EveryMind Privacy Code

Introduction

EveryMind respects the privacy of the personal health information of children, youth, and young adults. That is why we have developed the EveryMind Privacy Code. The objective of the EveryMind Privacy Code is to promote responsible and transparent personal information management health practices in a manner consistent with the provisions of the Ontario *Personal Health Information Protection Act, 2004, as well as the Child, Youth and Family Services Act, 2017 Part X.*

The EveryMind Privacy Code is a statement of the privacy and information practices which we follow in order to protect an individual's personal health information. We will continue to review the Privacy Code to make sure that it is relevant and remains current with changing industry standards, technologies and laws.

Scope and Application

This Privacy Code applies to personal health information collected, used, or disclosed by EveryMind in the course of providing mental health assessment, treatment and support services to children, youth, and young adults from birth to twenty-five years of age.

Personal health information is information in any form that identifies an individual and that relates to an individual's health and health care including name, address, gender, age, health history, health care programs and services, health care providers, substitute decision makers, health card number and other personal identification numbers.

The EveryMind Privacy Code in Detail

Collection and Use of Personal Health Information

EveryMind collects personal health information from and about our clients at the beginning of our involvement with clients and every time our clients visit us, for the primary purposes of providing direct care and treatment. Your personal health information is also used for the following purposes:

- ✓ Administration of Children's Mental Health Services
- ✓ Program Evaluation and Quality Improvement
- ✓ Accreditation
- ✓ Teaching and Training
- ✓ Research
- ✓ Fundraising
- ✓ Provision of Volunteer Services
- ✓ Legal, Funding, and Regulatory Requirements

Personal health information collected for the administration of direct clinical services includes, but is not limited to, name, contact information, date of birth, health card number and related mental health concerns and treatment.

By law, and in accordance with professional standards, EveryMind maintains a record of services to, and contact with, all clients. Client files may be an electronic and/or hard copy paper format and contain the following information:

- ✓ Intake Documentation
- ✓ Completed Clinical Reports, Plans and Service Summaries
- ✓ Contact Notes
- ✓ Other Internal Clinical Documentation
- ✓ Any Agreements with, and Correspondence sent to, external sources
- ✓ Reports and Correspondence received from external sources
- ✓ Observation Forms

EveryMind collects personal health information about clients directly from clients and their parents or from another person authorized to act on their behalf. Occasionally, we also collect personal health information about clients from other sources, including other care providers and schools, if we have obtained consent to do so or if the law permits. We will not collect personal health information if other information will serve the purpose. In addition, we will not collect more personal health information than is reasonably necessary to meet the purpose.

EveryMind maintains a website which is available to the public. EveryMind only collects personal information that is submitted voluntarily, such as address or other contact information that is provided to us via the website. The personal information we collect via the website is only used to respond to requests received via the website.

EveryMind specifies orally, electronically or in writing the identified purposes to the individual at or before the time personal health information is collected. Persons collecting personal health information will explain these identified purposes or refer the individual to a designated person within EveryMind who can explain the purposes.

When personal information that has been collected is to be used or disclosed for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is permitted or required by law, the consent of the individual will be acquired before the information can be used or disclosed for the new purpose.

Obtaining Consent for Collection, Use or Disclosure of Personal Health Information

EveryMind will only collect, use and disclose your personal health information with your consent or as required or permitted by law.

In obtaining consent, EveryMind uses reasonable efforts to ensure that an individual is advised of the identified purposes for which personal information will be used or disclosed. The identified purposes are broadly stated in a manner that can be reasonably understood by the individual and further information will be provided upon request.

Generally, EveryMind seeks consent to use and disclose personal health information at the same time it collects the information. However, EveryMind may seek consent to use and/or disclose personal health information after it has been collected, but before it is used and/or disclosed for a new purpose.

For consent to be valid, it must:

- relate to the treatment;
- be informed;
- be given voluntarily; *and*
- not be obtained through misrepresentation or fraud.

