Privacy/Confidentiality Policies and Procedures

Included in this handbook are the following privacy policies and procedures:

I. **Collection, Use, Disclosure and Security.**
II. **Guidelines for Access and Correction to Client Record.**
III. **Obtaining Consent for Collection, Use or Disclosure of PHI.**
IV. **Refusing or Revoking Consent – Impact on the Common Client Record (CCR).**
V. **Physical Security of PHI.**
VI. **Principles for Protection of Personal Health Information.**

This policy is applicable to all employees, volunteers, students, contractors, and consultants.

Last Review/ Revision – April 2026

Approved by: Amandeep Kaur, Chief Executive Officer

I. Collection, Use, Disclosure and Security

PURPOSE

PCHS will ensure that clients' Personal Health Information (PHI) is managed in a way that complies with the PHI Protection Act 2004 (PHIPA)

POLICY

All employees will receive training related to the collection, use, disclosure, and security of PHI.

PROCEDURE

- PHI will not be collected, used, or disclosed without the client's express written/verbal consent, except where there is a risk of injury to self or others, there is a duty to report, or disclosure is otherwise legally required. Any changes to the client's consent must be immediately documented in the Privacy, Confidentiality and Consent form. The circumstances related to the change are documented in the progress notes.
- PCHS employees are not permitted to access PHI of any person without permission or reason to do so. While it is general practice that information is shared within agencies/services about clients, this is only done so for the purpose of providing service. PCHS will hold its employees accountable for inappropriately accessing the personal information of clients were it was not required for service related reasons.

- Duplication of PHI should be kept to a minimum and only done when necessary to provide services. Whenever possible, employees should refer to the information contained in the client's health record/file.
- All employees must take every precaution to ensure that PHI is protected from loss, theft, or unauthorized access.. PHI should not be removed from the organization unless required to provide services. Electronic copies are kept safe and secure under password protected cloud storage. Any paper copies/ notes should be kept in locked storage.
- Employees must take precautions when logging into non-secure/ public networks to access PCHS network/SharePoint for client records.
- Employees must report all breaches and potential breaches of PHI to their Supervisor upon being discovered. The Supervisor will notify the Privacy Officer as soon as they are advised or become aware of a potential breach. The Privacy Officer will notify the Chief Executive Officer or their designate.

- All clients whose personal information has, or may have been breached, will be notified of the breach, and the organization's follow up actions.

- All breaches will be investigated under the direction of PCHS' Privacy Officer to determine how they occurred and what mechanisms can be put in place to prevent such breaches from occurring in the future.

II. Guidelines for Access and Correction to Client Record

POLICY

All current clients of PCHS have the right to review, read and obtain a copy of their records.

PROCEDURE

- Requests by individuals for access to their personal health record must be made in writing and directed to the attention of PCHS' Privacy Officer. (*Refer to Request Form for Access to Personal Health Records – Appendix A of Client Bill of Rights, Responsibilities and Complaint Policy)*

- Requests will be reviewed and responded to within reasonable timelines and costs to the individual, as applicable. Individuals will normally receive a response within 30 days. In some cases, additional time may be required.

- The Privacy Officer will identify a designate who will review the record to determine if all or part of the file can be made available to the client.

- The client will be contacted to advise them of the response to their request and set up time to review their file.

- Generally, clients are required to review their file in the presence of a designated person from the organization and may have access to specific information or the entire file.

- Clients requesting changes to their records must successfully demonstrate the update/inaccuracy/incompleteness of the information contained in their file prior to any amendments being made. Any changes, additions, deletions, concerns the client brings forward should be recorded by the designate and added to the

file/client notes.

- Clients may request and receive a copy of their file. PCHS may charge a reasonable fee for this service, as applicable.

III. Obtaining Consent for Collection, Use or Disclosure of PHI

POLICY

All employees will ensure that clients have given informed consent prior to collection, use or disclosure of their PHI.

PHI will not be collected, used, or disclosed without the client's express written/verbal consent, except where there is a risk of injury to self or others, there is a duty to report, or disclosure is otherwise legally required. Any changes to the client's consent must be immediately documented in the Privacy, Confidentiality and Consent form. The circumstances related to the change are documented in the progress notes. Employees will use the 'Privacy, Confidentiality and Consent Form (see appendix A) to obtain client consent for provision of PCHS services in collaboration with other healthcare/service providers. The form would be used for individuals and agencies that are part of the client's "circle of care." With the client's permission, family members or significant others can also be included on this form.

