

SECTION III:

SERVICE DELIVERY

Subsection: FRAMEWORK FOR SERVICE DELIVERY

Policy Title: Privacy and Confidential Personal Health Information

Policy Number: III, 1.5

Initial Date of President and CEO Approval: 2024-10-30

Last Review/Revision Date: 2025-04-16

Purpose

The purpose of this policy is to detail the expectations of the Organization about how the health and personal information about clients and their families acquired at the Organization will be protected. It clearly defines the Organization's collection, use, storage, and disclosure of the Personal Health Information of its client.

Application

All Strides Toronto employees, volunteers, students, vendors, contractors, and any other agent who encounters client information for the purposes of their work with Strides Toronto.

Definitions

N/A

Policy

Strides Toronto (the Organization) is committed to ensuring client¹ privacy and to protecting the confidentiality of the client information the Organization holds.

Strides Toronto is a Health Information Custodian (HIC) under the *Personal Health Information Protection Act, 2004* (PHIPA). Strides Toronto is accountable and liable for compliance with PHIPA and the protection of all personal health information and health records in its possession.

Strides Toronto is also a service provider under the *Child, Youth and Family Services Act, 2017* (CYFSA). In relation to programs and services that fall under CYFSA, Strides Toronto is accountable and liable for compliance with Part X of the CYFSA and the protection of all Strides Toronto service recipient records of personal information.

All the Organization's employees, volunteers, students and vendors and any other agents (contractors and others) will abide by this policy and reflect Strides Toronto's commitment to protecting client information.

This policy acts as the articulation of privacy and confidentiality practices and standards to guide Strides Toronto employees and any others who collect, use, or disclose client information. There are additional privacy and confidentiality procedures referenced below and listed in Cross References with which the Organization shall also comply.

Principle 1: Accountability for Personal Health Information and/or Client Personal Information

Strides Toronto is responsible for any personal health information and/or client personal information Strides Toronto holds.

¹ Client refers to a person served.

Policy Title: Privacy and Confidential Personal Health Information**Policy Number:** III, 1.5

The Organization will appoint a Privacy Officer to ensure compliance with this policy and any relevant legislation, including PHIPA and Part X of the CYFSA.

Strides Toronto's commitment to privacy and confidentiality is demonstrated by adherence to the Organization's policies and procedures to protect the client information Strides Toronto holds and by educating employees and any others who collect, use, or disclose client information on the Organization's behalf about their privacy and confidentiality responsibilities.

Principle 2: Identifying Purposes for Collecting Personal Health Information or Client Personal Information

Strides Toronto collects personal health information for purposes related to direct client service, administration and management of Strides Toronto's programs and services, client billing, administration, and management of the health care system and/or of service delivery, research, teaching, statistical reporting, quality improvement, meeting legal obligations and as otherwise permitted or required by law.

Strides Toronto may de-identify health information and allow it to be used by third parties.

When personal health information that has been collected is to be used for a purpose not previously identified, the new purpose will be identified prior to use. Unless the new purpose is permitted or required by law, consent will be required before the information can be used for that purpose.

Principle 3: Consent for the Collection, Use and Disclosure of Personal Health Information and Client Personal Information

In general, Strides Toronto requires consent to collect, use, or disclose Personal Health Information. However, there are some cases where the Organization may collect, use, or disclose Personal Health Information or client personal information without consent as permitted or required by law.

Implied consent (Disclosures to other health care providers for health care purposes to another) – Circle of Care

Client information may be released to a client's other health care providers who are Health Information Custodians for health care purposes (within the "circle of care") relying on implied consent and without requiring the express written or verbal consent of the client if it is reasonable in the circumstances to believe that the client wants the information shared with the other health care providers.

No client information will be released to other health care providers if a client has stated they do not want the information shared (for instance, by way of the placement of a "lockbox" or "consent directive" on their records).

A client's request for treatment or service constitutes implied consent to use and disclose their personal health information for health care or service delivery purposes unless the client expressly instructs otherwise.

Who can be in the "**Circle of Care**" includes (among others providing direct client care if authorized by PHIPA):

Within Strides Toronto:

- All employees, students and volunteers are involved in service provision for the client or family.
- Any individual who may have access to client information, including Strides Toronto sub-contractors, and others (such as psychologists, psychiatrists, etc.)

