Reconnect Health Services:

Privacy Policy and Procedures

EFFECTIVE DATE: NOVEMBER 2020

CONTENTS

INTRODUCTION

Reconnect recognizes the importance of privacy and the sensitivity of its clients' personal health information and other personal information (**Client Information**). The purpose of this policy is to protect the privacy of Reconnect clients and ensure that Client Information is collected, used, disclosed, retained and disposed of in a manner consistent with this policy, applicable laws and agreements.

Reconnect is a "health information custodian" under Ontario's *Personal Health Information Protection Act, 2004* (**PHIPA**), and will comply with the obligations outlined by the act. Reconnect provides services to children and youth and, as such, also complies with its obligations under the Child, Youth and Family Services Act.

Reconnect's commitment to protecting Client Information is reflected in its policies and procedures, which are designed to follow the principles set out in the Model Code for the Protection of Personal Information (**Code**) as reflected in PHIPA.

The Code's 10 principles are:

1. **Accountability:** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. **Identifying Purposes:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. **Consent:** The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate (e.g. if the client is unable to consent or has a substitute decision maker).

4. **Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure, and Retention:** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for fulfillment of those purposes.

6. **Accuracy:** Personal information shall be as accurate, complete, and up to date as necessary for the purposes for which it is to be used.

7. **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness:** The organization shall make specific information about its policies and practices relating to the management of personal information readily available.

9. **Individual Access:** Upon request, an individual shall be informed of the existence, use and disclosure of their personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Challenging Compliance:** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

SCOPE OF POLICY/REVIEW

All Reconnect employees (whether working directly with clients or not), directors, volunteers, students and contractors who have access to Client Information (e.g. psychiatrists) are required to understand and comply with this Privacy Policy and Procedure. Annual confirmation of compliance with the Policy and maintenance of confidentiality is required as part of the annual performance review process. Any breach of this Policy may result in significant disciplinary action, including suspension and termination.

This policy will be reviewed as required to respond to changes in the law and best privacy practices.

DEFINITIONS

"Agent" means any person who acts on behalf of Reconnect for Reconnect's purposes, and includes Reconnect's employees, directors, volunteers, students and contractors who have access to Client Information.

"Client" refers to any person who is receiving or is about to receive services from Reconnect.

"Client Information" means the information about the client that Reconnect collects, in whatever media or format, and whether such information is expressed in English or another language. Client Information includes PHI but may be broader than PHI and include other identifying information.

"Code" means the Model Code for the Protection of Personal Information, which is set out in the federal privacy legislation, the *Personal Information Protection and Electronic Documents Act* (**PIPEDA**) and embedded within PHIPA.

"Consent Directive" means where a client has withheld or withdrawn their consent to the collection, use or disclosure of all or a part of their PHI. A Consent Directive can be given orally by a client, but must be documented by the Reconnect Staff in the Client record.

"Corporate Services Staff" means administrative staff within Reconnect who do not provide program services directly to Clients.

"Health Information Custodian" or **"HIC"** is a listed individual or organization under PHIPA that, as a result of their power or duties, has custody or control of Personal Health Information. Examples of health information custodians include health care practitioners, hospitals, psychiatric facilities and individuals or organizations that operate a program, service, or centre for community health that's primary purpose is the provision of healthcare (which includes physical and mental conditions).

"Integrated Assessment Record" or **"IAR"** means the computer application implemented in Ontario that allows authorized users to view a consenting client's assessment information done by other providers.

"Personal Health Information" or **"PHI"** is defined in PHIPA and generally refers to identifying information (in oral or recorded form) pertaining to an individual's health or health services.

"PHIPA" means the *Personal Health Information Protection Act, 2004* and regulations thereunder.

"Policy" means this Privacy Policy and Procedures.

"Program Staff" means Reconnect staff who deliver programs and services directly to Clients.

"Reconnect Staff" means Corporate Services Staff, Program Staff and all other staff employed or engaged by Reconnect.

"Substitute Decision Maker" or "SDM" means a person authorized under PHIPA to consent on behalf of a client to the collection, use or disclosure of their PHI.

PRIVACY PRINCIPLES AND PROCEDURES

ACCOUNTABILITY

Reconnect is responsible for Client Information under its control and shall designate an individual (or individuals) who is (are) accountable for Reconnect's compliance with this Policy.

Reconnect's privacy officer is the contact person for all issues related to the confidentiality of Client Information. Their responsibilities include investigating and managing privacy breaches and incidents, fostering compliance with confidentiality and privacy-related policies and procedures, and the provision of training for Reconnect Staff.

