Health Myself Patient Portal

Health Myself Takes Privacy & Security Seriously

From the bottom up our system has been designed to safely, securely and reliably deal with highly sensitive data. Please see our **Privacy Policy** by following this link: **https://portal.healthmyself.net/privacy-policy/**

The following questions and answers will help alleviate any concerns:

Q: How do you protect the patient's personal health information (PHI)?
A: We use policies as well as technology to ensure the safeguard of your privacy. On the policy front, the Portal only sends out invitation to known individuals that are current patients of the clinic using our services. We also enforce a strong password minimum requirement to reduce risk. System activity is logged and monitored for suspicious activity, and audit trails are available.

On the technology side, all data going to and from our system is encrypted and transmitted over secure channels. All PHI is stored and transferred in an encrypted format. We provide an optional dual authentication technology on any account.

Q: How do you deal with account permissions among family members?

A: Our consent management policy is generally one-way in nature, meaning that a person can only give permission to someone else but not take it. So if a wife would like to manage her husband's Portal account, then the husband must give consent. The only caveat is that a parent/guardian of a child below 16 years can register on behalf of the child. Upon reaching 16 years of age, the permission is revoked and the child must register herself or to grant permission to the parent/guardian.

Q: Where is the location of your Data Centers where this solution is hosted? Are these data centers located:

a. In your own facilities and managed by your employees?
b. In your own facilities and managed by third party?
c. Collocated in data centre provider facilities and managed by your employees?
d. Collocated in data centre provider facilities and managed by third party?

A: Our data centre is located in Canada and the hardware infrastructure is managed by a trusted and reputable 3rd party. Our application and all sensitive data is managed and only accessible to Health Myself staff.

Q: Do your employees have access or can have access by the nature of their function (developer, database analyst, etc.) to sensitive data hosted on your systems? If so:

a. Do you perform criminal, credit and reference checks for all of your employees before you allow access to the systems containing patient data?
b. Do your employees sign NDA/Confidentiality agreements?
c. Do your employees accept terms and conditions requiring from them to comply with applicable regulatory requirements (FIPPA, PIPEDA and HIPPA)?

A: Company founders have limited access to Portal data. PHI is stored in an encrypted state cannot be accessed in an unencrypted format. The company has signed a service agreement with your medical clinic which binds the company to confidentiality. We have developed hiring policies that require our employees to sign NDA's, Confidentiality Agreements, and comply with all applicable regulatory requirements. Of course, we also perform criminal background checks on all candidates.

Q: Do you outsource to third parties any of the following aspects:

a. Development of your software?
b. Maintenance and support of your systems and infrastructure?
c. Physical security related to systems, infrastructure and data?

d. When is backup performed?

A: All of our software development has been done in house. We have partnered with a Canadian based hosting provider that specializes in managing sensitive data. They support and maintain our hardware and network infrastructures as their core competency.

The following is a portion of their policy on both physical and network security:

Each customer sits on their own private network, and has zero visibility into any other clients. In addition to be located within Tier 4 (high security) data centres, we also have internal security policies that we practice and maintain.

This includes:

- *SSH public/private key authentication in place of password authentication*
- *Databases reside on private network, not directly visible to the public network*
- *No vendor-supplied passwords are in use*
- *System access is continually logged*
- *Strict firewall policies for inbound connections*
- *Only authorized operations staff have access to your infrastructure*
- *Operations staff are subject to criminal background checks*
- *Operations staff are agnostic to data stored on the servers - customers retain ownership of their data at all times*
- *Operations team is in-house, and does not use 3rd party contractors*
- *Active intrusion detection is in place*
- *Vendor-redundant DNS services to safeguard against DDoS attacks*
- *Backups are performed nightly, are encrypted, and shipped to a secure offsite location that we maintain.*
- *Images of each server is ready and on standby to be activated on demand*

Q: Since you will be effectively custodians for hosting/transmitting sensitive personal and patient data – do you have insurance in place that will cover information security and privacy breaches and to what limits considering that each record breached usually cause $200 in direct and indirect cost?

A: We have extended cyber liability insurance that covers up to $1,000,000 in damages.

Q: Is your support 24x7x365? What are methods of accessing support (phone, Web, on-site, combination ….)?
A: Our official support hours are 9 - 5 Monday to Friday and can be accessed by email or phone (out-bound only) when necessary. We also have limited support outside of normal office hours.

Q: Does Health Myself include provisions for accountability in safeguarding of the information in compliance with applicable legislations and penalties in case that required controls are not in place?
A: Health Myself will provide Portal services in a manner consistent and fully compliant with general industry standards as well as fully comply with all requirements of PHIPA including, without limitation, the requirements set forth in Ontario Regulation 329/04, Section 6 and will: (i) not use or modify the PHI or disclose the PHI to any third parties; (ii) use commercially reasonable efforts to maintain the security and integrity of the Portal and its contents; (iii) promptly inform the medical clinic and the impacted patient of any violation and breach of security related to the services; (iv) provide support to both health care provider and patients during the normal service hours; and (v) use commercially reasonable efforts to make the Portal available twenty-four (24) hours a day, seven (7) days a week, except for: (a) planned downtime; or (b) any unavailability caused by a force majeure.

Q: In case the patient decides to stop using the Portal in the future, will you delete all of the patient's personal health information?
A: Under the Retention section of the Privacy Policy, we are obligated to inform the patient's medical clinic of the impending account closure and delete all personal health information within 90 days.