In addition, consent is only valid if it is obtained from a capable person. To be capable of consenting, a person must be able to understand the information relevant to make the decision; and appreciate the reasonably foreseeable consequences of giving, withholding or withdrawing consent. If a person is not capable of making a decision about their information, it will be necessary to obtain consent from a substitute decision-maker, as determined by law.

Where EveryMind needs to collect, use, or disclose personal health information from a child under 16 years of age, a parent or other legal guardian may consent even if the child has the capacity, unless the information relates to counseling in which a child 12 years of age or older has participated on his/her own under the Child Youth and Family Services Act, 2017 pursuant to section 23. However, if there is a conflict between the child and the parent, the capable child's decision prevails.

For youth over 16 years of age who have the capacity to consent, consent to the collection, use or disclosure of personal health information must be obtained from the youth. In addition, for children 12 years of age or older who have sought or are receiving counselling on their own, as per the Child, Youth and Family Services Act, 2017 s. 23, consent for the collection, use or disclosure of personal health information must be obtained from the child.

For children who do not have the capacity to consent, the parents or authorized substitute decision maker including the properly appointed custodial parents may give consent. Properly appointed custodial parents are those set out in a separation agreement or court order or guardian appointed under the Children's Law Reform Act.

In determining the appropriate form of consent, EveryMind takes into account the sensitivity of the personal health information and the reasonable expectations of the individual.

Where we are collecting, using or disclosing personal health information for health care purposes, the law normally permits us to rely on implied consent. Implied consent can be determined where the surrounding circumstances allow us to make a reasonable determination that the client or a person authorized to act on their behalf would agree to the collection, use or disclosure.

If the purpose for which we are collecting, using or disclosing information is something other than health care of our client or involves the disclosure of personal health information to someone other than a health information custodian, we will normally obtain express consent.

Unless we receive instructions to the contrary, we may disclose our clients' personal health information to other health care providers in their "circle of care", who need to know certain information to help provide our clients with care. The "circle of care" includes health care professionals, pharmacies etc. who provide care to our clients.

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Individuals may contact EveryMind for more information regarding the implications of withdrawing consent.

In addition, specific instructions may be provided that certain personal health information in a client's record of personal health information is not to be used or disclosed. If we believe that the withdrawal or

limiting of consent may compromise client care, we will convey our concerns to the client or a person authorized to act on their behalf.
EveryMind may collect or use personal health information without knowledge or consent if it is clearly in the interests of the individual and consent cannot be obtained in a timely way, such as when the individual is seriously ill or mentally incapacitated.

EveryMind may collect, use or disclose personal health information without knowledge or consent in some circumstances, such as:

- in the case of an emergency where the life, health or security of an individual is threatened;
- where we suspect certain types of abuse;
- to reduce a significant risk of bodily harm to a person or to the public;
- to assist professionals who do health research, as long as strict privacy requirements are met;
- for a legal proceeding, or to obey a court order or another legal requirement.

Limiting Use, Disclosure, and Retention of Personal Health Information

Only EveryMind's employees with a business "need-to-know", or whose duties reasonably so require, are granted access to personal health information about individuals. EveryMind does not disclose personal health information without an individual's consent unless it is permitted or required by law.

EveryMind keeps personal health information only as long as it remains necessary or relevant for the identified purposes or as required by law. Depending on the circumstances, where personal health information has been used to make a decision about an individual, EveryMind retains, for a period of time that is reasonably sufficient to allow for access by the individual, either the actual information or the rationale for making the decision.

EveryMind maintains reasonable and systematic controls, schedules and practices for information and records retention and destruction which apply to personal information that is no longer necessary or relevant for the identified purposes or required by law to be retained. Such information is destroyed, erased or made anonymous.

Where personal health information is to be disposed of, we will take reasonable steps to ensure that it is permanently destroyed. For paper records, permanent destruction means cross-cut shredding, pulverization or incineration. For electronic records, permanent destruction means either physically damaging the storage device to the point that it is not re-usable or utilizing wiping utilities that irreversibly erase the data. Where a third party is retained to dispose of personal health information, we will ensure that the third party signs a written agreement confirming that it will protect the security and confidentiality of personal health information and that it will permanently destroy the information in an expeditious manner.