Guidelines for Completion of Privacy, Confidentiality and Consent Form:

- When obtaining consent to share the Client Record, employees must review the guidelines outlined in the 'client orientation package' with the client. For consent to be informed, employees must ensure that clients understand what is being collected, used, and disclosed.

- The Privacy, Confidentiality and Consent Form should be dated and signed by the client or their substitute decision maker, as applicable. Signatures are required for in-person services.

IV. Refusing or Revoking Consent – Impact on the Integrated Assessment Records (IAR)

STATEMENT

PCHS agrees that services will not be withdrawn from individuals either refusing consent or revoking consent. That said, however, there may be individual circumstances where an agency believes that it cannot provide safe and responsible services without the involvement of another agency (or agencies) and the sharing of information. In those circumstances, the partner agency may withdraw service.

Refusing Consent

- When a client refuses to provide consent, it is understood that participating agencies will maintain independent clinical records on the IAR database. The result will be duplicate records.
- When a client refuses to provide consent, it is the responsibility of the service provider to explain the consequences of not signing consent.
- Services will not be refused if the client does not sign consent.

Please see "Refusing Consent Form" as A*ppendix B.*

Revoking Consent

When a client revokes previously given consent, the following procedures apply:

1. PCHS staff will need to contact the client to complete a written request for revoking their consent.

2. PCHS staff informs the client about the consequences of revoking consent.

3. If consent is revoked after Step 2, employees must inform their respective Supervisors at PCHS.

4. If consent is revoked after Step 1, a "Client Revoking Consent Form (Request to Remove Agencies from My IAR)" must be completed by the client. *Please see Appendix C.*

5. The Supervisor authorizes the PCHS staff to create duplicate records for the client for future use by each affected agency. The former record will be called "Historical" and can be accessed as "read-only."

V. Security of PHI

POLICY

All PCHS employees will ensure the safe and secure handling of client information. All reasonable steps should be taken to prevent loss, theft, or misdirection of client

information.

PROCEDURE

1. Electronic Records/ Paper Documentation

- Definition of Records: Client records include any documentation—whether in paper or electronic form—that contains personally identifiable information (PII) about a client. This includes but is not limited to digital files, emails, cloud-stored documents, and handwritten notes such as those in day planners or notebooks.

- All client records must be stored securely to protect client confidentiality and prevent unauthorized access. Electronic records must be saved in a secure, password-protected system such as SharePoint or any other cloud-based storage solution approved by PCHS. Paper records must be kept under lock. Access must be restricted to authorized personnel only.

- Client's information should be stored in the client's file at all times. No client information should be made accessible to any visitor or other person not authorized to access that information for the provision of services.

- Printing and photocopying client information should be kept to a minimum and only done when necessary for the provision of services.

- Follow PCHS' Data Security Policy (IT Policies and Procedures) especially while accessing client information offsite. Employees should securely log off the client record when not actively using it to document or review information.

- Follow PCHS Use of Artificial or Augmented Intelligence (AI) policy while using the AI.
- No identifiable client information is to be transferred, copied or entered onto personal devices such as portable computers, pocket PCs, Palm devices, or external storage devices such as data sticks, hard drives, memory cards, home computers, etc. Should it be necessary to use the above-mentioned devices, prior written approval must be obtained from the supervisor; devices must be password protected, and portable storage devices such as USB keys must be encrypted by PCHS.

- Only official email account/ID should be used while communicating related to clients' services.

- Disclosing that an individual is a client of PCHS without their express consent,

constitutes a breach of their privacy.

2. Faxing of client information

- When faxing information ensure that the fax number of the receiving agency/individual is correct.
- Employees must check whether the sent fax has been received by the authorized person or not.
- If the client consent is very narrow and/or the information being faxed is very sensitive, request that the receiving party wait for the fax to arrive and confirm receipt of the fax you have sent immediately upon receipt.
- Always double-check the number you have entered into the fax machine before sending the fax.