Reconnect's privacy officer may be reached at:

Privacy Officer, Reconnect Community Health Services

1281 St. Clair Ave. W.

Toronto, Ontario, M6E 1B8

Tel: 647-580-7059 Fax: 416-248-6557

E-mail: privacy.officer@reconnect.on.ca

The privacy officer and chief executive officer shall deal with any privacy-related policy issues and implement any organization-wide changes that are required to comply with this policy. Overall accountability for Reconnect's compliance with this policy and privacy law rests with the Senior Management Team of Reconnect and, ultimately, with the Board of Directors.

All Reconnect staff, directors, volunteers, students and contractors who have access to Client Information will sign and be bound by the *Reconnect Pledge of Confidentiality* and by this policy. This pledge is renewed annually, at the time of the individual's performance review.

IDENTIFYING PURPOSES

The purposes for which Client Information is collected shall be identified by Reconnect at or before the Client Information is collected.

Reconnect collects Client Information for the following purposes:

- Coordinated and effective healthcare and related services to clients
- Sharing information within the client's circle of care
- Referrals to other related programs
- Planning, delivering and evaluating programs and services
- Quality assurance
- Reporting aggregate information and statistics to funders
- Payment or processing payment for healthcare
- Research conducted by Reconnect (in accordance with privacy legislation)
- Other purposes permitted or required by law

Upon a person's enrollment as a client, program staff will advise the client about the purpose of collecting Client Information. Reconnect has a Privacy Statement and other privacy information posted and available to clients. Program staff will provide the client with consent forms to sign where required, in order to lawfully collect and share Client Information. Clients may access or request a copy of the Privacy Policy posted on Reconnect's website. The Privacy Policy on the website is a shorter version of this policy and does not include the procedures. Clients may also have a copy of this Privacy Policy and Procedures, upon request.

CONSENT

The knowledge and consent of the client are required for the collection, use or disclosure of Client Information, except when inappropriate.

TYPES OF CONSENT

In order to provide coordinated and effective health care, it is important that Reconnect collect Client Information from other service providers and share information about clients with such providers.

There are three types of consent under PHIPA: (1) express (2) implied and (3) assumed implied consent.

(1) **Express Consent** – a client directly agrees to the handling of Client Information. Express consent may be oral or written.

(2) **Implied Consent** – a person reasonably concludes from the surrounding circumstances that the Client would consent to the handling of Client Information.

(3) **Assumed Implied Consent** – generally refers to the sharing of PHI among specific HICs for the provision of healthcare to a person. This is often referred to as "circle of care" and is described in Section (c) below.

Reconnect's Consent Practices

Reconnect relies on implied consent and assumed implied consent when sharing Client Information within the "circle of care" as further described in Section (c) below.

Reconnect seeks express consent when we:

(1) share Client Information with a person/entity that is not a health information custodian; and

(2) share Client Information with another HIC for purposes other than the provision of healthcare.

In circumstances (1) and (2) above, Reconnect Staff should endeavor to obtain express written consent. From time to time, express written consent may not be possible. Express oral consent is acceptable when clients are unwilling or unable to sign a Consent Form (but otherwise consent to the sharing of such information) and such consent is to be documented in the client's file.

Reconnect Staff shall obtain express written consent when Reconnect:

(1) collects, uses or discloses PHI for marketing purposes.

(2) collects, uses or discloses PHI for research purposes (unless certain conditions are met).

(3) collects, uses or discloses PHI for fundraising (other than an individual's name and mailing address).

- Please see the Obtaining and Documenting Client Consent procedure.
- Please see Section (k) for a discussion of Reconnect's consent form.

ELEMENTS OF CONSENT

For consent to be valid the following four elements must be satisfied:

(1) **Capacity -** The client must have the capacity to consent. The test for capacity is discussed in Section (d) below.

(2) **Knowledgeable** - Consent must be knowledgeable. They must understand the reason for the collection, use and disclosure of Client Information and their right to refuse or withdraw consent.

(3) **Voluntary** - Consent must be voluntary.

(4) **Relate to the Information** - Consent must be related to the information in question.

CIRCLE OF CARE

The term **"circle of care"** is not used in PHIPA. It refers to a situation where certain HICs can rely on "assumed implied consent" of clients to share PHI with other specific HICs, **solely** for the purpose of healthcare. This does not require express or implied consent; the elements of consent are assumed to have been fulfilled.