Outside of Strides Toronto: Disclosure to other Health Information Custodians:

Policy Title: Privacy and Confidential Personal Health Information**Policy Number: III, 1.5**

-
- Primary care and specialists: doctors' offices, family health teams, nurse practitioner-led clinics, birth centers
 - Hospitals
 - Regulated health professionals or social workers and social service workers in solo or group practice
 - Ambulance and paramedics
 - Pharmacies
 - Laboratories
 - Home and community care service providers
 - Indigenous health service providers and Aboriginal Health Access Centers
 - A center, program or service for community health or mental health whose primary purpose is the provision of health care
 - Supportive housing
 - Public health

Selective and secure sharing of a client's personal health information within the Circle of Care may include through shared electronic health systems such as the TREAT, OCEAN, the One Stop Talk/Parlons maintenance platform, and local, regional, and provincial programs.

For clarity, the following groups are NOT in the Circle of Care and Strides Toronto does not share Personal Health Information about Strides Toronto clients with them relying on implied consent. That does not mean the Organization never discloses to these individuals and groups however, Strides Toronto only does so if the client has provided express consent or is otherwise permitted or required by law to disclose:

- Children's Aid Societies
- Police
- Landlords
- Employers
- Spiritual leaders/healers
- Insurance companies
- Teachers and schools (however, psychologists, social workers, nurses, psychiatrists, speech-language pathologists, occupational therapists, physiotherapists, or audiologists affiliated with schools may be in the Circle of Care if they are providing health care).

Express Consent

Clients may also provide verbal or written consent if they wish Strides Toronto to release their information.

Strides Toronto notes that PHIPA does not apply to Aboriginal midwives or Aboriginal healers who are providing traditional services in Aboriginal communities². The provincial laws do not have authority over these providers. Strides Toronto considers these providers to be vital members of Strides Toronto's care community. When the Organization shares information with these providers, the Organization does so with the express permission of clients.

No Consent

There are certain activities for which consent is not required to collect, use, or disclose personal health information or personal information. These activities are permitted or required by law. For example, the Organization does not need consent from clients to (this is not an exhaustive list):

- Duty to Report
- Plan, administer and manage the Organization's internal operations, programs and services;

² This is the language included in section 3(4) of PHIPA.

Policy Title: Privacy and Confidential Personal Health Information**Policy Number: III, 1.5**

-
- Provide financial reporting;
 - Engage in quality improvement, error management, and risk management activities;
 - Participate in the analysis, administration and management of the health care system;
 - Engage in some research projects (subject to certain rules, such as obtaining research ethics board approval and having research contracts);
 - De-identify health information to provide to third parties;
 - Teach, train and educate Strides Toronto's employees, students and volunteers;
 - Compile statistics for internal or mandatory external reporting;
 - Respond to legal proceedings; and
 - Comply with mandatory reporting obligations.

A list of mandatory reporting obligations is found in Strides Toronto's document listed under Cross reference titled *Access and Corrections – Release of Client Information*.

If employees or others have questions about using and disclosing personal health information without consent, they can ask the Privacy Officer.

Withholding or Withdrawal of Consent

If consent is sought, a client may choose not to give consent ("withholding consent"). Where a client chooses to withhold consent, the Organization may not have sufficient information to provide services to the client. If there are any risks associated with withholding or withdrawing consent, these will be identified and shared with the client.

If consent is given, a client may withdraw consent at any time, and withdrawal of consent is immediate for future sharing of information. The withdrawal may also be subject to legal or contractual restrictions and reasonable notice.

Lockbox: Consent Directive

PHIPA and CYFSA give clients the opportunity to restrict access to any personal health information or personal information or their entire health record by their health care providers within Strides Toronto or by external health care or service providers. Although the term "lockbox" is not found in the privacy legislation, lockbox is commonly used to refer to a client's ability to withdraw or withhold consent for the use or disclosure of their Personal Health Information or personal information.

Principle 4: Limiting Collection of Personal Health Information or Client Personal Information

Strides Toronto limits the amount and type of personal health information that it collects to that which is necessary to fulfill the purposes identified above. Information is collected directly from the client, unless the law permits or requires collection from third parties. For example, from time to time the Organization may need to collect information from clients' family members, other service providers and others.

Personal health information and client personal information may only be collected within the limits of each employee's and other's role. Employees and others should not initiate their own projects to collect new personal health information or client personal information from any source without being authorized to do so by Strides Toronto.

Principle 5: Limiting Use and Disclosure of Personal Health Information and Client Personal Information Use

Personal health information and client personal information is not used for purposes other than those for which it was collected, except with the consent of the client or as permitted or required by law.

Personal health information and client personal information may be used only within the limits of each

Policy Title: Privacy and Confidential Personal Health Information**Policy Number:** III, 1.5

employee's and other's role. Employees and others may not read, look at, receive or otherwise use personal health information or client personal information unless they have a legitimate "need to know" as part of their position. If an employee or other is in doubt whether an activity to use personal health information or client personal information is part of their position, they shall ask the Privacy Officer. For example, it is not permitted to look at client records out of personal curiosity or to conduct a self-initiated education project without being assigned to those clients and without specific authorization for an approved educational exercise.