Personal health information may be disposed of either on-site or off-site, depending on the circumstances. Where personal health information is disposed of, we will make every effort to ensure that both the paper and electronic versions are disposed of in a contemporaneous manner.

Access to Personal Health Information

A client or a person authorized to act on the client's behalf has the right to request access to a record of personal health information in our custody or control containing the client's personal health information. Such a request may be made by completing the "Request for Access" form. We will provide a response to all access requests within 30 days, although in certain legally permissible circumstances, we may inform the requestor that additional time may be required to provide a response.

Personal health information is provided in understandable form within a reasonable time, and at minimal or no cost to the individual.

The right to obtain access to personal health information is not absolute. In certain situations, EveryMind may not be able to provide access to all the personal health information that it holds about an individual. For example, EveryMind may not provide access to information if doing so would likely reveal personal health information about a third party or could reasonably be expected to threaten the life or security of another individual or themselves. If we refuse to provide access to a record of personal health information, written reasons will be provided.

Upon request, EveryMind provides an account of the use and disclosure of personal health information and, where reasonably possible, states the source of the information. In providing an account of disclosure, EveryMind provides a list of third parties to which it may have disclosed personal information about the individual when it is not possible to provide an actual list.

In order to safeguard personal health information, an individual may be required to provide sufficient identification information to permit EveryMind to account for the existence, use and disclosure of personal health information and to authorize access to the individual's file. Any such information is used only for this purpose.

Individuals can obtain information or seek access to their individual files by contacting the EveryMind Privacy Officer. A response is given within thirty days of the request.

Accuracy of Personal Health Information

EveryMind takes all reasonable steps to ensure that personal health information regarding our clients is as accurate, complete and up-to-date as possible, in order to minimize the possibility of inaccurate information being used to make a decision about a client. This includes reviewing the personal health information collected at the outset of service and regularly thereafter.

From time to time, we may seek to update certain personal health information about our clients, such as addresses and telephone numbers. We encourage our clients or persons authorized to act on their behalf to contact us with any changes to personal health information that may be relevant to our ability to provide timely and effective care.

We do not routinely update personal health information, unless such a process is necessary to fulfil the purposes for which the information was collected.

We promptly correct or complete any personal health information found to be inaccurate or incomplete.

Correction of Personal Health Information

Depending on the circumstances, a client or a person authorized to act on the client's behalf has the right to request correction to a record of personal health information in our custody or control containing the client's personal health information, which they believe is incorrect or incomplete. Such a request may be made by completing the "Request for Correction" form. We will provide a response to all correction requests within 30 days, although in certain legally permissible circumstances, we may inform the requestor that additional time may be required to provide a response

If we agree with a correction request, we will make every effort to record the correct information in the record and cross out the incorrect information, without obliterating it.

A request to correct records may be denied where:

- we are not satisfied that the record is incomplete or inaccurate for the purposes for which it uses the information;
- the request consists of a record that was not originally created by us and we do not have sufficient knowledge, expertise and authority to correct the record;
- the request consists of a professional opinion or observation that a health information custodian has made in good faith; or
- the request is frivolous, vexatious, or made in bad faith.

If we refuse to make the correction requested, written reasons will be provided.

Any unresolved differences as to accuracy or completeness are noted in a client's file. Where appropriate, EveryMind transmits to third parties having access to the personal health information in question any amended information or the existence of any unresolved differences.

Safeguarding Personal Health Information

EveryMind takes all necessary steps to ensure that personal health information in our custody or control is protected against theft, loss and unauthorized use, copying or disclosure. This includes personal health information in paper and electronic form. All EveryMind employees with access to personal health information are trained in the appropriate use, disclosure, and protection of personal health information.