There are six conditions that must be met to fall within the circle of care:

(1) The HIC collecting, using or disclosing the PHI must fall into a category of HICs that are permissible (**Permissible HICs**). Permissible HICs include all HICs, except for evaluators, assessors, the Minister or Ministry of Health and Long-Term Care, Medical Officer or Board of Health.

(2) The PHI collected, used or disclosed by a Permissible HIC must have been received from the individual, SDM or another Permissible HIC.

(3) The PHI must have been received for the provision of healthcare to the individual.

(4) The purpose of the collection, use or disclosure of the PHI must be for healthcare to the individual.

(5) If PHI is to be disclosed, it must be disclosed to another Permissible HIC.

(6) The HIC that discloses or receives the PHI must not be aware of an instruction from the client to lock-box the PHI to be shared. See Section (h) below for a definition of "**lock-box**".

CAPACITY TO CONSENT FOR DECISIONS UNDER PHIPA/SUBSTITUTE CONSENT

A person may consent to the collection, use or disclosure of PHI if the person has the capacity to do so. The test for capacity under PHIPA, is whether the person (1) can understand the information relevant to a decision under PHIPA **and** (2) can appreciate the reasonably

foreseeable consequences of making (or not making) a particular decision. In this Policy, we use PHIPA's explanation of capacity for decision-making.

An individual is presumed to be capable of making decisions under PHIPA, unless there are reasonable grounds to believe that the individual is incapable of making such decision. The HIC (i.e. Reconnect) may determine capacity for purposes of providing consent required under PHIPA. The HIC would use its agents (e.g. psychiatrists, social workers) to determine capacity.

If a person is found to be incapable of making decisions under PHIPA, it is best practice to document that finding in the client's health record. In addition, Reconnect must determine the appropriate substitute decision maker (SDM). The list of SDMs in order of priority are:

(1) Guardian of the person
(2) Attorney for personal care
(3) Representative appointed by the Consent and Capacity Board
(4) Spouse/partner
(5) Child or parent of the incapable person (including children's aid society)
(6) Parent of the incapable person with only a right of access
(7) Brother or sister
(8) Any other relative of the incapable person
(9) Public Guardian and Trustee

The SDM must be the highest-ranking SDM and must also be:

- Capable
- at least 16 (unless the parent of the incapable person)
- not prohibited from access or consenting
- willing and available to assume the responsibility.

If the decision under PHIPA relates to a decision about treatment, admission to a care facility or a personal assistance service, and the client has an SDM for one of those purposes, then the SDM for treatment, admission to a care facility or a personal assistance service (whichever applies) is the SDM for purposes of PHIPA.

It is best practice to confirm who is the highest ranking SDM (i.e. ask whether there is a guardian of the person or attorney for personal care, spouse, parent etc.) and to document the name and position of the SDM. If there is a guardian or attorney for personal care, then there will be an associated guardianship order, or power of attorney for personal care. A copy of the guardianship order or power of attorney should be requested and scanned into the patient record.

If there is any doubt about determining capacity or the appropriate SDM, consult with the privacy officer.

CONSENT IF CLIENT IS DECEASED

If the client has died, the client's estate trustee or the person who has assumed responsibility for the administration of their estate (if the client does not have an estate trustee) is authorized to consent to decisions under PHIPA. When dealing with a consent matter for a deceased client, the privacy officer must be consulted.

EXCEPTIONS TO CONSENT

There are several situations under PHIPA, where it is permissible to collect and disclose Client Information without consent. The privacy officer must be informed and will document all exceptions to client consent. Exceptions to consent include:

- If Reconnect Staff have reasonable grounds to believe that the disclosure of Client Information is necessary to eliminate or reduce a significant risk of serious bodily harm to a person or group of people.
- The duty to report to Children's Aid Society for a child in need of protection under the *Child, Youth and Family Services Act*

Although, as discussed above, there are situations where it is permissible to disclose Client Information without consent, it is still best practice to seek informed consent. If consent is not possible, it is still best to inform clients that their Client Information will be disclosed, unless such a discussion is inappropriate. If a program staff member requires advice about this, they should discuss the situation with their manager or the privacy officer.

DISCLOSURES PURSUANT TO COURT ORDERS/DEALING WITH POLICE REQUESTS

It is Reconnect policy that no Client Information be disclosed to police in the absence of a valid legal document from the court, such as a subpoena.

If the disclosure of Client Information is required under a warrant, subpoena or other legal document, this must be brought to the privacy officer. The privacy officer may seek legal counsel to determine whether the document is valid and will handle the disclosure of Client Information with the assistance of the chief executive officer and program staff.

