# Health Myself Innovations Inc.

## Patient Portal Privacy & Security
## Executive Summary

Version: 1
Date: October 25, 2018

# Contents

# Purpose

This Privacy and Security Executive Summary is designed to help Health Myself users identify the procedures for the safe and secure handling of personal information that have been incorporated into the Health Myself Patient Portal (HMPP). This document is not to be considered a PIA or SIA in and of itself but, rather, as a support document to assist with a comprehensive PIA/SIA review undertaken by data custodians using Health Myself Patient Portal and inform the clinic policies they will determine in leveraging the Health Myself platform.

## Versioning

| Version | Date | Comments |
|---|---|---|
| 1 | 2018-10-25 | v1 |

## Glossary

| | |
|---|---|
| **API** | Application Programming Interface |
| **CRM** | Customer Relationship Management |
| **EMR** | Electronic Medical Record |
| **HCP** | Health Care Provider |
| **HMPP** | Health Myself Patient Portal |
| **PCP** | Primary Care Provider |
| **PHI** | Personal Health Information |
| **PHN** | Personal Health Number |
| **PI** | Personal Information |
| **PIA** | Privacy Impact Assessment |
| **SIA** | Security Impact Assessment |
| **SMS** | Short Message Service  or text message |

## Related documents

- Health Myself Privacy Policy
- Health Myself End User Agreement

## Contact

For questions pertaining to details in this document, please email privacy@healthmyself.ca

# General Description

The Health Myself Patient Portal is a web-based, highly configurable Patient Portal application that provides physicians and clinic staff with a cloud hosted digital platform to connect clinics with their patients and patient caregivers.

## 1. General Attributes

The general attributes of the HMPP can be described as follows:

- Presentation: The system provides a comprehensive set of tools for capturing, searching, formatting and displaying patient and clinic data.

- Access Control: The application provides the ability to limit and control access to patient specific data and functionality using specific parameters, including: user permissions, role permissions, type of information, specific patient masking and specific item masking.
- Data Provision: Different types of patient data are encrypted and securely stored within the database and data repository including: text based information, photographs, scanned images, and electronic documents.
- Consent Management: HMPP provides mechanisms to record a patient's consent to application service terms and conditions
- Authentication: The system provides mechanisms to authenticate users with username, password, and users may optionally configure their account to require a second factor.
- Patient Preferences: HMPP supports patient directives relating to the security and communications. Patients may choose to: Share proxy control over eBooking and messaging with another Health Myself Account, Receive SMS notifications, Require 2 factor authentication for their account
- Attachments: Digital files may be included in patient messages.
- Correction: Data corrections and annotation may be requested by a patient
- Search Capability: Patients are searchable by last name (exact, partial or), first name (exact, partial or phonetic), PHN, user-defined registration numbers, chart number, full or partial date of birth, aliases, phone numbers and multiple other demographic fields in multiple combinations.
- Audit: The access, creation or revision of patient information as well as other user actions is recorded in an audit trail.
- EMR Connectivity: The Health Myself Patient Portal is certified to integrate with the TELUS Health Exchange EMR API, to securely connect the HMPP with the clinics EMR system to synchronize patient demographic data, clinic schedules, appointment bookings and patient messages.
- Patient Identification: System-to-system access to source electronic medical record system via TELUS provided Application Programming Interface (API).

## 2. Patient Onboarding and Patient Account Management

- Patient onboarding: The HMPP queries the clinic source EMR using predefined criteria for a list of patients whose demographic information will then be used to create records in the HMPP. Alternatively, users can manually enter Patient demographic information to generate the email invitation
- Patient Registration: Patients receive an email invitation with a time-sensitive link. After accessing the link they must verify their identity through a combination of demographic details and shared secret as configured by clinic policy
- Patient Account Management: Patients can manage their HMPP accounts including username, password, primary email address, and communication preferences.
- Patient Connections: patients may choose to connect their account to that of another user, to allow a caregiver to book appointments, message or receive reminders for their account. Patients may explicitly connect their account to that of another patient who may accept the caregiver role, or clinic users may connect 2 accounts, in accordance with clinic policies.

## 3. eBooking

- Provider Appointment Types and locations: clinics will store information in the system related to the types and locations they will be making available for eBooking availability
- Provider availability: HMPP will query the providers EMR schedule to determine provider availability for patient eBookings
- Appointment Reminders: HMPP will send email reminders to patients in advance of their appointment, the content and timing of which can be configured by the clinic. Clinics might also choose to engage SMS reminders in advance of patient appointments. SMS reminders are sent only if patients have opted in to receive SMS text reminders.

