CENTRETOWN COMMUNITY HEALTH CENTRE
POLICY AND PROCEDURES MANUAL

PRIVACY & CONFIDENTIALITY OF PERSONAL HEALTH INFORMATION

No: PRV 1-01	**Title:** COMMITMENT TO PRIVACY OF PERSONAL HEALTH INFORMATION	
Approved By: Board of Directors	**Signature:**	
Approved: February 2023	**Next Review:** February 2027	**Page:** 1 of 10

PREAMBLE

Centretown Community Health Centre ("CCHC" or the "Centre") will manage the collection, use and disclosure of all personal health information ("PHI") in verbal, hard copy and electronic formats in accordance with provincial and federal government legislation, including the *Personal Health Information Protection Act, 2004* (PHIPA) and the *Freedom of Information and Protection of Privacy Act* (FIPPA).

POLICY

CCHC is committed to maintaining the privacy of all personal health information of its clients. To ensure compliance with legislative obligations, CCHC will establish and maintain a privacy protocol to guide the collection, use (including viewing) and disclosure of personal health information in its custody.

DEFINITIONS

Agent: Refers to a person that, with the authorization of CCHC, acts on behalf of the organization with respect to PHI for professional purposes (rather than the agent's own purposes). CCHC agents are employees, students and volunteers, and may or may not belong to a regulatory college.

Breach of privacy: Occurs when an individual's PHI has been disclosed, used, or viewed without the individual's consent or pursuant to an exemption described in the Act, or has been stolen, lost or accessed by unauthorized persons, or has been collected by electronic means without authority.

Circle of care: Not a legal term. Describes the ability of a health information custodian (HIC) to assume an individual's implied consent to collect, use or disclose PHI for the purpose of providing health care, so long as the following conditions are satisfied:

a. The PHI to be collected, used or disclosed by the HIC was received from the individual, his or her substitute decision-maker, or another HIC.

b. The HIC must have received the PHI for the specific purpose of providing or assisting in the provision of health care to the individual.
c. The purpose of the collection, use or disclosure of PHI by the HIC must be for the provision of health care or assisting in the provision of health care to the individual.
d. For disclosures, the disclosure of PHI by the HIC must be to another HIC.
e. The HIC that receives the PHI must not be aware that the individual has expressly withheld or withdrawn their consent to the collection, use or disclosure.

Personal health information (PHI): Refers to any identifying information about an individual, in oral or recorded form, if the information:

a. relates to the physical or mental health of the individual, including the health history of the individual's family;
b. relates to the provision of health care to the individual, including the identification of the individual's health care provider(s);
c. is a plan for services pursuant to the *Connecting Care Act, 2019*;
d. relates to the individual's payments for health care, eligibility for health care, or eligibility for coverage of health care;
e. relates to the individual's donation of any body part or bodily substance;
f. is the individual's health number; or
g. identifies an individual's substitute decision-maker.

PROCEDURE

1. Consent

1.1. **Implied consent:** HICs may imply an individual's consent to collect and use PHI for most health care purposes within the circle of care. They may also imply consent to disclose PHI to another HIC for the purposes of providing (or assisting in the provision of) health care to the individual. However, HICs generally cannot rely on implied consent when disclosing PHI to a person or organization that is not a HIC (except in cases of mandatory reporting). For disclosures to non-HICs, express consent is generally required.

1.2. **Express consent:** For all purposes falling outside of the parameters of the direct provision of client care (i.e. research, advocacy, media), HICs must obtain the express consent of the client (or their substitute decision-maker) whose PHI would be collected, used or disclosed for the non-care related purpose. The HIC must be satisfied that the required elements of consent are fulfilled in the course of obtaining express consent (i.e. consent is knowledgeable, specific to the PHI being collected/used/disclosed, and not obtained through deception or coercion).

2. Protecting PHI

2.1. CCHC employees, students, and volunteers are required to follow PRV 1-02 Privacy Protocol for CCHC Operations to protect all PHI held by the Centre.

2.2. Employees, students, and volunteers will keep all PHI confidential.

2.3. Employees, students, and volunteers who handle PHI will be trained in the proper ways to collect, use (including viewing) and protect such information.

2.4. Employees, students, and volunteers who fail to abide by CCHC's privacy policies and procedures may face disciplinary action.

2.5. The Centre will maintain appropriate physical and electronic safeguards to ensure all PHI at the Centre is protected from external threats.

2.6. Only designated staff can access PHI stored on computers by using a secured pass code. Volunteers and students may be granted limited access for specific purposes.