Any contact with, or information requested by, the police must go through the chief executive officer.

LOCK-BOX

Clients have the right to withhold or withdraw their consent to the collection, use or disclosure of all or a part of their PHI. This is referred to as the "lock-box" (although the term is not used or defined in PHIPA). It is also referred to in this Policy as a Consent Directive.

As examples of lock-box, clients may expressly require staff **not to**:

- Collect, use or disclose a particular item in their health record (e.g. diagnosis).
- Collect, use or disclose their entire health record (e.g. to another HIC).

- Disclose their PHI to a particular HIC, employee or a class of HICs (e.g. a particular worker at Reconnect that knows the client).
- Allow a particular HIC or employee or a class of HICs to use their PHI.

Reconnect staff can discuss with the client how locking the PHI may affect their healthcare and why Reconnect may need the PHI to provide the best care. However, the decision remains that of the client.

If a client requests a form of lock-box (either orally or in writing), this is referred to as a Consent Directive and must be documented in the client record so that other Reconnect Staff also know to respect the lock-box. If Reconnect staff have any questions about how to appropriately document a lock-box, the privacy officer should be contacted for assistance.

There are some exemptions from the lock-box, such as when disclosure is necessary to reduce a significant risk of harm to oneself or others. The privacy officer needs to be consulted if there is to be an exemption from the lock-box.

Where PHI has been locked and Reconnect is prevented from disclosing the PHI to a HIC (which Reconnect considers reasonably necessary for healthcare), Reconnect must notify the receiving HIC of that fact.

CLIENT WITHDRAWAL OF CONSENT

The client may withdraw consent to share PHI at any time, although this does not function retroactively for PHI previously shared. Should the client choose to withdraw consent, the program staff will explain the implications of the consent withdrawal. If the client still wishes to withdraw consent, the program staff will use the electronic client management to note that consent has been withdrawn, and no further information will be shared.

If a client has signed a consent form and subsequently wishes to withdraw such consent, the client shall sign the Withdrawal of Consent Form.

CLIENTS WHO HAVE BEEN DISCHARGED

If a client has been discharged from Reconnect and re-engages with Reconnect, they must be informed again of Reconnect's information management and privacy protocol. If there is a request to share previous Client Information with another HIC for the purpose of providing healthcare, then the Client Information may be shared. However, if the Client had a Consent Directive, then express consent would be necessary to share the Client Information.

CONSENT FORM

There is only one Client Consent Form in use at Reconnect (Consent to Collection and Disclosure of Personal Health Information). **This consent form authorizes the sharing of information between Reconnect and specific providers/persons and is to be used for situations where express written consent is required. There may be multiple consent forms signed if express written consent is required for different providers/persons.**

For clients receiving on-going services from Reconnect, the Consent Form(s) will be valid for the entire period during which they receive service from Reconnect, unless the client indicates otherwise.

The Express Consent Decision Tree on the next page can be used to determine if express consent is required.

DISCLOSURE OF CLIENT INFORMATION TO NON-HICS

Client Information will be disclosed to non-HICs (such as schools and family members) only with the express consent of the client. Staff will work with the client to explain the rationale for sharing information. Staff will document the information that has been disclosed and will consult with the privacy officer if there is any concern about disclosures.