## 4. Patient Messaging

- Clinic initiated messages: Clinic providers and staff may initiate a conversation with a patient or caregiver, and may also archive or conclude the conversation thread.
- Patient initiated messages: Clinic can allow patients to initiate messages to the clinic, and may set up clinic staff as individuals or groups to receive patient messages
- Read receipts: Messages to patients can be tracked for follow up if not read
- Save to chart: Messages can be saved into the patients chart in the EMR
- Attachments: Clinic users can include attachments that may contain PHI in patient messages. HMPP presents clinic users with warnings to ensure the attachment has been verified for the intended audience and is being directed appropriately. Clinics may allow patients to attach files in Patient generated messages.

## 5. Notifications

- Broadcast Notifications: Clinics can create newsletters or other group communications for their patients, with information that excludes PHI. Clinics can choose to present this information to patients in an email that does not require authentication.
- Targeted Notifications: Clinics can create targeted, secure communications for specific cohorts e.g. patients who require preventative care. Communications of this nature could imply PHI, and patients email would indicate there is a notification waiting for them. Depending on settings, the email would either include a one-time access link or a link prompting them to authenticate before they can access notifications. Clinic users may identify cohort of patients using criteria in the EMR, and import the list of patients to create a patient group in the HMPP, which will determine patient eligibility for receiving the notification.

## 6. Proxy Accounts

- Connected Accounts: HMPP has the ability to connect user accounts so that caregivers can act (manage appointments or message) on behalf of a dependent. Use of this functionality is completely optional and some clinics choose not to enable connected accounts. Portal users with connected accounts can revoke permissions for the Proxy to act on their behalf at any time. Dependents who do not have their own account can contact the clinic and ask that the Proxy access be discontinued. Clinics should establish clear protocols and policies with respect to proxy accounts and ensure staff is trained in their application. The granting and revocation of proxy rights is documented in the audit logs.
- Mature Minor: HMPP has support to automatically expire parental/guardian access at a specific configurable age, after which the dependent patient would have to provide explicit consent to

act as a proxy on their account. We strongly advise clinics to articulate a clinic wide Mature Minor Policy to help parents appreciate that it is in the best interest of their child's health to have a confidential relationship with their Health care provider when they are sufficiently mature to have need of such privacy.

## 7. Consent and Terms of Use

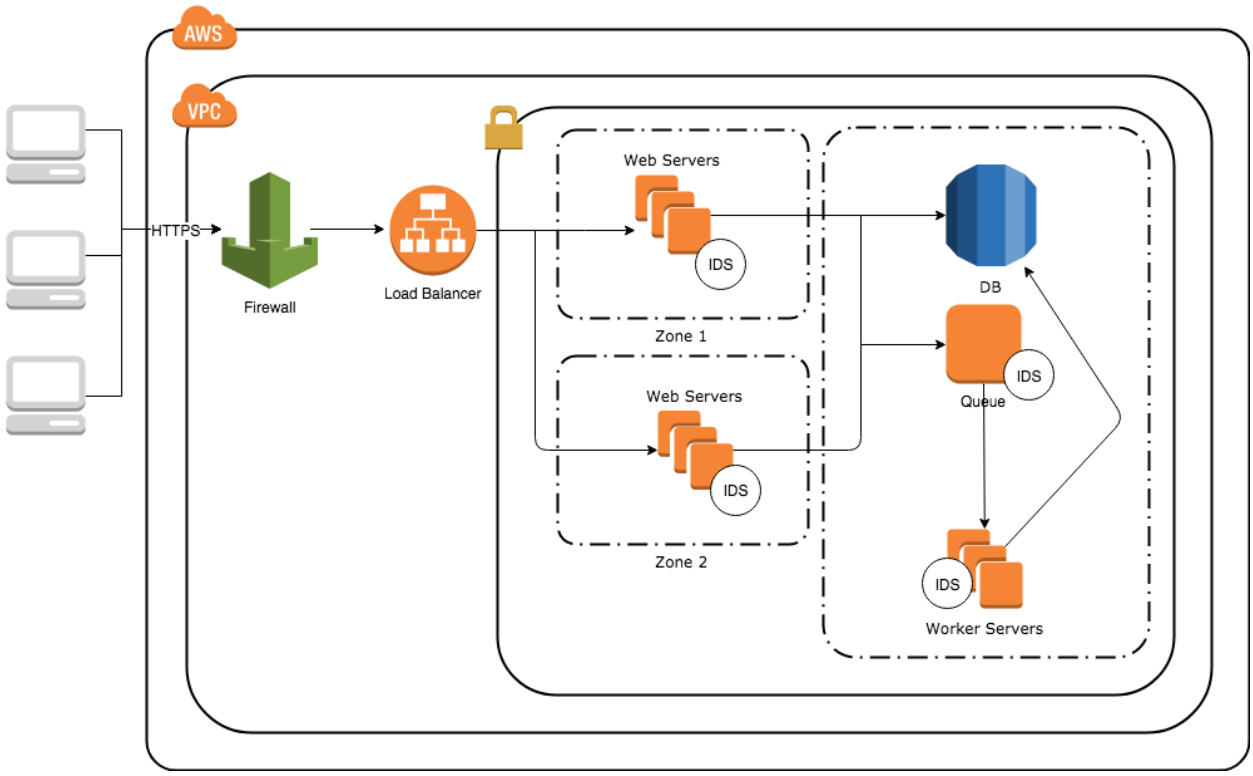
- Consent: Invitations to HMPP are sent to prospective patient users via email. Clinics capture consent to use email (implied or explicitly) when the email address is collected and stored in the EMR. Prospective portal users may decline the invitation to join the portal, and will be put on a do not contact list and not contacted via HMPP thereafter.
- Terms of Use: When registering for HMPP, prospective users are prompted to read and accept the HMPP terms of use, which can be found here. Users must accept the terms and conditions to use the service.