2.7. External consultants and agencies with access to PHI must enter into privacy agreements with CCHC.

3. Retention and Destruction of PHI (see ORG 3-03 Records Retention)

3.1. For adult clients, PHI must be kept for 15 years from the date of the last entry in the record.

3.2. For clients who are children, PHI must be kept until 15 years after the day on which the patient reached or would have reached the age of 18 years.

3.3. In some instances, CCHC may be required to keep PHI longer than the above time periods, for example when a request for access to PHI under PHIPA is made before the retention period ends.

3.4. Paper records of clients that are being vaulted will be recorded on microfiche or computer disks, and the paper copies will be destroyed by shredding. The microfiche/disks are securely stored in a fireproof filing cabinet at CCHC or off-site in a secured storage facility. The Centre will ensure that all hard drives are physically destroyed when discarded.

4. Access to PHI

4.1. With few exceptions, clients have the right to access and receive copies of their PHI in CCHC's custody. The original records are the property of CCHC and will not be released.

4.2. To access PHI, clients must sign a Consent to Disclose Personal Health Information and confirm their identity.

4.3. CCHC will provide access to records for review within 30 days of receiving a written request, or 60 days if the search is complex. Clients will be asked to review their records with a CCHC provider present so that information can be explained properly.

4.4. CCHC may refuse to disclose health records if a service provider believes that such access would risk serious harm to treatment or recovery, or risk serous bodily harm to the individual or another person.

4.5. Clients have the right to ask that a correction be made to the PHI in their records when they believe there is a mistake. This applies to factual information only and not to any professional opinions formed. CCHC may ask clients to provide proof that the information held on file is wrong.

4.5.1. Where CCHC agrees that a mistake was made, the Centre will make the correction and notify the individual and, at the request of the individual, notify any other providers with whom the information was shared, to the extent reasonably possible, unless such correction cannot reasonably be expected to affect the ongoing provision of health care or other benefit to the individual.

4.5.2. If CCHC does not agree that a mistake was made, the Centre will inform the individual of reasons for its refusal to correct, and inform the individual of their right to have a statement of disagreement placed in the PHI record, their right to require CCHC to make reasonable efforts to have the statement of disagreement disclosed to others to whom the PHI had been disclosed, and inform the individual of the right to make a complaint to the Information and Privacy Commissioner.

5. Collection, Use (Including Viewing) and Disclosure of PHI

5.1. CCHC collects and uses PHI to: determine what care, programs or services clients require; document the course of client care or involvement in programs or services; provide a means of communication among CCHC staff who provide care for a given client; and comply with any legal and regulatory requirements.

5.1.1. CCHC limits the information collected to what is needed for these purposes. CCHC will collect PHI directly from an individual, unless it has the individual's consent to collect PHI indirectly, or CCHC is permitted by law to collect PHI indirectly.

5.2. All client communications with CCHC are treated as confidential at all times to the extent possible, while still allowing CCHC to comply with its legal responsibilities. PHI may be shared for purposes of consultation between CCHC staff and external collaborative agencies in the course of providing care.

5.3. CCHC will not share PHI without a client's implied or express consent, unless required to comply with its legal obligations within the circle of care, if necessary to reduce significant risk serious bodily harm to persons, or as otherwise permitted or required by PHIPA or FIPPA.

5.4. When disclosing PHI without a client's express or implied consent, CCHC will not disclose more information than what is required by law.

5.5. When fulfilling a request to release a client's PHI, CCHC will document: the client's name; the name of the CCHC provider releasing the information; the name of the person or organization receiving the information; the information being released; and the date of the client's express consent (where applicable).

6. Privacy Concerns

6.1. CCHC is committed to addressing questions or concerns about its privacy policies and practices, and has therefore appointed a Privacy Officer to support this process.

6.2. Clients and staff may contact the Privacy Officer by mail, phone, or email. The contact information of CCHC's Privacy Officer will be made publicly available.

6.3. Complaints regarding privacy practices will be directed to the Privacy Officer whose responsibility is to acknowledge receipt of complaints, ensure complaints are promptly investigated, and provide a formal written response.

6.4. For general inquiries concerning the protection of PHI, or to report a complaint about CCHC's privacy practices, clients may contact the Information and Privacy Commissioner of Ontario (IPC).

7. Breach of PHI privacy

7.1. CCHC is committed to keeping PHI safe and confidential, and following the rules set out by law and by CCHC policies to collect, use, view, and disclose PHI. CCHC will have a Privacy Officer responsible for managing and responding to all perceived or real breaches of privacy with regards to PHI. The Privacy Officer is also responsible for monitoring legislative changes to ensure that CCHC privacy policies and practices are in compliance, as well as reporting on compliance with legislation to the Board on an annual basis.