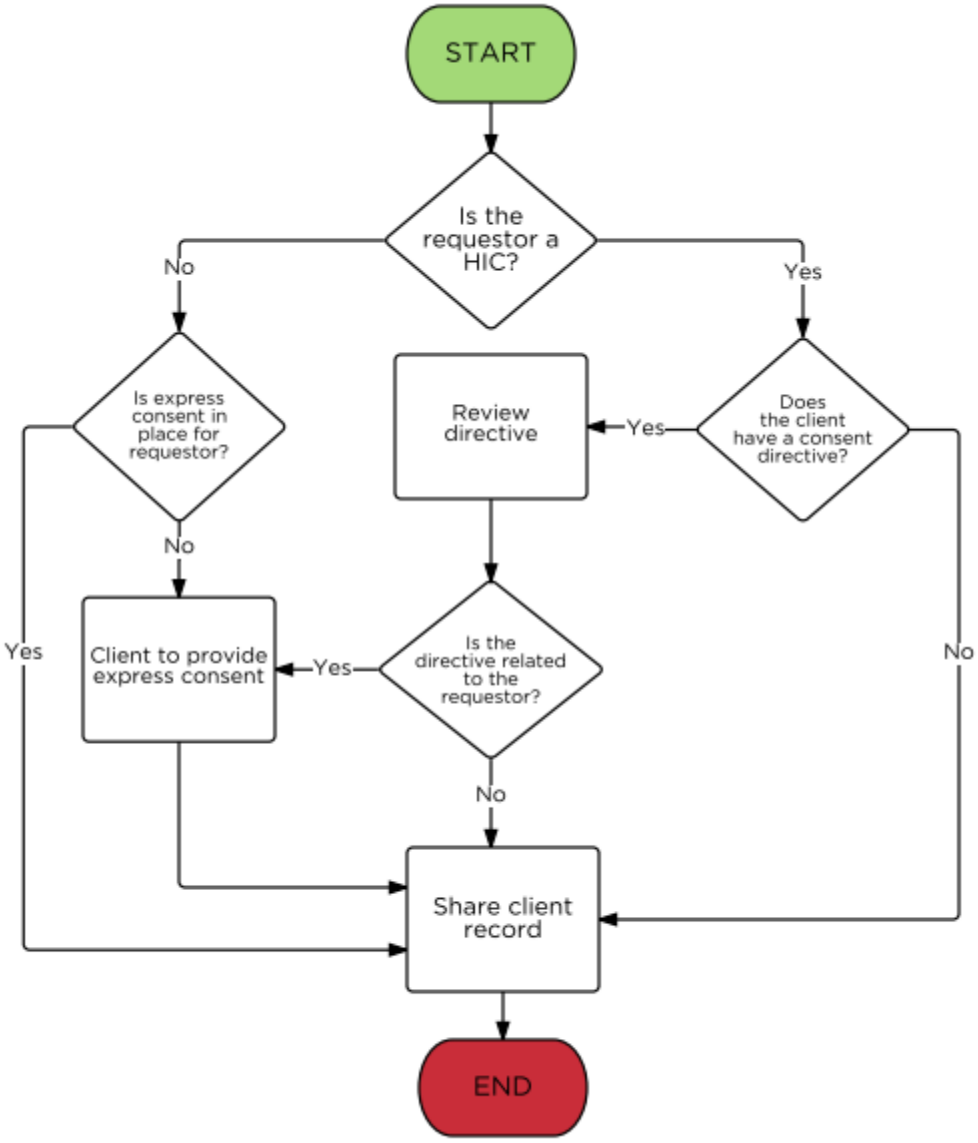
PHOTO/RECORDING CLIENTS

A client's participation in any Reconnect program is confidential; therefore, taking photographs and recordings of clients (video and audio) should be given the same consideration as the use of other confidential information.

Express written consent must be given by the client before any photos or recordings (individual or group) are taken. Reconnect Staff will explain the purpose for which the photograph(s) or recording (s) will be used, and request that the client give written consent by completing a specialized consent form available from the privacy officer. Photographs and recordings will be used and/or distributed only as agreed to by the client. Videos taken for training purposes will be on a specified device. A specified destruction date must be established and a consent form signed before any recording can begin.

EXPRESS CONSENT DECISION TREE

The Decision Tree below can be used to determine if express consent is required.


START
Is the requestor a HIC?
No
Yes
Is express consent in place for requestor?
Review directive
Yes
Does the client have a consent directive?
No
Client to provide express consent
Yes
Is the directive related to the requestor?
Yes
No
No
Share client record
END

LIMITING COLLECTION

The collection of Client Information shall be limited to that which is necessary for the purposes identified by Reconnect. Client Information shall be collected by fair and lawful means.

Reconnect will only collect the information required to provide clients with optimal care and for the other purposes specified in Principle 2 above. Collection will be carried out by fair and lawful means and in accordance with PHIPA and other relevant legislation.

LIMITING USE, DISCLOSURE, AND RETENTION

Client Information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required (or permitted) by law. Client Information shall be retained only as long as necessary for fulfillment of those purposes.

SHARING INFORMATION

All information about a client's involvement with Reconnect must be considered confidential. It must not be shared with anyone outside of Reconnect, except when permitted or required by law. Although the Code refers to sharing as "required" by law, PHIPA is a permissive statute that allows collection, use and disclosure without consent in certain circumstances. Reconnect will not disclose PHI if other information can serve the same purpose and will not disclose more Client Information than is reasonably necessary to meet the purpose. Reconnect shall not use or disclose Client Information other than for the purposes for which it was collected.