## 8. Records Management

Health Myself Innovations Inc. does not automatically delete or archive records unless explicitly requested by clients or portal users. HMPP will accommodate clinic policies for records management as requested by clients.

- Termination by Patients: If a Patient closes their account, Health Myself will inform Health Care Provider about the Patient's decision and give Health Care Provider 90 days to copy relevant Patient records and content into their EMR or internal system. After such 90 days, Health Myself will delete the Patient's records from the Portal.
- Termination by Provider or Clinic: As data custodians, Providers, will have their own policies with respect to records retention. Health Myself Innovations Inc. will work with clinics to accommodate their policies for records management as requested.

## 9. System Topography



## Personal Information Elements

Data elements that are collected or displayed are identified below.

| Category | Type | Description | Data Elements |
|---|---|---|---|
| **Demographic Information** | PI/PHI | Information about the patient's identity, dwelling, contact information etc. | Patient name<br>Patient date of birth<br>Patient address<br>Patient Telephone number(s) – home, work, cell<br>Personal Health Number<br>Gender<br>Patient's Provider Name<br>Patient Groups<br>Email address |
| **Appointment Schedule** | PI/PHI | Information about the patients upcoming appointments | Appointment date & time<br>Location of Service<br>Appointment Provider<br>Reason for Service<br>Appointment Notes or Comments<br>Associated Appointment Type ID |
| **Patient Messages** | PI/PHI | Information relating to the exchange of messages within the portal. This can include PHI disclosed as part of the message content. | Patient ID<br>Clinic Recipient User or Group<br>Message Subject/Body, unstructured data may include PHI |
| **Notifications** | PI/PHI | Bulk communications may contain PHI where a patient is identified as a member of a cohort, and this cohort may have been defined based on patient demographic data as described in the HMPP, or the list of patients may have been generated by clinical data in the source EMR. (e.g. patients overdue for preventative care procedure). | List of qualifying patients based on clinic criteria<br>Patient ID |
| **Connected Accounts** | PI | HMPP users have the option to invite other users to perform portal activities on their behalf. (e.g. allow family members to booking appointments or message with the clinic on behalf of a dependent) | Contact Relationship<br>Explicit permissions for Proxy user (allow eBooking/ Messaging/Notification) |
| **Provider Information** | PI | In order to facilitate the above services, Clinic and provider information is also captured. | Provider Name<br>Provider Credentials<br>Provider Phone<br>Provider Address |

# Information Flows

The information flow between EMR and Portal is bi-directional. Information typically originates from a provider in the EMR and flows to the Portal for consumption by a patient, however, the opposite is also possible. Patients may generate information in the Portal that will then flow into the EMR.

In the course of interacting with the clinic, the patient provides patient demographic information, which is typically entered into the EMR, and subsequently imported by HMPP to generate account registration information. HMPP invites patients to register for the portal, and patients may choose to decline and not be further contacted by HMPP.

Health Myself staff provide "Remote Help Desk" technical support to patients, providers and their staff in connection with troubleshooting issues that arise from the operation of the HMPP. As a result, such Health Myself support staff may access profile information.

Providers and staff at clinics receive messages with or without attachments in connection with the communication provision of healthcare services.

## 1. Sources of Information

Information may be generated by clinic providers or staff users or imported and synchronized from the source EMR. Messages would be created and accessed by patients, providers and/or provider staff. Patients may also update/correct their demographics/contact information through the HMPP.

## 2. Outflows of Information

Information may flow out through the interfaces described above (e.g. clinic EMR system, patient emails).
This does not include information imported into templates, attached via messaging or otherwise provided to patients, other providers, or third parties. Information may also be disclosed to Health Myself personnel as part of support activities.

