

Letourneau Psychological Services Privacy Policy

Letourneau Psychological Services is the trade name for Jeffrey Letourneau Psychology Professional Corporation, solely owned and operated by Dr. Jeffrey Letourneau. My policies for protecting personal information are governed by the College of Psychologists of Ontario, the Regulated Health Professions' Act (RHPA, 1991), the Personal Health Information Protection Act (PHIPA, 2004), and parts of the Personal Information and Protection of Electronic Documents Act (PIPEDA, 2000).

What is Personal Information?

Personal information is information about an identifiable individual. Personal information includes information about my client's *personal characteristics* (e.g., gender, age, income, home address or phone number, ethnic background, family status). PIPEDA is federal legislation that establishes rules to govern the collection, use, and disclosure of personal information by organizations in the course of commercial activities. Health Information includes information that relates to *the physical or mental health of the individual* in oral or recorded form (e.g., health history, health conditions, information related to the provision of healthcare, a health number, or information that relates to payment or eligibility for healthcare). PHIPA is a provincial legislation that establishes rules to govern the collection, use, and disclosure of personal health information about individuals while providing healthcare. Generally speaking, the information I collect from clients is governed by PHIPA and not PIPEDA as PHIPA is deemed to be substantially similar to PIPEDA and because the personal information I collect is usually intertwined with health information, which is governed by PHIPA.

As a psychologist, I am considered a *health information custodian* under PHIPA. This means that I have custody and control of some of my client's personal health information. As such, I am bound by certain rules set out in the PHIPA legislation. For example, I must take reasonable steps to ensure that health information is as accurate, complete, and up-to-date as necessary for the purposes for which it is used and disclosed. I must also take reasonable steps to ensure health information in my custody is protected against theft, loss, unauthorized use, and disclosure and I must ensure that records of personal health information are protected against unauthorized copying, modification, or disposal.

Health Information: Primary Purposes

Like all psychologists, I collect, use, and disclose health information in order to serve my clients. The main reason for collecting and using personal and health information is for accurate identification and to provide quality assessment and treatment services. For example, I collect certain information about my client's history, including medical, psychological, family, employment, and social history, and current symptoms and status in order to best assess needs, and to provide treatment that my clients consent to receive. Another primary purpose is to have an initial baseline of health and social information and to monitor change over time.

Health Information: Secondary Purposes

Like most organizations, I also collect, use and disclose personal and health information for secondary purposes. The most common examples of secondary purposes are as follows:

- Basic information (e.g., name, address, contact information) may be used and/or disclosed to invoice clients for services, to process payments, to collect unpaid accounts, or to send receipts.
- To consult with accounting or legal professionals to assist with the operation of my practice. Some personal information (e.g., name, dates of visits, amounts paid for services) may be disclosed to these professionals. These professionals are mandated by their own regulatory organizations to maintain the confidence and privacy of any personal information they access through the course of their job duties.
- The cost of some services I provide to some clients is paid for by third parties (e.g., WSIB, private insurance). These third-party payers have either the client's consent or the legislative authority to direct me to collect and disclose to them certain information in order to demonstrate entitlement to funding.
- As a psychologist, I am regulated by the College of Psychologists of Ontario. For quality assurance reasons, the College may inspect my records and/or interview me as part of their regulatory activities acting in the public interest. In addition, as a psychologist I must report serious misconduct, incompetence or incapacity of other practitioners if they belong to certain other organizations or my own organization.
- Also, like all organizations, various government agencies (e.g., Canada Customs and Revenue Agency, the office of the Information and Privacy Commissioner of Ontario, etc.) have the authority to review my files and interview me as a part of their mandates. In these circumstances, I may consult with professionals (e.g., lawyers, accountants) to ensure that these requests are legitimate and required by law.