RETENTION AND DESTRUCTION

All Client Information is to be recorded and stored in the electronic client management system. Hard copy documents are scanned and stored in the system and then shredded. Client Information must not be copied from the electronic client management system or Reconnect's network. If such information is required while working in the community, it can be accessed directly from the network and saved to the network wherever possible. In specific instances, it may be necessary to have hard copy documents while in the community; if this is absolutely necessary, they must be kept secure at all times.

Reconnect keeps electronic copies of Client Information for as long as necessary to fulfill the purposes for which it was collected, or as required or permitted by law.

Where a client has requested access to their record, or the record has been identified as potentially relevant in a known or reasonably anticipated litigation or investigation by a government entity (e.g. Information and Privacy Commissioner/Ontario), Reconnect will retain that record until the access request, litigation or investigation is exhausted.

Reconnect's Services for Seniors programs store paper files in a locked area on-site. Paper files more than seven years old are destroyed by a professional paper shredding company.

NOTE: In 2011, all paper records for health services Clients who were active within the previous ten years were scanned and stored electronically. Paper records from before 2001, for clients who were not active in the following ten years, were shredded.

ACCURACY

Client Information shall be as accurate, complete, and up to date as is necessary for the purposes for which it is to be used.

All Client Information should be recorded completely, correctly, and in a timely manner. Reconnect will take reasonable steps to ensure this is done, and that PHI is as accurate as necessary. Reconnect will update this information when routine updates are necessary to fulfill the purposes for which the information was collected. When Reconnect becomes aware that information is not accurate, complete, or up to date, this will be indicated at the time of use or disclosure, and the appropriate corrections and updates will be made.

A Client's health record is comprised of all the information pertinent to their involvement with Reconnect, including electronic records (the electronic client management information system), hard copies of documents that have not been scanned, handwritten notes and generic information that includes Client Information). Corporate Services staff will create the initial electronic records for new clients and will assist program staff in maintaining client records. Program staff are responsible for ensuring that Client Information is completed correctly, in a timely manner, includes all pertinent information, and is stored appropriately and securely.

SAFEGUARDS

Client Information shall be protected by security safeguards appropriate to the sensitivity of the information.

Reconnect recognizes the sensitivity of PHI and takes reasonable measures to ensure that Client Information is kept safe from loss, theft, unauthorized access, use, copying, disclosure, or modification. Reconnect has several policies in place to maintain the security of Client Information, including the Computer Use Policy.

Client Information in Reconnect's custody or control is protected by security physical, administrative and technical safeguards, including:

- Restricted access to information stored electronically, including an electronic health record which is password protected and may only be used by authorized staff.

- Premises security, including locked filing cabinets, ensuring client information is locked up when not in use and central desk control for visitors.
- Securely shredding materials that are no longer required.
- Using technological safeguards such as security software and firewalls to prevent hacking or unauthorized computer access.
- Initial and ongoing privacy training for staff.
- Destruction of client information in a secure manner, using destruction methodologies appropriate to the format, media or device, such that reconstruction is not feasible.
- Promptly scanning hard copy documents into the electronic client management system and shredding hard copies.
- Entering into contracts with third parties (e.g. contractors, volunteers) who may have access to Client Information to test our security safeguards.

In order to prevent accidental disclosure, Client Information must not be copied from the electronic client management system or Reconnect's network. Reconnect Staff are discouraged from carrying Client Information outside of Reconnect's premises.

All mobile data storage devices must be protected by a strong password and are encrypted.

Staff working in the community may need to document PHI onto their laptops or other mobile data storage devices. This must be encrypted. When doing so, extreme care must be taken to ensure the security of that information. All PHI created on any mobile device must be deleted from the mobile device as soon as it is no longer required for immediate use. Refer to the Computer Policy for further details.

Email and texting are not considered secure methods of communication; however, they are a commonly used and convenient way to send information to, and on behalf of clients. While staff are discouraged from sending any client PHI electronically, if the client has been made aware of the risks involved and consents to do so anyway, staff may use email and text to send information. Staff have the option of encrypting attached documents and/or limiting the amount of PHI in the message. If both staff and the receiver of the email are using OneMail, sending unencrypted PHI is permissible. When communicating electronically about a client, staff should only reference the client's initials and their client management system number.

All hard copy documents containing confidential Client Information that are required while working in the community must be kept secure in the red envelope provided for such documents. These must be shredded immediately when no longer required.

Reconnect periodically reviews staff access to the electronic client records (see Auditing Client Management Systems' procedure). If it is suspected that Client Information has been accessed inappropriately (sometimes referred to as 'snooping'), the privacy officer will investigate, including reviewing the audit logs of the client management system.

