Personal Information Privacy Policy

Privacy of personal information is an important principle to HamSMaRT. We are committed to collecting, using and disclosing personal information responsibly and only to the extent necessary for the goods and 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.

Who We Are

- Our organization, HAMSMaRT, includes at the time of writing 6 professionals and 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 and website managers. We restrict their access to any personal information we hold as much as is reasonably possible. We also have their assurance that they follow appropriate privacy principles.

Why We Collect Personal Health Information

We collect, use and disclose personal information in order to serve our clients. For our clients, the primary purpose for collecting personal health information is to provide healthcare. For example, we collect information about a client'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:

Related Purpose #1: To obtain payment for services or goods provided. Payment may be obtained from the individual, OHIP, WSIB, private insurers or others.

Related Purpose #2: To conduct quality improvement, program evaluation, and risk management activities. We review client 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.

Related Purpose #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 client prior to collecting or handling personal health information for this purpose.

Related 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 College of Physicians and Surgeons 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.).

Related Purpose #5: To educate our staff and students. We value the education and development of future and current professionals. We will review client records in order to educate our staff and students about the provision of health care.

Related Purpose #6: To fundraise for the operations of our organization, with the express or implied consent of our clients. If we rely on implied consent, we will only use the client's name

and address, we will provide clients with an easy opt-out option, and we will not reveal anything about our client's health in the request.

Related Purpose #7: To facilitate the sale of our organization. If the organization or its assets were to be sold, the potential purchaser would want to conduct a "due diligence" review of the organization's records to ensure that it is a viable business that has been honestly portrayed. The potential purchaser must first enter into an agreement with the organization to keep the information confidential and secure and not to retain any of the information longer than necessary to conduct the due diligence. Once a sale has been finalized, the organization may transfer records to the purchaser, but it will make reasonable efforts to provide notice to the individual before doing so.

Protecting Personal Information

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

- Paper information is either under supervision or secured in a locked or restricted area.
- Electronic hardware is either under supervision or secured in a locked or restricted area at all times. In addition, strong passwords are used on all computers and mobile devices.
- Personal health information is only stored on mobile devices if necessary. All personal health information stored on mobile devices is protected by strong encryption.
- When we use your information outside of the office such as from home, we transport, use and store the personal health information securely.
- Paper information is transferred through sealed, addressed envelopes or boxes by reputable companies with strong privacy policies.
- Electronic information is either anonymized or encrypted before being transmitted.
- Our staff members are trained to collect, use and disclose personal information only as necessary to fulfill their duties and in accordance with our privacy policy.
- We do not post any personal information about our clients 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. However, in order to protect your privacy, we do not want to keep personal information for too long.

We keep our client files for at least ten years from the date of the last client interaction or from the date the client turns 18.

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.

You Can Look at Your Records

With only a few exceptions, you have the right to see what personal information we hold about you, by contacting [contact person]. 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 $30.00 for the first twenty pages of records and 25 cents for each additional page.

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 at all possible. If we cannot give you access, we will tell you the reason, as best we can, as to why.

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 point.

If there is a Privacy Breach

While we will take precautions to avoid any breach of your privacy, if there is a loss, theft or unauthorized access of your personal health information we will notify you.

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 if applicable
    - Retrieving hard 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., change passwords, restrict access, temporarily shut down system)
- 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)
    - Ensuring staff is appropriately trained and conduct further training if required

Depending on the circumstances of the breach, we may notify and work with the Information and Privacy Commissioner of Ontario. If we take disciplinary action against one of our practitioners [or revoke or restrict the privileges or affiliation of one of our practitioners] for a privacy breach, we are required to report that to the practitioner's regulatory College. 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.

Do You Have Questions or Concerns?

Our Information Officer can be reached at:

Nala Ismacil, 822-426-7678 x1 or clinics@hamsmart.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/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8

Telephone: Toronto Area (416/local 905): (416) 326-3333

Long Distance: 1 (800) 387-0073 (within Ontario)
TDD/TTY: (416) 325-7539
FAX: (416) 325-9195
www.ipc.on.ca

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.