7.2. It is the responsibility of all CCHC staff, students and volunteers who discover or suspect a breach of privacy (or observe a "near miss") to inform their supervisor and notify the Privacy Officer immediately by completing a Privacy Incident Form. Supervisors will seek to protect staff reporting privacy breaches involving other staff, students and volunteers from reprisal, by protecting the anonymity of reporting staff to the extent possible and, more generally, aiming to foster a culture of staff engagement and systems improvement around the protection of clients' PHI.

7.3. Willful breaches of privacy or repeated instances of privacy breaches by a CCHC employee, student or volunteer may result in disciplinary action, including possible dismissal and reporting to legal or regulatory authorities (see Appendix I - Privacy Breach Levels and Related Action).

8. Privacy Officer

8.1. The Executive Director (ED) (or designate) will act as CCHC's Privacy Officer.

8.2. The Privacy Officer will have a dedicated secure e-mail address for the purpose of receiving concerns about the Centre's privacy practices. This email address will be made publicly available to persons served and the general public.

9. Managing a Breach of Privacy

9.1. Any CCHC employee who discovers or suspects a breach of privacy with respect to PHI will:

- inform their supervisor;
- immediately notify the Privacy Officer; and
- complete a Privacy Incident Form.

9.2. The Privacy Officer will identify the scope of the potential breach and take steps to contain it by:

9.2.1. Retrieving the hard copies of any PHI that have been disclosed.

9.2.2. Ensuring that no copies of PHI have been made or retained by the individual who was not authorized to receive the information and obtain the person's contact information in the event that follow-up is required.

9.2.3. Determining whether the privacy breach would allow unauthorized access to any other PHI (e.g. an electronic information system) and take the necessary steps to

prevent further breaches (e.g. change passwords, identification numbers and/or temporarily shut down a system).

9.2.4. Notifying the Information and Privacy Commissioner of Ontario (IPC), regulatory colleges, eHealth Ontario and/or legal counsel as legally required (see section 9.3 below).

9.3. The Privacy Officer (or designate) will identify and notify in writing those individuals whose privacy was breached by:

9.3.1. Notifying any affected clients at the first reasonable opportunity.

9.3.2. Providing details of the extent of the breach and the specifics of the PI or PHI at issue.

9.3.3. Advising affected clients of the steps that have been or will be taken to address the breach, both immediate and long-term.

9.3.4. Notifying the client of their right to file a complaint with the IPC and including the IPC's contact information in the written notification.

9.4. The Privacy Officer will keep copies of all privacy breach notifications sent to clients.

10. Reporting Privacy Breaches Related to Personal Health Information (PHI)

10.1. To Regulatory Colleges:

10.1.1. The Privacy Officer is legally required to notify the employee's regulatory college (including the Ontario College of Social Workers and Social Service Workers) when, in response to a breach of privacy by an employee:

- The employee is terminated, suspended or subject to disciplinary action; or
- The employee resigns and CCHC suspects that the resignation is related to the investigation into the breach.

10.1.2. The Privacy Officer must notify the regulatory college within 30 days of the event occurring.

10.2. To the Information and Privacy Commissioner of Ontario (IPC):

10.2.1. The Privacy Officer will immediately notify the IPC of a breach of privacy in any of the following situations:

- PHI is purposely used or disclosed without authority (for e.g. snooping).
- PHI is stolen.
- Following an initial breach of privacy, CCHC suspects or knows the information was or will be further used or disclosed without authority.
- There is a pattern of similar thefts, losses or unauthorized uses or disclosures of PHI under CCHC's control.
- CCHC notifies a regulatory college (including the Ontario College of Social Workers and Social Service Workers) when, in response to a breach of privacy by an employee:
  - The employee is terminated, suspended or subject to disciplinary action; or
  - The employee resigns and CCHC suspects that the resignation is related to the investigation into the breach.

- When a staff, student or volunteer who is not a member of a college has committed a breach of privacy that under the same circumstances, had they been a member, would have triggered notification to a college.
- When none of the above situations apply but CCHC determines that the breach of privacy is **significant** nonetheless. The following factors influence the significance of a breach:
  - the nature of the PHI;
  - the volume of PHI records;
  - the number of individuals whose PHI was contained in the record(s);
  - the number of Health Information Custodians (such as CCHC) or agents responsible for the breach.

10.3. To eHealth Ontario:

10.3.1. The Privacy Officer must report all breaches involving the ConnectingOntario EHR Solution to Ontario Health (Digital Services) Privacy Department at the first reasonable opportunity, but no later than by the end of the next business day after CCHC becomes aware of the breach.

11. Annual Reporting

11.1. The Privacy Officer will report all PHI privacy breaches that occurred during the previous calendar year to the Board of Directors in February of each year. This report will be part of the annual report to the Board on complaints, incidents and accidents.