Disclosure of Health Information

As a health information custodian, I cannot release personal health information to a third party (e.g., an insurance company) without written consent, however, PHIPA does allow the sharing of information without consent in certain circumstances. For example, I am required to disclose personal information without a client's consent in the event of certain emergencies or other urgent circumstances in order to eliminate or reduce a significant risk of serious bodily harm. I am obligated to disclose information, with or without a client's consent when I suspect or am informed that:

- A client poses an imminent danger to themselves or someone else
- A child under the age of 18 years has suffered or is at risk of suffering physical or emotional harm, or sexual abuse
- There are reasonable grounds to believe that a client has been sexually assaulted by a registered health professional

PHIPA also allows the sharing of information with other health professionals who are involved in my client's care without explicit written consent, however there are provisions in the Act that allow an individual to deny information from being shared with other health professionals by

Updated November 21, 2019

specifying exactly what should not be shared. The health care professional receiving the information would then be told that part of the individual's health record has been withheld.

Protecting Personal and Health Information

To protect my clients' personal and health information, I adhere to the following office procedures:

- Client information in paper form is either under my direct supervision or is secured within my locked filing cabinet within my locked office at all times. No one other than myself has access to my locked filing cabinet. My office building has an alarm system that is armed when the building is not in use.
- My electronic hardware (e.g., computer equipment) is either under my direct supervision or is secured in my locked office or locked home at all times. My electronic hardware is secured with passwords and/or a biometric thumb print. Information stored on all electronic hardware is protected with encryption and a firewall.
- Client information accessed with computer hardware is stored using an online cloud storage service that uses end-to-end encryption on servers stored in Canada. The cloud service and its employees do not have access to the data stored using their service. My access to the cloud service is secured with a strong password and with two-factor authentication.
- Paper information is delivered through sealed and addressed envelopes and delivered by reputable organizations (e.g., Canada Post) with tracking information and requiring a signature to ensure delivery to the intended recipient. When it is time to destroy paper files containing personal information, I do so by cross-cut shredding.
- Electronic information is transmitted using end-to-end encrypted email, password protected documents, and/or encrypted links with password protection. When it is time to destroy electronic information, I do so using secure deletion.
- I strive to collect, use and disclose personal information only as necessary to provide services that my clients agree to and in accordance with relevant privacy legislation, the College of Psychologists of Ontario, and this privacy policy.

In the Event of a Privacy Breach

As a health information custodian, I am required to notify the Information and Privacy Commissioner of Ontario (IPC) of certain privacy breaches as follows:

- Use or disclosure of health information without authorization
- Stolen information
- Further use or disclosure of information
- Breaches that occur as part of a pattern
- Breaches related to the disciplinary action against a college or non-college member
- Significant breaches

In the event that health information is stolen, lost, or accessed by an unauthorized person, I will notify the client directly (in addition to any requirements to notify the IPC) and make a note of the issue and include it in the client's file.

Retention of Information

The College of Psychologists of Ontario requires that all Psychologists must retain client information in a secure location for a period of at least 10 years following the last contact with the client. Following 10 years after the last contact, paper files are destroyed by cross-cut shredding and electronic files are destroyed by secure deletion. If electronic hardware needs to be discarded, I will ensure that the hard drive is physically destroyed.

Access to Information

Clients have the right to access the personal information contained in their file. This might mean looking at what is in the file or getting a copy of the file or parts of the file. Please note that PHIPA allows me to charge a reasonable fee for providing a copy of all or part of a file. This fee is calculated based on a reasonable cost recovery basis.

I encourage clients who would like to access the information contained within their file to please ask me. I may need to ask that the request to view or receive a copy of the file is made in writing. I always try to respond to requests for access of personal health information as soon as possible but I do reserve the right to take up to 30 days (or longer in rare circumstances) to provide a client with access to their file following a written request. This is to allow me enough time to review the file carefully and consult with other professionals to ensure that I am meeting the requirements of PHIPA.

