionality requirements. Please see: https://www.ontariohealth.ca/system-planning/digital-standards/virtual-visits-verification/verified-solutions-list/Accuro-Engage

QHR conducts annual SOC 2 Type 2 audits by an independent third party auditor and maintains SOC 2 Type 2 Certification (Criteria Security and Availability) for its products, including Accuro Engage and Medeo. QHR also maintains certifications for ISO 13485:2016 for its Quality Management System and PCI DSS. Furthermore, QHR, at the direction of our parent Loblaw Companies Ltd. (LCL), undergoes a yearly Information Security Forum (ISF) Assessment performed by an independent third party.

For a full list of QHR's compliance frameworks, please see https://qhrtech.my.site.com/community/s/article/QHR-Compliance-at-QHR.

3.5.2 Privacy Regulations

QHR Technologies complies with all applicable Canadian privacy laws and regulations. For an exhaustive list, please refer to https://qhrtech.my.site.com/community/s/article/Privacy-and-security-questions.

3.6 Privacy Breach Management

QHR has a policy to notify the customer should there have been a privacy breach impacting the customer data, or significant suspicion of such a breach.

QHR has documented internal t processes that QHR on how to handle privacy events. Breaches are reported to the effected parties as per federal and provincial legislation and the relevant privacy office when required. Specific details and policies can be provided after an NDA is signed.

QHR has obligations under applicable Canadian laws as Agents of our customers. Providers, as the custodians of data, are responsible for the data within their control. In the event of a breach or unapproved exposure of data, QHR would work alongside Providers to assist them in managing the breach.

4.7 Risk Management System

Privacy Risks are a core consideration within QHR's risk management system, which is built into change management for the business and product processes. The Privacy Office performs scheduled reviews of the Risk Register to ensure Risk processes are being appropriately followed and is responsible for approval of Risks at certain risk levels which allows for ongoing monitoring for privacy impacts.

5 Appendix

5.1 About QHR Technologies

Address: 200-1620 Dickson Ave, Kelowna, BC V1Y 9Y2

Client support: 1-866-729-8889

Email support: accuro@qhrtech.com

Customers can submit feedback on features or services through any of the above support methods used by QHR.

QHR's Privacy Office can be contacted by email at privacy@qhrtech.com.

Additional client resources are available at the Accuro Resource Centre: https://qhrtech.my.site.com/community/s/.

5.2 Privacy Policy and Terms of Service

For full information on QHR's privacy measures and consent mechanisms, please review:

QHR's Privacy Policy: https://accuroemr.com/privacy-policy/

Accuro Terms of Service: https://accuroemr.com/terms-of-service/

Medeo Terms of Service: https://patient.medeohealth.com/legal/user

5.3 Frequently Asked Questions (FAQ)

Q. Can QHR help Clients complete a Privacy Impact Assessment (PIA) for Accuro Engage?

A. QHR provides this document to assist clients in the conducting of their own PIAs. However, QHR is not under the obligation to conduct PIAs for clients.

Q. What is the difference between Accuro Engage and Medeo?

A. 'Accuro Engage' is an add-on tool accessed by Providers through the Accuro©EMR software. 'Medeo' is a secure virtual care platform that is accessed by Patients using either the web application or by using the free mobile application. In short, Accuro Engage is the provider connection whereas Medeo is the patient connection.

Q. Is your product certified with PIPA/PIPEDA/HIPAA/GDPR (or other privacy laws/regulations)?

A. Legislations do not provide certifications for compliance with their laws.

Q. Is your product OIPC-compliant/certified?

A. OIPC stands for the 'Office of the Information and Privacy Commissioner.' The OIPC does not have a list of requirements or a certification process which validates a product as 'OIPC-compliant.'

Q. Can you provide more information regarding QHR's Operational, Security, Privacy, and Compliance Frameworks?

A. Yes, QHR has prepared the following document:
https://qhrtechnologies.com/files/client/QHR_Operational_Security_Privacy_Practices.pdf