11.2. The Privacy Officer will submit an annual statistical report of PHI privacy breaches to the Information and Privacy Commissioner of Ontario (IPC). This report will be submitted by March 31 every year and will include the total number of times CCHC notified individuals in the previous calendar year that their PHI had been stolen, lost, used, viewed, or disclosed without authority.

REFERENCES

Personal Health Information Protection Act [S.O. 2004, c. 3, Schedule A]. Available at: https://www.ontario.ca/laws/statute/04p03

Freedom of Information and Protection of Privacy Act [R.S.O. 1990, c. F.31]. Available at: https://www.ontario.ca/laws/statute/90f31

Circle of Care: Sharing Personal Health Information for Health-Care Purposes. Available at: https://www.ipc.on.ca/wp-content/uploads/Resources/circle-of-care.pdf

RELATED POLICIES

PRV 1-02 Privacy Protocol for CCHC Operations
PRV 1-03 Consent to the Collection, Use and Disclosure of Personal Health Information (PHI)

PRV 1-04 Safeguards for Protecting Personal Information
PRV 1-06 Lock-box Provisions
ORG 3-03 Records Retention
HR 2-07 Complaints and Appeals
ORG 1-08 Client Feedback and Complaints

APPENDIX I – PHI PRIVACY BREACH LEVELS AND RELATED ACTION

Level 1: Unanticipated
This level of breach occurs when personal health information (PHI) is revealed or disclosed by an employee who would not have grounds to anticipate the information being shared to unauthorized parties. Examples include but are not limited to:

- An employee faxes PHI to the correct fax number on-file but the fax number on-file is wrong (i.e. someone gave CCHC an incorrect fax number)
- An employee faxes PHI that ends up lost or unaccounted for due to a problem with an e-fax or other electronic system

Because an employee could not have mitigated this type of breach, there is no disciplinary action at this level. CCHC will nonetheless inform clients a breach of privacy occurred.

Level 2: Unintentional or Careless
This level of breach occurs when an employee unintentionally or carelessly accesses, reviews or reveals a client's PHI to him/her or others without a legitimate need to know the information. Examples include but are not limited to:

- Unintentionally faxed PHI to the wrong number (i.e. not the number on-file)
- An employee discusses PHI in a public area.
- An employee leaves PHI in a public area.
- An employee leaves a computer terminal with PHI unattended.

<u>Disciplinary Actions for Level 2 Breaches</u>
In consultation with the Executive Director, the Supervisor/Director will determine if disciplinary action is required. This may include a verbal warning, written warning, and could include suspension or termination, including termination with cause if the misconduct meets the standard outlined in the *Employment Standards Act, 2000* ("*ESA*"). Documentation will be maintained in the individual's personnel file. As part of the corrective nature of the disciplinary process, the employee will be required to review all appropriate policies.

If disciplinary action is taken, CCHC is required to report the privacy breach incident to the applicable professional regulatory college or association.

Level 3: Curiosity or Concern (no personal gain)
This level of breach occurs when an employee intentionally accesses or discusses a client's PHI for purposes other than the care of the client or other authorized purposes but for reasons unrelated to personal gain.

Examples include but are not limited to:

- An employee looks up birth dates or other demographic information about a client.
- An employee accesses and reviews a record of a client out of curiosity or concern.
- An employee reviews a public personality's record, a fellow staff member, family member or other well-known individual.

Disciplinary Actions for Level 3 Breaches

1st Offense

- A written warning, suspension or termination, including termination with cause if the misconduct meets the standard outlined in the *ESA*, documented and maintained in the employee's personnel record. As part of the corrective nature of the disciplinary process, the employee will be required to review all appropriate policies.
- Severity of first offense may result in termination, including termination without cause if the misconduct meets the standard outlined in the *ESA*
- Disciplinary actions shall be reported to the applicable professional regulatory college or association

2nd Offense

- Termination, including termination with cause if the misconduct meets the standard outlined in the *ESA*
- Disciplinary actions shall be reported to the applicable professional regulatory college or association.

Level 4: Personal Gain or Malice

This level of breach occurs when an employee accesses, reviews or discusses a client's PHI information for personal gain or with malicious intent. Examples include but are not limited to:

- An employee reviews a client record to use the information in a personal relationship or for personal gain.
- An employee compiles a mailing list for personal use or to be sold.
- An employee uses a client's PHI in a civil proceeding (e.g. divorce, family court, custody matters)

Disciplinary Actions for Level 4 Breaches

Disciplinary action includes suspension without pay and/or termination, including termination with cause if the misconduct meets the standard outlined in the *ESA*, and report to applicable professional regulatory college or association. In cases where behavior may be criminal in nature, police involvement may be required.