Reconnect responds promptly, effectively and sensitively, in accordance with all laws and requirements to any unauthorized collection, use, or disclosure of Client Information. Please Refer to Section E for Reconnect's Privacy Breach/Incident Protocol.

OPENNESS

Reconnect shall make specific information about its policies and practices relating to the management of Client Information readily available to individuals.

Reconnect's Privacy Policy and Privacy Statement are available to the public on the Reconnect website. Additionally, clients may obtain a copy of this Privacy Policy and Procedures upon request. Program staff will speak to clients about privacy and how their Client Information will be used and safeguarded. The privacy officer is always willing to meet with clients to address their questions or concerns about privacy. Reconnect will develop privacy brochures which will be available to clients.

INDIVIDUAL ACCESS

Upon request, an individual shall be informed of the existence, use and disclosure of their Client Information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

A client may request access to any records in Reconnect's custody or control that contain Client Information, by writing to Reconnect's privacy officer. A client will receive at least a preliminary response from the privacy officer as soon as possible (within a maximum of 30 days), and a full response within 60 days.

A client's right to access their information is not absolute. There are several exceptions, such as if the information is subject to legal proceedings, if it could result in a risk of serious harm to the treatment or recovery of the individual, or if it poses a risk of serious bodily harm to the individual or another person. If the privacy officer refuses an access request, they will give the client a clear reason, and the client will be notified of their right to lodge a complaint with the Information and Privacy Commissioner of Ontario. When a client is incapable of making decisions under PHIPA, the SDM may exercise the rights of access to a health record.

Where a client has requested access to their record, Reconnect will retain that record until the access request is exhausted. Any disclosure from the client's file is documented in the client's file.

A client is entitled to challenge the accuracy or completeness of any of their information in Reconnect's custody or control. Requests to challenge and/or change information should be directed to the privacy officer. A client will receive at least a preliminary response from the privacy officer as soon as possible (within a maximum of 30 days), and a full response within 60 days.

CHALLENGING COMPLIANCE

An individual shall be able to address a challenge concerning compliance with the above principles.

Clients are entitled to challenge Reconnect's compliance with this policy. Any challenge should be put in writing and directed to Reconnect's privacy officer. If a client has difficulty putting the challenge into writing, assistance will be provided. Anyone who submits a written complaint, challenge or inquiry will be given a written copy of Reconnect's procedures governing such complaints, challenges and inquiries.

Reconnect will investigate all complaints received. If a complaint is found to have merit, Reconnect will take appropriate measures to address the complaint, including, if necessary, taking disciplinary action against Reconnect staff and amending its policies relating to the management of information.

If a client has any issues or concerns about how their Personal Health Information is being handled, they have the right to contact the Reconnect privacy officer as well as the Information and Privacy Commissioner of Ontario at:

Office of the Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, ON M4W 1A8
Phone: 416-326-3333 or, 1-800-387-0073 or, TDD/TTY: 416-325-7539
Online: http://www.ipc.on.ca

PRIVACY BREACH/INCIDENT PROTOCOL

DEFINITIONS

*"**Privacy Breach"** or "**Breach"** means an unauthorized collection, use, access, copying, modification, disclosure, retention, exposure or disposal of PHI. Any person can become aware of a privacy breach. The breach may be deliberate or inadvertent, and may be a breach of privacy law, contract and/or policy.*

*"**Privacy Incident"** or **"Incident"** or **"Near Miss"** means the contravention of a Reconnect policy or procedure, legal duty or contractual obligation that results in the potential exposure of Personal Health Information to unauthorized persons; however, in these cases, the breach Investigation determines the information was only shared with authorized parties.*

***"Privacy Breach Management"** means the end-to-end management of a series of events that are initiated in response to a suspected privacy breach.*

Although Reconnect always strives to protect Client Information, there may occasionally be a privacy breach or privacy incident. Privacy breaches may be detected by Reconnect staff (e.g. printed client records are lost, user account and password are compromised), a client (e.g. a client finds out their ex-spouse is working at Reconnect and inappropriately accessed their health record for a child custody case), or a third party (e.g. a server at a restaurant finds a list of Reconnect Clients).

This section sets out the protocol to follow in the case of a suspected breach. The aim is to first determine if a breach has occurred and then to contain and remedy the breach. If the breach relates to the Integrated Assessment Record, additional steps are required. Please consult the privacy officer to implement these additional steps if the breach relates to the IAR.

Reconnect's privacy officer is the contact person for all aspects of privacy breach management, including containment, investigation and resolution of all privacy breaches and privacy incidents (whether related to Reconnect Client Information or the IAR).