Please be aware that there are certain circumstances described in PHIPA that allow me to refuse requests for access to personal health information. If I must refuse a request for access (i.e., if there are parts of a file that I cannot share with a client who requests access) I will indicate this in writing and I will provide a reason in those situations in which PHIPA allows me to do so. In all cases, I will still allow access to the part(s) of the file that I am able to share. Where possible, I will assist in helping a client to understand any information in their file that they do not understand (e.g., any term, code, or abbreviation). If a client is not happy with the outcome of their request for access to their file, they are encouraged to discuss their concern with the office of the Information and Privacy Commissioner of Ontario (contact information provided below).

As per the College of Psychologists of Ontario standards of practice and PHIPA, a succession plan is in place to ensure that client files will be retained and can be accessed in the event of my death, incapacitation, or a change in my practice. A colleague who is a psychologist registered with the College of Psychologists of Ontario has agreed to take charge of my files in the event of my death or incapacitation. In the event of a sudden change of my status or that of the practice, all clients will be notified by the psychologist that has agreed to take charge of my files.

Corrections to File Information

If a client believes that there is a mistake in their personal health information recorded in their file, they are encouraged to ask me to correct it. I may need to ask that a request to correct a file

Updated November 21, 2019

be made in writing. I always try to respond to requests to make corrections as soon as possible but I do reserve the right to take up to 30 days (or longer in rare circumstances) to respond to written requests to change file information. This is to allow me sufficient time to review the request and the file carefully and consult with other professionals to ensure that I am meeting the requirements of PHIPA. I may ask that a client provide documentation that my file is wrong and I will place this documentation in the file.

Please be aware that there are certain circumstances described in PHIPA that allow me to refuse requests for correction to files. For instance, correction requests are appropriate when they apply to errors of factual information (e.g., date of birth) and not to my professional opinions or my observations that were formed in good faith. As well, I cannot make corrections to reports or records that I did not author. If I agree that a correction is needed, I will make the correction and I will notify anyone to whom the incorrect information was sent. If I do not agree that a correction is needed, I will explain why. In such a case, I will also ask for a brief written statement of disagreement. I will include this statement of disagreement in the file and will attach the statement of disagreement any time I disclose related file information. If a client is unhappy with the outcome of their request for a correction, they are encouraged to discuss their concern with the Information and Privacy Commissioner of Ontario (contact information provided below).

Questions

Please contact me directly about any questions or concerns that you have with regard to the collection, use, and disclosure of your personal information.

My privacy policy was created under the rules and guidelines set out by the Regulated Health Professions' Act (RHPA), the Personal Health Information Protection Act (PHIPA), the Professional Information Protection and Electronic Documents Act (PIPEDA) and within the standards of practice and guidelines set out by the College of Psychologists of Ontario. There are additional exceptions to the privacy principles that are too detailed to set out here as well as some rare exceptions to the commitments set out above.

If you have concerns about the professionalism or competence of my services or my mental or physical capacity I would ask you to discuss those concerns with me. However, if I cannot satisfy your concerns, you are entitled to discuss your concerns with my regulatory body:

COLLEGE OF PSYCHOLOGISTS OF ONTARIO

Suite 500 - 110 Eglinton Avenue West

Toronto, ON M4R-1A3

Phone: (416) 961-8817

Toll Free: (800) 489-8388

Fax: (416) 961-2635

Email: cpo@cpo.on.ca

Web: www.cpo.on.ca

For health information-related concerns, and to lodge a complaint related to my collection, use, or disclosure of your personal health information, talk to the provincial Privacy Commissioner:

Updated November 21, 2019

Information and Privacy Commissioner of Ontario
80 Bloor Street West, Suite 1700
Toronto, Ontario
Phone: (416) 326-3333
E-mail: commissioner@ipc.on.ca
Web: www.ipc.on.ca

As well, the federal Information and Privacy Commissioner oversees the administration of privacy legislation that applies in the private sector and in some circumstances when working with a psychologist in Ontario. The federal Commissioner can also act as an ombudsman for certain type of privacy disputes and may be able to provide assistance in the event of a concern regarding the collection, use, and disclosure of your personal information:

Information and Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
Phone: (613) 995-8210
Toll Free: 1-800-282-1376
Fax: (613) 947-6850
www.privcom.gc.ca