## 3. Information Flow Diagrams

### HMPP and EMR Integration Overview

*For more detail on the hosting, architecture and security of the TELUS EMR API, please contact your TELUS Health Account Rep and request the TELUS EMR API Security Whitepaper.*

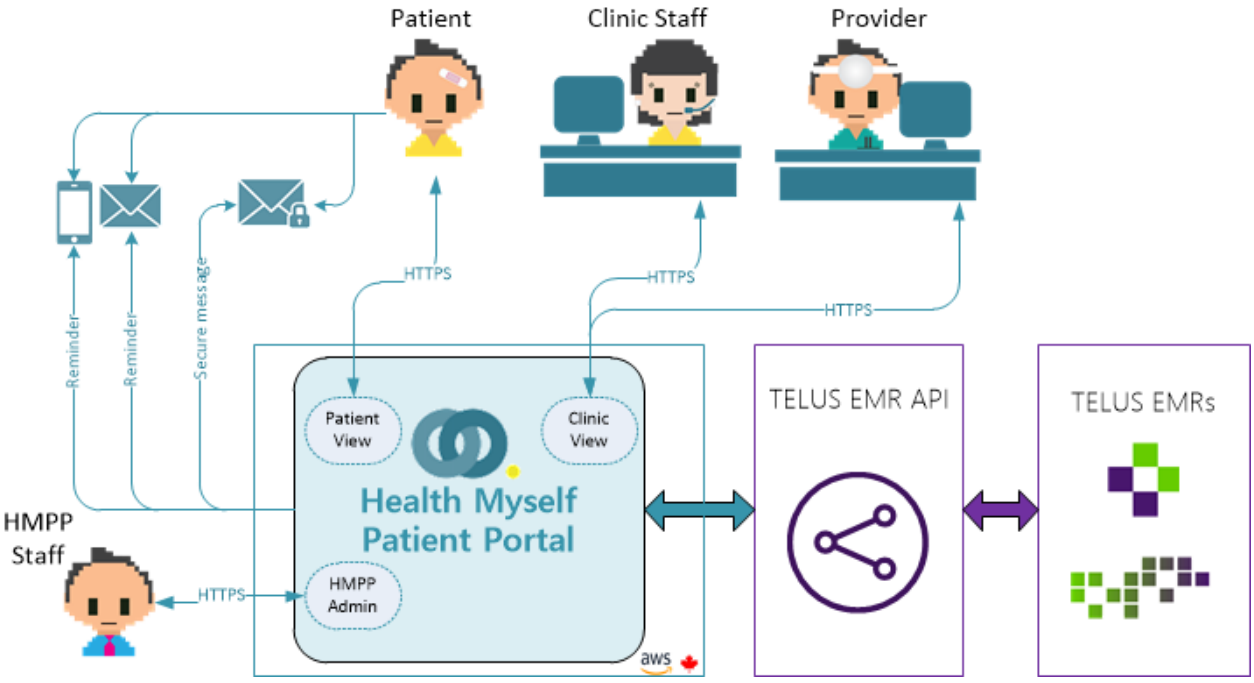



*Figure 1 HMPP and EMR Integration Overview*

## Patient Onboarding and Registration

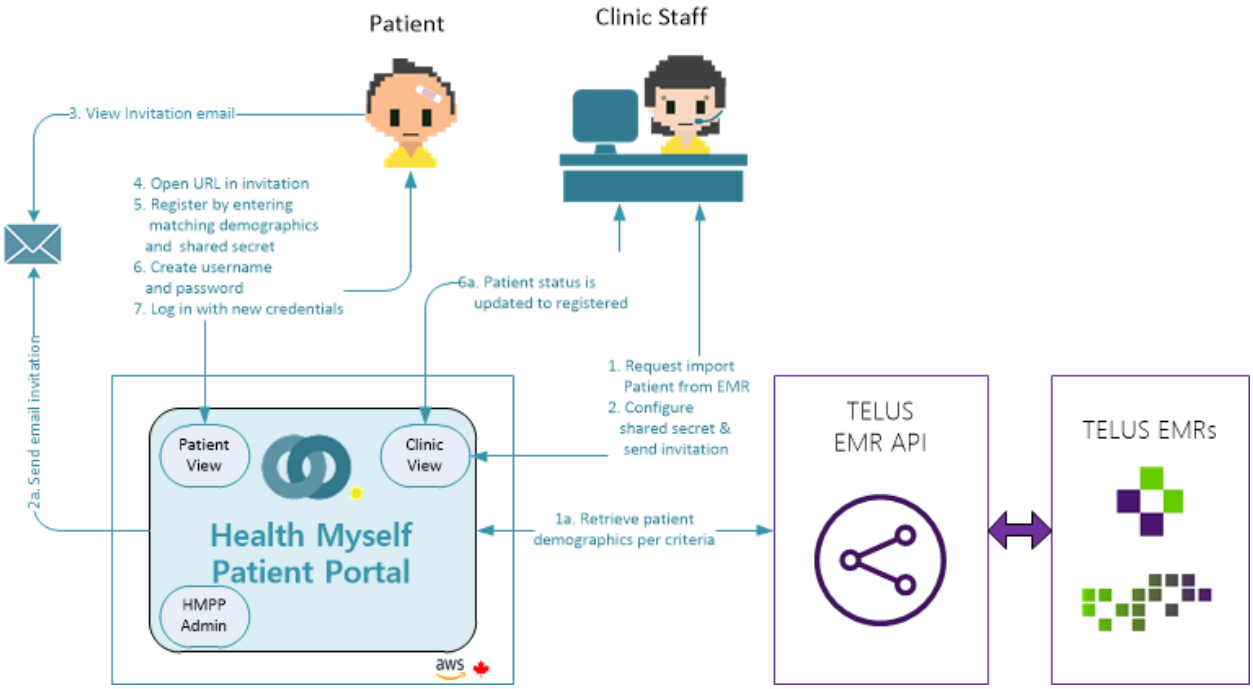



*Figure 2 Patient Onboarding and Registration*

## Patient eBooking

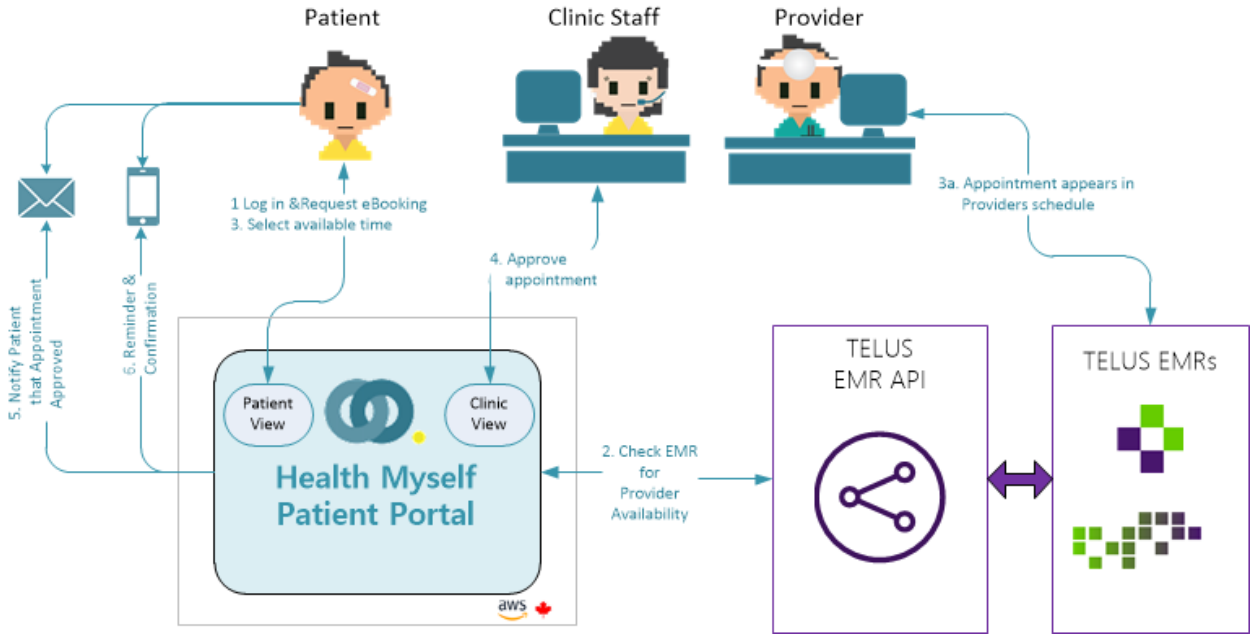



*Figure 3 Patient eBooking*

## Patient Messaging

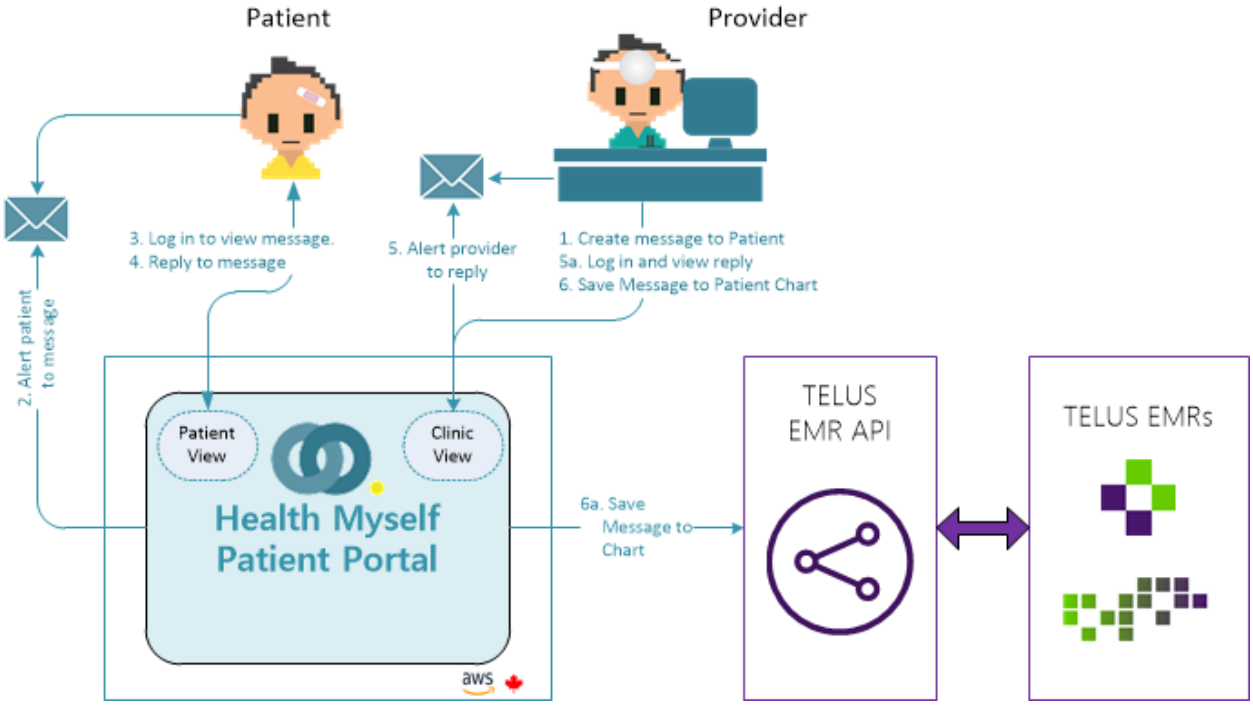



*Figure 4 Patient Messaging*

## Notifications

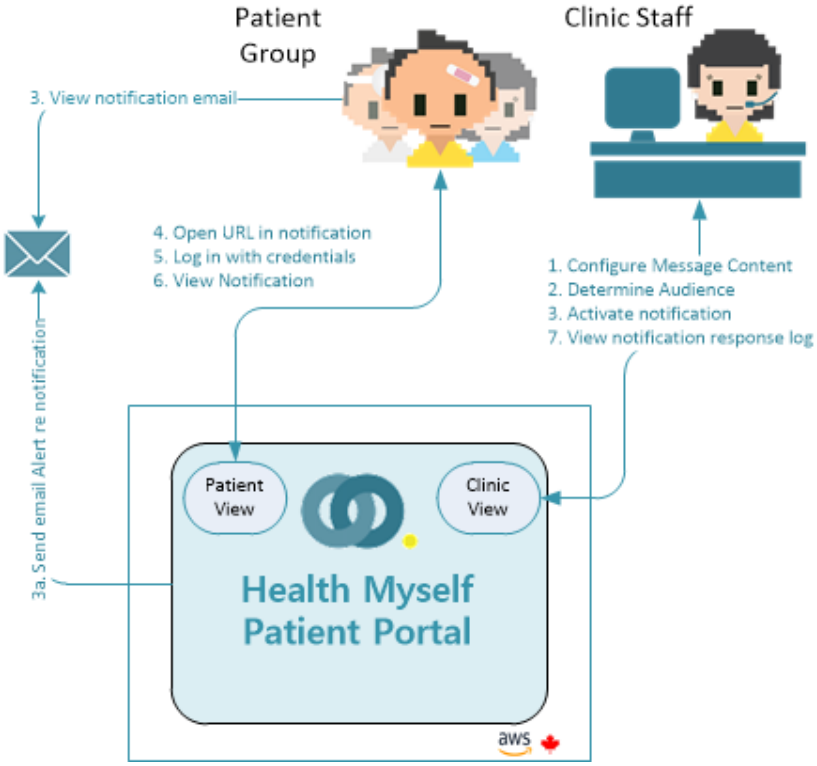



*Figure 5 Notifications*

## Access

As partners of TELUS, Health Myself personnel are covered by the clinic's Information Manager Agreement with TELUS. The following are job roles or job functions for Health Myself employees/ contractors and agents that will have partial access to PI/PHI.

- Help desk personnel and managers.
- Implementation personnel and managers.
- Programmers assisting with non-routine troubleshooting.
- TELUS employees and contractors, who would be covered by the clinics TELUS Information manager agreement with the clinic.

For all Health Myself portal clinics Health Myself Innovations Inc maintains appropriate privacy and security policies and procedures in place to address:

- Employee access to, and use of, portal data and systems.
- Contractor access to, and use of, portal data and systems.
- Employee/contractor training and awareness.

All employees and contractors will sign the Employee/Contractor Privacy Agreement (Health Myself Security Policy, Appendix A) which includes a pledge of confidentiality and privacy. Prospective employees/contractors will not have access to collect or use patient health information or customer information. Reference checks, including trustworthiness with secure information, will be undertaken for all new employees and contractors. Employee and contractor criminal checks and security clearances shall be undertaken when appropriate.
Employee and contractor access to portal information is based on "need to know" and includes:

- Role based access rules appropriate to job duties and
- Unique user ID and passwords are required for all employees and contractors.

