LABELLE CENTRE
Psychosocial assessment and intervention

Timmins Office
180 Jubilee Ave W
Timmins, ON
P4N 4M9

Kapuskasing Office
75 Queen St
Kapuskasing, ON
P5N1H5

Hearst Office
60 9th St
Hearst, ON
P0L 1N0

Protection of Personal Health Information Policy

(Personal Health Information Protection Act, 2004)

Definitions

Centre Labelle Centre (CLC): All employees, interns, students, contractors of the Centre Labelle Centre (CLC).

Express consent: Valid consent offered in a written or verbal manner.

Personal Health Information (PHI) Custodian ("Dépositaire des renseignements personnels de la santé"): This person is responsible for PHI and allows *agents* to collect, use, disclose, store, or eliminate PHI when certain criteria are met (for example, with the individual's consent).

Agent ("Mandataire"): This person acts for or on behalf of the custodian regarding the collection, use, and disclosure of PHI, regardless of whether this employed person is remunerated or not.

Contact person: This person (identified by the ***custodian***) helps the ***custodian*** comply with the Act, meaning that this person ensures that all agents are informed and comply with the Act. This person responds to public queries about the policies of CLC and to requests for access or correction. This person also receives complaints from the public regarding privacy breaches.

Policy

The protection of personal health information (PHI) is a principle that the Centre Labelle Centre (CLC) takes very seriously. The CLC and CLC employees are committed to respecting and protecting the personal health information of clients and to comply with the *Personal Health Information Protection Act*, 2004. The main goals of this Act are as follows:

- ✓ to obtain consent to collect, use, or disclose an individual's PHI (except in specific circumstances discussed below);
- ✓ to maintain the security of PHI by taking reasonable measures to ensure protection against theft, loss, and non-authorized use or disclosure;
- ✓ to ensure the accuracy of PHI and to allow any corrections if the information is incomplete or incorrect (except when it is impossible to make a correction or if the information comes from a professional opinion);
- ✓ to collect, use or disclose PHI only when necessary; and
- ✓ to give individuals access to their PHI (except in specific circumstances permitted by the

law).

At the CLC, we collect (in a direct or indirect manner), use, and disclose PHI only when necessary, to ensure the delivery of our services. All information will remain confidential except as provided in this document and according to the law. The CLC is committed to transparency about how PHI is collected, used, and disclosed. This document describes our policies regarding the protection of personal health information. Employees, students, interns, and contractors of the CLC are notified that any security breach of PHI may result in disciplinary action from the employer, a report to the respective College (if the employee is also a regulated health professional), a complaint with the Information and Privacy Commissioner or, in cases of deliberate offences, criminal prosecution.

What is PHI?

PHI is an individual's identifiable health information. It includes all information in verbal or written form (including electronic versions) that deals with an individual's health. The *Personal Health Information Protection Act*, 2004 also applies to identification information such as address and phone number.

Who are we?

The CLC currently includes employees, interns, students, and contractors. We use a number of consultants or organizations who can, in carrying out their duties, have access to specific PHI. This information includes maintenance staff, the proprietor, technological support workers, etc. We are taking all possible measures to prevent their access to PHI and we have their written commitment that they are following the fundamental principles of personal health information protection.

Why do we collect PHI?

We collect, use, and disclose PHI in order to offer our services. We offer mental health services to our clients (including psychological services, psychotherapy, counseling, professional consultation, and supervision). For example, we collect PHI (in a direct and indirect manner) regarding the problem that is discussed, including the client's developmental and familial history, the administration of certain psychological tests, etc., in order to better assess the individual's needs with the aim of improving the situation.

We collect, use, and disclose PHI for various other reasons such as:

- to prevent damages from taking place and to respond to emergency situations;
- to educate and train students and employees (including contractors) of the CLC;
- to maintain a high quality of services and to conduct clinical research;
- to obtain payment for our services (from the individual or a third party such as a school or an agency); and
- to comply with external regulations and with the law (for example, the standards of the College of Psychologists of Ontario, Children's Aid Society, the Information and Privacy Commissioner of Ontario).