3. Reporting the Loss, Theft, or Breach of Client Information

Lost or stolen information is a serious breach of client privacy. Employees must report loss, theft, and potential breaches of client information to their Supervisor immediately. The Supervisor will notify the PCHS' Privacy Officer to determine what steps need to be taken in response to the breach. The Privacy Officer at PCHS is the Sr. Manager, Quality Assurance.. The Privacy Officer will inform the Chief Executive Officer.

5. Privacy Breach Protocol:

In case of privacy breach, PCHS will take the following steps:

Step 1: Employees/volunteers/ students must report all breaches of PHI to their Supervisor upon being discovered. The Supervisor will notify the Privacy Officer as soon as they are advised or become aware of a potential breach. The Privacy Officer will notify the Chief Executive Officer or their designate.

Step 2: Privacy Officer will book a meeting with the employees/volunteers/ students and Supervisor to obtain all the details regarding the breach (within 48 hours).

Step 3: Privacy Officer will conduct the investigation and create a report, and make sure that the affected individual(s) are informed about the breach. Privacy Officer's investigation and process should consider 'Containment' and 'Notification' following:

Containment: Identify the scope of the potential breach and take steps to contain it.

- Retrieve the /electronic copies of any personal information that has been disclosed.
- Ensure that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information and obtain the individual's contact information if follow-up is required.
- Determine whether the privacy breach would allow unauthorized access to any other personal information (e.g., an electronic information system) and take necessary steps are appropriate (e.g., change password, identification numbers and/or temporarily shut down a system).

Notification: Identify those individuals whose privacy was breached and barring exceptional circumstances, notify those individuals accordingly:

- Notify the individual whose privacy was breached, by phone or in writing.
- Provide details of the extent of the breach and the specifics of the personal information at issue. If financial information or information from government-issued documents are involved, include the following in notice:
  As a precautionary measure, we strongly suggest that you contact your bank, credit card company, and appropriate government departments to advise them of the breach. You should monitor and verify all bank accounts, credit cards, and other financial transaction statements for any suspicious activity.

VI. Principles for Protection of PHI

POLICY

PCHS is committed to protecting the confidentiality of the PHI in its control and custody. Any person who collects, uses, or discloses PHI on behalf of PCHS is required to adhere to the following information practices.

DEFINITION of Personal Health Information (PHI)

PHI is "identifying information" collected, whether in oral or recorded form, about a current, past, or potential PCHS client. It includes virtually any health information that pertains to an identified individual, including:

- Information concerning physical or mental health.
- Information about any services provided.
- Information collected while providing services.

Principle 1 - ACCOUNTABILITY for PHI

PCHS is responsible for the PHI in its control and custody and demonstrates its commitment by:

- Implementing policies and procedures to protect PHI.
- Ensuring all individuals who collect, use, and disclose PHI on behalf of PCHS receive training on PCHS' privacy/confidentiality policies and practices.
- Designating a Privacy Officer for the organization. **The role of the Privacy Officer is to:**
  - Provide training materials and/or training to PCHS employees.
  - Respond to privacy related inquiries.
  - Develop and review privacy policies for the organization.
  - Assess PCHS' privacy practices and compliance with the PHI Protection Act (PHIPA
  - Provide the CEO or the designate with advice, recommendations and information related to the PCHS' privacy practices.
  - Receive and respond to privacy complaints made against the organization under the supervision of the CEO.
  - Act as the liaison with the Office of the Privacy Commissioner/Ontario (if necessary).
  - The Privacy Officer is accountable to the CEO or designate of PCHS.

Principle 2 - Identifying Purposes

- PCHS advises individuals from whom it collects PHI, in terms of the purposes for which it is being collected, and it is only used for the purpose for which it was

collected.

- PHI is collected for purposes related to direct service provision to clients, administration and management of PCHS' programs and services, statistical reporting, research, teaching and fundraising as permitted by law.

- PCHS posts its "Statement of Information Practices" *(attached as Appendix D)* at PCHS locations- Malton and Brampton. PCHS makes a copy of its "Statement of Information Practices" available to all clients.

Principle 3 - Consent for Collection, Use and Disclosure of PHI

- PCHS relies on express written/verbal consent to collect, use, and disclose PHI. In some circumstances implied consent may be used when a written/verbal consent is not available. PCHS may disclose PHI as required by law without consent.