STEPS TO FOLLOW IF A PRIVACY BREACH IS SUSPECTED

The steps below use the term "privacy breach". However, the steps below are to be followed (to the extent applicable) in the event of a suspected privacy breach **or** a privacy incident. By the end of the process, Reconnect is usually able to determine if a privacy breach has occurred or whether the occurrence would be more appropriately defined as a privacy incident.

Detection and Reporting

1. When a privacy breach is suspected, the person suspecting the breach must immediately (i.e. on the same day) report it to Reconnect's privacy officer by phone or email (without identifying information).

2. The privacy officer will verbally contact the appropriate Reconnect staff to get as much detail about the breach as possible and to discuss, in general terms, how to proceed.

Containment

3. Containment of information related to the privacy breach is a critical priority. The privacy officer will work with appropriate Reconnect staff to contain the breach so that no further Personal Health Information is exposed.

Privacy Breach Report Form

4. The privacy officer will email (or will provide instructions on how to access) a copy of the *Privacy Breach Report Form* to the Reconnect staff.

5. Reconnect staff will complete sections 1 and 3 of the *Privacy Breach Report Form* before the end of the next business day and save it to the Reconnect Main Drive in the Breach Management Folder (as further specified in the Privacy Breach Report Form). The Reconnect staff will notify the privacy officer via email that the form has been completed.

Investigation

6. The privacy officer will start an investigation, which will involve all appropriate individuals (e.g., the chief executive officer, the clinical team, the management team, lawyers, etc.). Details of the breach should be discussed only among those directly involved with the investigation.

7. The privacy officer will determine if the privacy breach involves the IAR. **IF YES,** then the privacy officer (in consultation with Reconnect Staff) will follow the additional steps required by the IAR Specific Breach Procedures.

Determination of Breach versus Incident

8. Upon completion of the investigation, the privacy officer will evaluate if PHI was shared with unauthorized parties. If so, this will be considered a **PRIVACY BREACH** and the client must be notified, as outlined in PHIPA. If Reconnect procedures were not followed but information was not shared with unauthorized parties, this will be considered a **PRIVACY INCIDENT.**

Notification

9. The privacy officer or designate will notify all affected clients of privacy breaches. This will be done in consultation with the client's clinical team.

10. The privacy officer will notify the Information and Privacy Commissioner/Ontario if, in consultation with the chief executive officer, this is deemed necessary.

Recommendations

11. If, as a result of the investigation, there are recommendations for improvements to procedures to prevent future breaches, these are to be added to the ***Privacy Breach Report Form*** along with an implementation plan.

Documentation

12. The privacy officer will complete the balance of the Privacy Breach Report Form started by Reconnect staff.

13. The privacy officer will document the privacy breach in the client's electronic chart.

14. The privacy officer will add this privacy breach or incident to the master tracking form.

15. Starting in 2019, the Information and Privacy Commission of Ontario requires annual statistical reporting of all breaches for the previous year. The privacy officer will compile and submit these reports quarterly to Reconnect's CEO, and annually to the IPC.

APPROVAL AND REVISION HISTORY

Policy Name	Revision Date	Change (Minor/Major or N/A)	Policy Owner	Approved By/Date	Related Policies	Next Review
Privacy Policy and Procedures	New Policy	N/A	Privacy Officer	Senior Management Team ***April 26, 2016**	• Guiding Principles for Employment at Reconnect • Reconnect Pledge of Confidentiality • Computer Use Policy • IAR Specific Breach Procedures	Major changes in Privacy Best Practices or Legislation
Privacy Policy and Procedures	April 2018	Minor	Privacy Officer	Senior Management Team - April 2018	Consolidation of privacy policies for SCWSS and Reconnect Creation of procedures on 1) how staff should obtain, document and update consent in each client management system, 2) regular auditing of each of Reconnect's CMS', 3) file retention and destruction policies	Major changes in Privacy Best Practices or Legislation
Privacy Policy and Procedures	May 2019	Minor	Privacy Officer	CEO – June 2019	Acknowledgement of obligations to clients who are under the age of 18 through the Child, Youth and Family Services Act. Updating email and text policy.	Major changes in privacy best practices or legislation
Policy	September 2021	Major	Director, HR	CEO, COO – September 1, 2021	COVID-19 Vaccination and Antigen Rapid Testing Policies, per Directive #6 from the Ministry of Health	Major changes in privacy best practices or legislation

COPYRIGHT NOTICE/DISCLAIMER