Measures in place to protect PHI

The CLC is committed to use appropriate security measures to prevent PHI from being stolen, lost, or consulted without authorization. A detailed description of these measures follows:

Consent to the collection, use, and disclosure of PHI:

- use a form of consent to collect, use, and share information (form #2) in order to obtain valid and informed consent;
- publicize the statement describing the practices used (form #2.1) by the CLC regarding the protection of PHI.

Protection of PHI :

- use a confidentiality form (form #4) signed by all employees, interns, students, and contractors of the CLC including the support staff, service staff, and the proprietor;
- secure every computer with a password;
- supervise its place of work (for example, close and lock the door, keep paper files locked away in the office);
- store pending or closed files in a locked filing cabinet in a locked room ;
- limit access to files;
- keep active files locked away in the employee's office;
- keep files in a locked briefcase when the employee needs to retrieve files from the office (express consent is required in advance);
- return files to the office as quickly as possible.

Protection of electronic information:

- limit or eliminate the use of electronic devices that are not dedicated for work, but, when it is absolutely necessary to use them, make sure to de-identify the data;
- use an electronic database that conforms to the requirements of the Act (we currently use *Owl Practice*);
- use a password for this database;
- use an additional password for this database on new electronic devices;
- de-identify the information while using computerized rating systems and delete the information once it has been rated.

Sharing PHI :

- make sure to obtain the individual's consent to share the PHI in question;
- use a consent form (form #3) when sharing PHI with any person who is not part of the "circle of care";
- share PHI "in person" or by mail (by using Canada Post);
- if it is necessary to share PHI by e-mail, de-identify the information, protect the documents with a password, and include a privacy notice at the bottom of the e-mail;
- if it is necessary to share PHI by text, de-identify the information;
- when sharing PHI by fax machine, use a cover letter that includes a privacy notice, confirm that the recipient is expecting the fax and confirm receipt;
- when sharing PHI by video conference (presently *Zoom for Education* with a Business Associate Agreement [BAA]), protect the meeting with a password, use a waiting room,

and lock the meeting once it is started;
- regardless of the method of communication, confirm the contact information in advance.

Training of employees, students, and interns/Peer consultation

- de-identify information;
- permanently delete or destroy the video or audio recordings once they have been transcribed and rated.

Retention and destruction of PHI

We are required to retain PHI for a certain period of time so that we can respond to questions regarding the services provided and for our own responsibility towards our professional bodies. However, in order to protect client PHI, we do not keep records for longer than necessary. At the moment, we keep client files for 10 years after the last provided service or for 10 years after the individual's 18th. After that time, we shred the paper copy of the file and permanently delete any electronic files.

Right of access and correction of PHI

The client has the right to access their file and their PHI, except in specific circumstances. All requests must be directed to the contact person. A written request may be required. The contact person will process the request and determine if it is acceptable. If so, the identity of the individual will be confirmed, and the contact person will remain available for any explanation or clarification. We reserve the right to charge a reasonable fee (as suggested by the Information and Privacy Commissioner of Ontario) for copies of the file. If the request is determined to be unacceptable, an explanation will be given to the individual in question. We are committed to responding to any request within 30 days. If it is not possible to do so within 30 days, an extension will be requested.

If there is false or incorrect information on file, the client may request a correction. A written request may be required. This applies to any factual information and not to professional impressions or opinions. Corrections will be made if they are deemed necessary (for example, if the information has an impact on the services offered to the client). Where possible, we will seek to make changes to all versions of the document in question. If it is determined that a correction is not necessary, a note with the individual's concern will be included in the file.

In the case of PHI protection violation

Although we take all necessary measures to protect client PHI, in the event that loss, theft, or unauthorized access occurs, informing the client is of primary importance. Upon detection of a breach, the following measures will be taken:

1. Immediately contain the breach (for example, by recovering distributed hard copies of PHI, ensuring that no other copies have been made, following the steps to prevent unauthorized access);
2. Alert affected individuals and provide them with our contact information as well as the contact information for the Ontario Information and Privacy Commissioner. Inform affected individuals of their right to file a complaint with the Commissioner.
3. Conduct an investigation on and remedy the situation (by identifying additional security measures and ensuring that employees are adequately trained on this issue).

Depending on the severity of the offence, we may work closely with the Commissioner. If we take disciplinary actions against an employee who is a regulated health professional, we are obligated to notify their respective professional body.