- Employees will use the Privacy, Confidentiality and Consent Form to obtain client consent for provision of PCHS services in collaboration with other healthcare/social services providers. These forms would be used for individuals and agencies that are part of the client's 'circle of care.' With the client's permission, family members or significant others can also be included on this form. When obtaining this consent, employees should follow the guidelines outlined in the 'client orientation package' with the client.

- If consent is required for communication and service coordination with non-health related individuals or agencies, the PCHS Privacy, Confidentiality, and Consent Form should be used.

- Clients have the right to refuse or revoke their consent at any time.

- PCHS has 'Use of Security Camera at Client's Home- Privacy Assurance Statement' (*appendix -E*) for the staff on home visits to ensure the privacy and safety of the staff members. This assessment will be completed for the clients who have security cameras installed at their homes.

Principle 4 - Limiting Collection of PHI

PCHS limits its collection of PHI to that which is required to provide services as identified in Identifying Purposes *(Principle 2).* Information is collected directly from the individual

or from third parties with the consent of the client for whom it is being collected or where the law requires collection from third parties.

Principle 5 - Limiting Use, Disclosure, and Retention of PHI

PCHS collects uses and discloses PHI for purposes related to direct provision of client services, administration and management of PCHS' programs and services, statistical reporting, research, teaching and fundraising as permitted by law.

PHI shall be retained only as long as necessary for the fulfillment of those purposes. It is generally accepted that information be retained for a period of up to 7 years or as legally years required.

Principle 6 – Accuracy of PHI

To the extent reasonably possible, personal information should be accurate, complete, up to date as is necessary for the purposes for which it is to be used.

Principle 7 – Ensuring Safeguards

PCHS has implemented safeguards for the security of the PHI in its control and custody which include:

Requirements for all persons who collect, use, and disclose PHI on PCHS' behalf to be aware of the importance of maintaining the confidentiality of PHI. This is done through privacy training, the signing of confidentiality agreements and contracts:

- Physical measures (i.e., , Locked cabinets/secure staff-only areas/Password protected cloud storage, as applicable)
- Only authorized access to confidential records
- Technological measures such as passwords, encryption, record locking and audit trails.

Principle 8 – Openness

Information about PCHS' policies and practices for the management of PHI include:

- Orientation Package - Client Orientation Package containing information about PCHS' privacy practices and policies.

- PCHS' Statement of Information Practices is posted on PCHS' website and available to all clients. and contains a description of the type of information held by PCHS, contact information for PCHS' Privacy Officer and contact information for

the Privacy Commissioner of Ontario.

- Obtaining access to PHI by submitting a request. Information is provided to clients as a part of 'client orientation package' (*Refer to Request Form for Access to Personal Health Records*)

Principle 9 - Individual Access

- All clients of PCHS have the right to review, read and obtain a copy of their record. Requests should be made in writing and directed to the attention of PCHS' Privacy Officer. (*Refer to Request Form for Access to Personal Health Records*).
- PCHS will respond to requests within 30 working days. In some cases, additional time may be required.
- Individuals who can demonstrate inaccuracies or incompleteness of their personal health records may request to have the record amended. Any changes, additions, deletions, concerns the client has, are to be recorded and added to the file. The original records are saved, as applicable.

Principle 10 - Challenging Compliance

- Complaints or challenges to PCHS' privacy policies and practices can be made to the PCHS Privacy Officer at 647-482-7354 or via email at Sheena@pchs4u.com
- PCHS will receive and respond to complaints or inquiries about its privacy policies/confidentiality and practices.
- If a complaint is found to be justified, PCHS will take appropriate measures to respond to the concerns. For additional information please contact the Privacy Officer.
- Obtain the name of caller (use sensitivity in asking) – the objective is to connect caller with the correct person at PCHS and ensure that PCHS employees know who they will be speaking to when they pick up the telephone.

Verification

My signature indicates receipt of and understanding of PCHS Privacy Policies and Procedures handbook (Page 1 to 12). I understand that if I violate the rules set forth in this policy, I may face legal, punitive, or corrective action, up to and including termination of employment.

Signature: _____

Print Name: _____

Date: _____