PHIPA PRIVACY POLICY

Privacy of personal information is an important principle to Maple Forest Family Physicians. We are committed to collecting, using and disclosing personal information responsibly and only to the extent necessary for the services we provide. We try to be open and transparent about how we handle personal information. This document describes our privacy policies.

What is Personal Health Information?

Personal health information is information about an identifiable individual. Personal health information includes information that relates to:

- the physical or mental health of the individual (including family health history);
- the provision of health care to the individual (including identifying the individual's health care provider);
- community and home care services;
- payments or eligibility for health care or coverage for health care;
- the donation or testing of an individual's body part or bodily substance;
- the individual's health number; or
- the identification of the individual's substitute decision-maker.

What regulations apply with respect to my information?

The *Personal Health Information Protection Act of 2004* (PHIPA) regulates the manner in which personal health information may be collected, used and disclosed within the health sector in Ontario.

Who We Are

Our organization, *Khan Ryan Medical Inc.*, operating as Maple Forest Family Physicians, acts as custodian of Personal Health Information, and includes at the time of writing two family physicians and one member of support staff. We use a number of consultants and agencies that may, in the course of their duties, have limited access to personal health information we hold. These include computer consultants, office security and maintenance, bookkeepers and accountants, lawyers, temporary workers to cover holidays, credit card companies, website managers and cleaners. We restrict their access to any personal information we hold as much as is reasonably possible. We also have their assurance that they follow all appropriate privacy principles.

Our office address is;
1801 Rutherford Road
Vaughan, Ontario
L4K 5R7

Why We Collect Personal Health Information

We collect, use and disclose personal information in order to serve our patients. For our patients, the primary purpose for collecting personal health information is to provide routine general healthcare services. For example, we collect information about a patient's health history, including their family history, physical condition and function, and social situation in order to help us assess what their health needs are, to advise them of their options and then to provide the health care they choose to have. A second primary purpose is to obtain a baseline of health and social information so that in providing ongoing health services we can identify changes that are occurring over time.

We also collect, use and disclose personal health information for purposes related to or secondary to our primary purposes. The most common examples of our related and secondary purposes are as follows:

1. To obtain payment for services or goods provided. Payment may be obtained from the individual, OHIP, WSIB, private insurers or others.
2. To conduct quality improvement and risk management activities. We review patient files to ensure that we provide high quality services, including assessing the performance of our staff. External consultants (e.g. auditors, lawyers, practice consultants, voluntary accreditation programs) may conduct audits and quality improvement reviews on our behalf.
3. To promote our clinic, new services, special events and opportunities (e.g. a seminar or conference) that we have available. We will always obtain express consent from the patient prior to collecting or handling personal health information for this purpose.
4. To comply with external regulators. Our professionals are regulated by the College of Physicians and Surgeons of Ontario, who may inspect our records and interview our staff as a part of its regulatory activities in the public interest. The CPSO has its own strict confidentiality and privacy obligations. In addition, as professionals, we will report serious misconduct, incompetence or incapacity of other practitioners, whether they belong to other organizations or our own. Also, our organization believes that it should report information suggesting illegal behaviour to the authorities. In addition, we may be required by law to disclose personal health information to various government agencies (e.g. Ministry of Health, children's aid societies, Canada Customs and Revenue Agency, Information and Privacy Commissioner, etc.).
5. To educate our staff and students. We value the education and development of future and current professionals. We will review patient records in order to educate our staff and students about the provision of health care.

Giving Consent

We require your consent to collect and process your data. In some cases we require your *express consent,* but in other cases *implied consent* is sufficient. When you choose to provide your personal health information to the practice, you provide implied consent for us to process this information for the purpose of providing health care. We may also infer implied consent to disclose this information to other health care providers within your circle of care for similar purposes.

In cases where we disclose your information for any other purposes, we will ask for express consent from yourself or a suitable substitute decision-maker to do so, apart from in certain exceptional circumstances such as if required by law or to prevent harm to yourself or others. For more information on the circumstances in which we may disclose your information, please see the guidance provided by the ICO.

You have the right to withdraw your consent at any time. If you do not consent to the collection or disclosure of your personal health information or some part of it, you should discuss this with your Physician or the Practice Manager. If you withdraw your consent after it has already been collected or disclosed, this will not apply retroactively, but we will cease collecting or disclosing your information in future cases.

Protecting Personal Information

We understand the importance of protecting personal information. For that reason, we have taken the following steps:

- Paper based records are not to be created or retained wherever possible. Any paper records containing personal information are to be kept either under supervision or secured in a locked or restricted area, and destroyed as soon as possible after use.
- Personal Health Information is not to be stored on site wherever possible, and instead resides in secure cloud storage provided by our Electronic Service Provider. We use Telus Health to store and process your data. For more information on Telus Health CHR, please review their privacy policy.
- Where a local digital copy of any patient health information is created, this is to be secured using strong encryption and only retained as long as necessary for processing or review before being securely deleted or transferred.
- Electronic hardware providing access to patient information is either under supervision or digitally secured at all times. In addition, strong passwords and/or biometric security measures are used on all computers and mobile devices.
- Electronic information is either anonymized or encrypted before being transmitted. Personal Health Information is not to be transmitted via unencrypted email. Patients are requested not to transmit personal health information to the practice using any unencrypted electronic system and any such information received is to be securely deleted.