For any questions or concerns

For any questions or concerns, clients can reach out to the CLC's contact person. The contact person will respond to all questions and concerns. Formal complaints must be made in writing. The contact person will then acknowledge receipt of the file and ensure that an investigation is initiated as soon as possible. The formal decision as well as the reasoning behind the decision will be communicated to the individual in writing.

Complaints may also be submitted directly to the Office of the Information and Privacy Commissioner at the following address:

2 Bloor Street East

Suite 1400

Toronto, ON M4W 1A8

Responsibilities of the CLC

Responsibilities of employees and agents

All employees must adhere to the "*Measures in place to protect PHI*" in this document. In addition, in the event of loss, theft, or unauthorized access to PHI, the employee must inform the custodian or the contact person as soon as possible. Moreover, employees agree not to take or post photos of clients or photos containing PHI on social media.

With regards to information sharing, where information can be shared in a more secure manner, the employee agrees to use the most secure method. No information, regardless of whether consent is legally required or not, will be collected or shared without the **valid and informed** consent of the individual.

Responsibilities of the custodian

The custodian is responsible for ensuring compliance with the Act at the CLC. The custodian must publish a written statement regarding PHI protection policies. This statement must include, at a minimum, the main reasons for why the information is being collected, how to communicate with the contact person (or custodian), the steps for making a request for access or correction of the file, and finally, how to file a complaint with the custodian, contact person or the Office of the Information and Privacy Commissioner.

The custodian is also responsible for overseeing relations with computer service providers. Specifically, an agreement must be signed between the provider and the CLC and must include, at a minimum, the services offered by the provider, the security measures in place and confirmation that the provider in question is complying with the legislation.

Responsibilities of computer service providers

Computer service providers must commit to using PHI solely for the purpose of providing their

service. They are strictly prohibited from disclosing PHI to which they have access. Providers must inform the custodian of any breach of PHI. Providers must submit a written description (without jargon) of the services they provide to the CLC, a risk evaluation of the system as well as a description of their own privacy policy. The database must also contain a record of any modifications and access sessions.

Responsibilities of the contact person

The contact person (in collaboration with the custodian) is committed to ensuring the professional development of the CLC's employees regarding PHI protection. The contact person is also committed to managing any access or change requests and to address all formal complaints within 30 days.

Examples of exceptions to the Act

The following list is not exhaustive. For more information, please consult the legislation in question: https://www.ontario.ca/fr/lois.

The Personal Health Information Protection Act, 2004

This Act allows us to disclose PHI if it is necessary in order to "eliminate or reduce a substantial risk of serious injury to an individual or group of individuals."

The right of access to a file may also be denied if there is a "risk of substantial harm to the treatment or recovery of the individual or serious injury to the individual or another person," or if access results in "the identification of a person who has, explicitly or implicitly and in confidence, provided the custodian with information contained in the record, if the custodian considers it appropriate under the circumstances that the person's identity be kept confidential". See specific legislation for more details.

Child, Youth and Family Services Act, 2017

This Act requires us to report to the Children's Aid Society all cases of suspected abuse of a child under the age of 16. This Act allows us to report to the Children's Aid Society in cases of suspected abuse of a child aged 16 or 17. See specific legislation for more details.

Retirement Homes Act, 2010

This Act requires us to report any suspicion of abuse of a person living in a retirement home to the Registrar. See specific legislation for details.

Fixing Long-Term Care Act, 2021

This Act requires us to report any suspicion of abuse of a person living in a long-term care home to the director. See specific legislation for more details.

Regulated Health Professions Act, 1991

This Act requires all regulated health professionals to report if they have "reasonable grounds to believe that another member of their College or another College has sexually abused a patient." A report "must be filed in writing with the Registrar of the College of the member who is the subject of the report." See specific legislation for details.

Notes. This policy was developed according to the requirements of the *Personal Health Information Protection Act*, 2004. This Act is complex and provides additional detailed exceptions to this policy. See the Act for further details.

This document was developed by consulting several resources such as the *Guide to the Ontario Personal Health information Protection Act* drafted by Perun, Orr and Dimitriadis (2005), the Act itself, and *The Personal Health Information Protection Act, 2004: A Guide for Regulated Health Professionals* by Steinecke, Maciura, and LeBlanc (2016).