Our methods of protection include the following:

a) *physical measures*
   - ✓ protecting the premises both by lock and alarm
   - ✓ locking offices that contain personal health information
   - ✓ storing all personal health information in locked filing cabinets
   - ✓ storing clients' paper files in a locked Clinical Records Room with access restricted to the Health Records Specialist or designated individuals

b) *administrative measures*
   - ✓ creating and implementing internal operational procedures regarding security including tracking all files within the organization
   - ✓ training staff regarding privacy responsibilities and reviewing this on a periodic basis
   - ✓ monitoring printers and fax machines at all times and ensuring that they are kept in secure areas
   - ✓ performing spot checks on a regular basis to ensure that security procedures are being complied with
   - ✓ establishing contracts with any third parties retained to store or dispose of personal health information

c) *technical measures*
   - ✓ requiring an individualized key to access all computers that store personal health information
   - ✓ encrypting any personal health information stored in electronic form on portable devices
   - ✓ running up-to-date anti-virus, firewall and spyware software on all computers that store personal health information
   - ✓ ensuring that no personal health information is stored on laptop computers and other electronic devices unless these are sufficiently secure and the information is encrypted
   - ✓ housing network servers in a locked computer room that is kept secure by a card reader system

- ✓ restricting access to the locked computer room to Information Technology staff or designated individuals

EveryMind requires organizations that perform services or provide programs on its behalf to protect the privacy of personal health information provided by EveryMind and to use that personal information only for the purposes that an individual has consented to or that is permitted or required by law.

Due to the nature of the internet, no data transmission over the internet is fully secure. Please be aware that EveryMind cannot guarantee that any information that is transmitted through email or its website will not be intercepted and/or misused by third parties.

EveryMind' website may from time to time contain links to other websites that may collect personal health information. EveryMind does not assume any responsibility for third parties' privacy practices or policies, and cannot be held liable for the actions of those third parties. The privacy policies of such third parties should be reviewed before you provide them with any personal information. We actively discourage email communication with clients unless it is the only means of communication and the client is made fully aware of the security concerns.

EveryMind will notify an individual at the first reasonable opportunity if an individual's personal health information is lost, stolen, or accessed by unauthorized persons (i.e., a privacy breach).

If a privacy breach occurs, we will make every reasonable effort to contain the breach, which includes locating and retrieving all personal health information outside of our control, as well as ascertaining whether other personal health information is at risk of exposure. We will then take any steps necessary to minimize the chances of a similar future breach.

Contact Information

If you are unhappy about something that has been done with your personal health information, we want to work out your concern with you. Please contact our Privacy Officer if you have any questions about our information practices, or would like to raise a privacy concern or report a privacy breach. Our Privacy Officer can be reached at:

Privacy Officer
EveryMind Mental Health Services
85A Aventura Court
Mississauga, ON L5T 2Y6
Telephone: (905) 795-3500 ext. 2647
Fax: 905-696-0350
*****Email: PrivacyOfficer@EveryMind.ca

We will answer your questions and will promptly investigate any concerns raised regarding this policy or a potential privacy breach. If an issue is found to have merit, we will take all appropriate measures including, if necessary, amending our policies and procedures. An individual shall be informed of the outcome of the investigation regarding his or her complaint.

Complaints to Information and Privacy Commissioner

If you are not satisfied with any decision reached by EveryMind regarding the handling of your inquiry or complaint, or wish to obtain general information about personal health information legislation, you may contact the Ontario Information and Privacy Commissioner. Although we will make every effort to provide an amicable resolution to all privacy concerns, PHIPA provides individuals with the right to complain to the Information and Privacy Commissioner of Ontario.

The Commissioner can be reached at:

Ontario Information and Privacy Commission
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Telephone: (416) 326-3333 or 1-800-387-0073
TTY: (416) 325-7539
Fax: (416) 325-9195
Website: www.ipc.on.ca
*****Email: info@ipc.on.ca

*****Note: Internet communications are not secure or verifiable so refrain from sending personal information by email.