- Transfer of paper information is to be avoided wherever possible. Where paper records must be processed in this way, they are to be transferred through sealed, addressed envelopes or boxes by reputable companies with strong privacy policies.
- Our staff members and any contractors are trained to collect, use and disclose personal information only as necessary to fulfil their duties and in accordance with our privacy policy.
- We do not post any personal information about our patients on social media sites and our staff members are trained on the appropriate use of social media sites.
- External consultants and agencies with access to personal information must enter into privacy agreements with us.

Retention and Destruction of Personal Information

We need to retain personal information for some time to ensure that we can answer any questions you might have about the services provided and for our own accountability to external regulatory bodies. In accordance with our obligations we keep our patient files for at least ten years from the date of the last patient interaction or from the date the patient turns 18, or until these records are transferred to an alternative custodian.

We destroy paper files containing personal health information by cross-cut shredding. We destroy electronic information by deleting it in a manner that it cannot be restored. When hardware is discarded, we ensure that the hardware is physically destroyed or the data is erased or overwritten in a manner that the information cannot be recovered.

Accessing your Information

With only a few exceptions, you have the right to see what personal information we hold about you, by contacting the Practice Manager. We can help you identify what records we might have about you. We will also try to help you understand any information you do not understand (e.g., short forms, technical language, etc.). We will need to confirm your identity, if we do not know you, before providing you with this access. We reserve the right to charge a reasonable fee for our costs in providing this information in line with current guidelines.

We may ask you to put your request in writing. We will respond to your request as soon as possible and generally within 30 days. If we cannot give you access for any reason, we will tell you the reason, as best we can, as to why.

Correcting your Information

If you believe there is a mistake in the information, you have the right to ask for it to be corrected. This applies to factual information and not to any professional opinions we may have formed. We may ask you to provide documentation that our files are wrong. Where we agree that we made a mistake we will make the correction. At your request and where it is reasonably possible, we will notify anyone to whom we sent this information (but we may deny your request if it would not reasonably have an effect on the ongoing provision of health care). If we do not agree that we have made a mistake, we will still agree to include in our file a brief statement from you on the matter.

If there is a Privacy Breach

Whilst we will take all practical precautions to avoid any breach of your privacy, in the event of a loss, theft or unauthorized access of your personal health information we will notify you as soon as possible.

Upon learning of a possible or known breach, we will take the following steps:

- We will contain the breach to the best of our ability, including by taking the following steps as applicable;
- Recovering any physical copies of personal health information that have been disclosed
- Ensuring no copies have been made
- Taking steps to prevent unauthorized access to electronic information (e.g., changing passwords, restricting access, temporarily locking down or disabling systems)
- We will notify affected individuals
- We will provide our contact information in case the individual has further questions
- We will provide the Commissioner's contact information and advise the affected individual of their right to complain to the Commissioner
- We will investigate and remediate the problem, by;
    - Conducting an internal investigation
    - Determining what steps should be taken to prevent future breaches (e.g. changes to policies, additional safeguards)
    - Reviewing staff training and conducting further training if required

Depending on the circumstances of the breach, we may notify and work with the Information and Privacy Commissioner of Ontario. We may also report the breach to the relevant regulatory College if we believe that it was the result of professional misconduct, incompetence or incapacity.

Marketing Information

From time to time, we may contact you with updates and information about the practice which we feel might be useful to you. Receiving this information is always optional and you can request to be removed from any mailing lists at any time.

Use of the Practice Website

You may visit our website at mapleforestfamilyphysicians.ca without providing any personal health information. If you choose to book appointments online, you may be asked to provide such information, however this will be collected directly by our Electronic Service Provider and not collected or retained on our servers. When you visit our website, our servers and third parties providing web services may collect certain cookie information from your browser to identify your computer and provide a record of visitors to the website. You can choose to set your browser to disable or refuse to accept cookies, however this may affect your viewing of some parts of the website.

Do You Have Questions or Concerns?

Our Information Officer, Laura Coffa, can be reached at: l.coffa@mapleforestfamilyphysicians.ca. She will attempt to answer any questions or concerns you might have.

If you wish to make a formal complaint about our privacy practices, you may make it in writing to our Information Officer. She will acknowledge receipt of your complaint, and ensure that it is investigated promptly and that you are provided with a formal decision and reasons in writing.

You also have the right to complain to the Information and Privacy Commissioner of Ontario if you have concerns about our privacy practices or how your personal health information has been handled, by contacting:

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
M4W 1A8

Telephone: (416) 326-3333

This policy is made under the *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3. It is a complex statute and provides some additional exceptions to the privacy principles that are too detailed to set out here.