Purpose

The sharing of personal health information (PHI) is a core element of aTouchAway, a patient remote monitoring solution that provides support to a patient and their caregivers when receiving remote care and communicating with healthcare providers who are on the patient's care team.

Healthcare providers can be staff of a single healthcare organization, or they may be staff of other healthcare organizations. Where Aetonix provides the aTouchAway solution to enable two or more healthcare organizations to disclose patient PHI to each other, Aetonix may function as a health information network provider (HINP), a type of service provider under Ontario's *Personal Health Information Protection Act* (PHIPA) regulations, O. Reg. 329/04. As a HINP, Aetonix will work on behalf of health care providers to allow them to share important PHI about shared clients to better enable coordinated care.

Aetonix HINP services include:

- Enabling health care providers to use telemedicine application and share PHI to facilitate care provided to the patient with the support of the patient's caregiver;
- Safeguarding the PHI stored and managed in the system;
- Limiting use of PHI to only the purposes identified by Aetonix's clients in agreements and ensuring that staff only access the least amount of PHI required to meet the identified purpose;
- Logging and reviewing events and activities such as access to PHI and administrative actions;
- Coordinating the secure transmission of your PHI in the shared system between health care providers using third-party service providers vetted and closely monitored by Aetonix; and
- Maintaining an enterprise-wide privacy program to support Aetonix's compliance with the requirements of PHIPA and its regulations as well as our agreements with health care providers. We follow recognized standards in privacy, security and information management to safeguard your PHI more broadly. Below is a summary of our privacy program and practices for PHI.

Accountability for Privacy

Aetonix's Chief Privacy Officer is accountable for ensuring that Aetonix complies with its privacy obligations as a HINP to health care providers and any other privacy obligations identified in agreements with its clients and in its organizational privacy policies.

Aetonix Privacy Program

Aetonix has developed and implemented an enterprise-wide privacy program through which it has defined and meets its privacy obligations including those of a HINP where applicable.

The foundation of this program is Aetonix's Privacy and Data Protection Policy, which defines how Aetonix as a service provider to health care providers protects the privacy of people whose PHI is in the system that Aetonix manages and provides to health care providers.

Aetonix has developed and implemented the following measures to support the organization in meeting the requirements in its privacy policy:

- Privacy and information management procedures to ensure that Aetonix staff, contractors and third-party vendors appropriately limit their access to and use and retention of your PHI for the purposes of providing and managing the system and services;
- Privacy training and awareness for all new employees, with refresher privacy training provided annually;
- Processes for identification and management of privacy risks; and
- Privacy review activities to confirm that Aetonix complies with its privacy requirements including those of a HINP where applicable, including Privacy Impact Assessments and Threat Risk Assessments of the services.

Consent

Getting your consent to collect, use, and disclose your PHI is the responsibility of the health care provider that captures, accesses, and shares your PHI in the shared system.

If you want to withdraw your consent for your PHI to be accessed or shared, you must contact the health care provider that provided you with care or placed your PHI in the shared system.

Safeguards

Aetonix has implemented information security safeguards to protect your PHI in the shared system from unauthorized collection, use, disclosure, and retention. Key safeguards include, but are not limited to:

- Access controls on the shared system and other repositories of PHI (electronic and hard copy) to ensure that access to your PHI by staff, contractors and third-party vendors has been appropriately limited;
- Data protection measures, including protection (e.g., encryption) of your PHI when transmitted between health care providers and when stored in the shared system; and
- Network protections, including firewalls, intrusion detection and prevention measures, and anti-malware protections.

Your Privacy Rights

You must contact the healthcare provider that provides you with the health care that is documented in this system for the following privacy matters:

- Request a copy of your PHI in the system;
- Request access to information about how health care providers have been using, accessing, and sharing your PHI in the system;
- Request a correction to your PHI in the shared system; and
- Make a privacy inquiry or complaint about how the health care providers are managing and ensuring the privacy of your PHI in the shared system.

If you contact Aetonix regarding any of the above, we will redirect your request to the health care provider(s) that placed your PHI in the shared system.

Contacting the Privacy Officer

If you have a general inquiry or complaint about the service that Aetonix provides to health care providers or our privacy and security program contact the Aetonix Privacy Officer at:

by phone:
1 855 561-4591

by email:
privacy@aetonix.com

or by mail:

Aetonix
7 Bayview Road
Ottawa, Ontario
Canada
K1Y 2C5

You can also contact Information and Privacy Commissioner of Ontario at (416) 326-3333 for privacy inquiry or complaint. See more information at: https://www.ipc.on.ca/