Employee and contractor education on the policy and procedures outlined in this document will be conducted during initial orientation and annually thereafter. Education will include:

- Information about health information principles and practice relating to health information issues, confidentiality and security;
- Information concerning the security vulnerabilities associated with the use of computer systems.

### 1. Account Provisioning

Account provisioning occurs as part of the implementation process. Each account is assigned to an individual working in a clinic/office environment and each individual is provided a unique alphanumeric username (identifier), with an internal numeric id stored for database. Health Myself project managers assist physician offices in determining portal roles, security settings, user groups and user delegations. Each user has a unique username and password, along with a role which has certain permissions associated with it. The Health Myself system can restrict functionality (administrative or configuration capabilities) by type of functionality and tasks (based on assignment).

- Encrypted access
- User passwords stored in database

- Two-factor authentication
- Configurable automatic log off for inactive sessions.
- Location specific login restrictions.

### 2. Support and Implementation Services

Health Myself provides technical support services to patients and clinic users .Support calls are entered into the Health Myself CRM system. All customer contact is recorded and tracked. Support staff are required to document all information received and outcomes within the Health Myself CRM including, reasons for remote access to the physician's site.

For typical support requests, Health Myself Staff never have access to PHI, however authorized Health Myself Staff may access a patient's basic demographic profile (Name, Age, Contact info) for the purpose of providing technical support.

Troubleshooting/resolution of issues may involve escalation and as a result other personnel and managers may access patient data. Such personnel would include implementation personnel and managers; programmers assisting with non-routine troubleshooting; and internal Health Myself technical support staff. Any personal health or other identifiable information obtained in the course of troubleshooting is to be destroyed following issue resolution.

During implementation, a clinic will designate a staff member as "Portal Administrator" the PA for clinic is responsible for provisioning and revoking access to the Portal for other staff members. This person is also responsible for validating and reviewing accounts.

## Collection, Storage, Retention

### 1. Disclosure

. Data from the patient portal can be matched to patient data in the EMR for the purposes of adding an appointment or archiving a message, to augment the user's health record.
HMPP will inform the appropriate regulatory bodies and/or contractual partners if any order, pursuant to any Foreign Disclosure Law is received.
All storage of Patient Personal Information will be within Canada.

Health Myself will not disclose or allow access or use of Patient Personal Information unless subject to court order. Health Myself staff provide cooperation with respect to investigations or inquiries of regulatory bodies and/or contractual partners.

Health Myself staff and/or designated subcontractors will protect equipment security, specifically cabling security and security of equipment off-premises, including:

- Protect power lines from unauthorized interception or damage.
- Protect communication cables from unauthorized interception or damage.
- Make sure that all off-site use of equipment is authorized.

Health Myself staff establish and maintain network controls, including:

- Controls to secure the information in computer networks.
- Controls to protect connected services from unauthorized access.

- Procedures to protect systems connected to public networks.
- Security controls are implemented, administered, monitored and communicated to all users.
- Audit information is available and reviewed.
- Appropriate information and training is provided to staff on security policy, programs and procedures.
- Employees and contractors will receive information on security policy, programs and procedures at the start of their employment/contract, upon any material change and annually.
- All employees and contractors will sign the Health Myself Employee Privacy Agreement.

Inter-provincial transmission of health information is required for our help desk in Ontario to access individually identifiable health information. Such transmission will be done over secure channels or consist of encrypted information.

### 2. Data Storage Security

- PHI is encrypted using the AES-256-CBC encryption algorithm
- Secure cryptographic keys are generated for each client programmatically
- Backups are performed nightly, are encrypted, and shipped to a secure offsite location (within Canada).
- PHI is only ever hosted in production, and never in staging or testing environments.
- Backups of clinic data are be maintained within Canada, and in encrypted format.

Health Myself typical backup schedule is:

- Daily backups no older than 48 hours
- Monthly backups are to be maintained for one year.
- Annual backups are maintained for two years.

## Security and System Controls

### 1. Security Assurance

Health Myself conducts annual risk assessments of its Patient Portal solution. All staff report security problems as indicated in a Privacy Breach procedure.
A Security/Privacy incident report is to be completed and submitted to management within 24 hours of an incident. Privacy and security-related responsibilities are set out in the document Organizational Policy – Security and Privacy.
The CEO is actively involved in HMPP product development (e.g. auditing, password management, etc.) and technical security controls (e.g. firewalls, intrusion prevention).

- User ID & authentication
- User Authorization (i.e. access controls)
- Audit logs
- Secure transmission (i.e. encryption)
- Intrusion detection
- Log management for unauthorized activity
- Log management for authorized activity
- System integrity tools

- Patch management

HMPP's audit log capabilities include: Tracks login attempts, password resets, ebooking requests and approvals, demographic information views and updates, message creation time, message read timestamp, email delivery report, email read receipt.

HMPP operates inside of a secure private network within the Amazon Web Services (AWS) cloud infrastructure. AWS is data (PHI/PI) agnostic, only managing the network infrastructure. AWS provides cloud infrastructure for countless other healthcare based companies including: The Ottawa Hospital ,Philips Healthcare, ZocDoc, Babylon, Novartis, Nextgen Healthcare, Icahn School of Medicine at Mount Sinai.

## 2. Data in Transit Security

All web-based interactions with the Health Myself Server are forced to use an HTTPS connection which uses 256-bit TLS encryption with 2048-bit encryption keys to secure data while in transit.

## 3. Network Security Features:

- Data resides within a private network with no public interface
- Network is protected by strict firewall polices and active intrusion detection
- Vendor-redundant DNS services in-place to help safeguard against DDoS attacks
- All system access is logged

## 4. Account Security

- Portal credentials are one way encrypted incorporating unique per hash salt to protect against rainbow table attacks.
- An adaptive iterative login function is used to prevent brute force attacks even with increasing computational power.
- 2-factor authentication and IP based login restrictions can be enabled on any account

## 5. Physical Security

HMPP is hosted in the AWS data centre located in Montreal, Canada. Physical security controls are present for a secured data facility. These include:

- Biometric and numeric codes to access the data centre;
- Secure equipment cages;
- Closed-circuit video monitoring;
- 24 hour/7 day security patrols;
- Access is recorded and auditable;
- Two separate power grids;
- Backup power is maintained on site;
- Redundant fiber connections from geographically distinct points;
- Data centre access is controlled and limited (currently identified as being limited to 2 Health Myself Innovations Inc. staff); and

## 6. Network security

Network security measures also exist. These include:

- System access controls;
- Firewall zones providing restrictive access controls;
- Intrusion prevention and detection software; and
- Anti-virus and malware scanning.

## 7. Application Security

Application security controls include:

- Account access is suspended for 10 minutes after 5 unsuccessful logins
- Password complexity controls implemented;
- “One-way” password encryption (SHA-256 algorithm);
- New clinic encryption keys are generated programmatically by the Health Myself Server and then encrypted using a master encryption key which is securely stored in a separate location on our private network.
- Each clinic has their own symmetric encryption key which is used to encrypt/decrypt PHI that rests in our database, ensuring data segregation and security.

## 8. Third parties/third party tools involved in solution delivery

- The cloud based Host Provider operates the hardware infrastructure that runs the Portal services, and stores PI/PHI in an encrypted state.
- The Email Service Provider sends out notification emails and appointment reminders but does not store PI/PHI.
- The SMS Service Provider sends out notification texts and appointment reminders but does not store PI/PHI
- There is also a possibility that certain application development projects associated with this initiative will be subcontracted to 3rd party, under the direction of Health Myself.

### 9. Personnel Screening and Training

All employees of Health Myself have,

- undergone criminal background checks,
- completed a PHIPA training course
- and completed Health Myself's internal security and privacy orientation

## Verification and Validation

### 1. TELUS Certification

- As part of the partner onboarding process, Health Myself must pass TELUS conformance testing for its integrations with the TELUS EMR API

### 2. Code Management & Backlogs

Health Myself uses an agile software development lifecycle to ensure the timely release of quality code to our production environment.

We keep two backlogs where all potential development activities are stored:

- **Product Backlog:** contains a list of new features, client feature requests and general feature enhancements.
- **Bug Backlog:** contains a list of known bugs that need fixing
-

Health Myself Innovations Inc. use a Git repository to manage code versioning and use the following branch strategy:

- **Master –** Current stable code for Production environment
- **Development –** Code currently being developed (branched from Master)
- **Release –** Code deemed almost ready for release (branched from Development and eventually merged back into Development and Master)
- **Hotfix –** Code for a critical bug fix (branched from Master and merged back into Development and Master)

### 3. Development & Release Process

Development cycles are driven by items in either our Bug Backlog or Product Backlog and prioritized as needed.

A regular development iteration goes through the following phases:

- **Gathering of requirements.** Define the requirements based on information contained in the backlog as well as stakeholder feedback.
- **Development.** Design and develop software based on defined requirements. Code will be contained in our Development branch.

- **Testing.** Versioned Release branch created from Development branch and code deployed to staging environment where testing is performed.
- **Delivery.** Release branch merged with Master and deployment to Production environment is scheduled. Any failed deployments will be result in a roll-back to the previous version.
- **Feedback.** Accept customer feedback to work into the requirements of the next iteration

## 4. Critical Bug Fixes

Critical bug fixes are expedited but generally handled using same tools and processes as other development tasks.