Disclosure

Personal health information and client personal information are not disclosed for purposes other than those for which it was collected, except with the consent of the client or as permitted or required by law.

Personal Health Information and client personal information may only be disclosed within the limits of each employee's or other's roles. Employees or others may not share, talk about, send or otherwise disclose client information to anyone else unless that activity is an authorized part of their position. If an employee or other is in doubt whether an activity to disclose client information is part of their position, they shall ask the Privacy Officer.

Principle 6: Accuracy of Personal Health Information

Strides Toronto will take reasonable steps to ensure that information it holds is as accurate, complete, and up to date as is necessary to minimize the possibility that inappropriate or wrong information may result in errors.

Principle 7: Safeguards for Client Information

Strides Toronto takes steps to ensure that the client information it holds is protected against theft, loss and unauthorized use or disclosure. Strides Toronto has put in place safeguards for the client information it holds, which include:

- Physical safeguards (such as confidential shredding bins, locked filing cabinets and rooms, clean desks, locked computer stations when workspace is not occupied);
- Keys/badges used for access to sensitive information shall not be left at an unattended desk;
- Organizational safeguards (such as permitting access to client information by staff on a "need-to-know" basis only);
- Technological safeguards (such as the use of passwords, encryption, audits, and secure disposal); and
- Printouts containing sensitive information shall be immediately removed from the printer; and whiteboards containing sensitive information shall be erased.

Strides Toronto requires anyone who collects, uses or discloses client information on its behalf to be aware of the importance of maintaining confidentiality of client information. This is done through the signing of confidentiality agreements, privacy training, and contractual means.

Care is used in the disposal or destruction of client information, to prevent unauthorized parties from gaining access to the information. Strides Toronto ensures appropriate care is taken if it transfers files to a health records storage company. For more detailed information refer to *Acceptable Use of Information Technology Resources policy* and the *Cyber Risk and Security policy* noted under Cross References.

Principle 8: Openness about Client Information

Information about Strides Toronto policies and practices relating to the management of client information is

Policy Title: Privacy and Confidential Personal Health Information**Policy Number:** III, 1.5

available to the public and clients, including:

- Contact information for Strides Toronto's Privacy Officer, to whom complaints or inquiries can be made;
- The process for obtaining access to client information Strides Toronto holds, and making requests for its correction;
- A description of the type of client information Strides Toronto holds, including a general account of the Organization's uses and disclosures; and
- A description of how a client may make a complaint to Strides Toronto's Privacy Officer or to the Information and Privacy Commissioner of Ontario.

Principle 9: Client Access to Client Information

Clients may make written requests to have access to their records of personal health information.

Strides Toronto will respond to a client's request for access within 30 days (subject to a time extension of up to an additional 30 days if necessary and with notice to the person making the request). The Organization will take reasonable steps to ensure that the requested information is made available in a format that is understandable.

Clients have a right to ask for their records to be corrected if they can demonstrate that the records Strides Toronto holds are inaccurate or incomplete in some way for the purposes for which the Organization holds that information.

Please Note: In certain situations, Strides Toronto may not be able to provide access to all the information Strides Toronto holds about a client. Exceptions to the right of access requirement will be in accordance with law. Examples may include information that could reasonably be expected to result in a risk of serious harm, or the information is subject to legal privilege.

Principle 10: Challenging Compliance with Strides Toronto's Privacy and Confidentiality Policies and Practices

The Privacy Officer will be responsible for receiving and responding to complaints or inquiries about Strides Toronto's policies and practices relating to the handling of client information. Any person may ask questions or challenge the Organization's compliance with this policy or with PHIPA or CYFSA by contacting Strides Toronto's Privacy Officer:

Contact information: privacy@stridestoronto.ca

Strides Toronto investigates all complaints. If a complaint is found to be justified, Strides Toronto will take appropriate measures to respond.

The Information and Privacy Commissioner of Ontario oversees the Organization's compliance with privacy rules and PHIPA and CYFSA. Any individual can make an inquiry or complaint directly to the Information and Privacy Commissioner of Ontario by writing to or calling:

2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8 Canada
Phone: 1 (800) 387-0073 (or 416-326-3333 in Toronto)
www.ipc.on.ca

Breach of Privacy Policy, Procedures, or Guidelines

Failure by an employee or other to adhere to this policy and its related procedures and guidelines may result in corrective action being taken. Such corrective action may include but is not limited to retraining; loss of

Policy Title: Privacy and Confidential Personal Health Information**Policy Number: III, 1.5**

access to systems; suspension; reporting conduct to the Information and Privacy Commissioner of Ontario or a professional regulatory body or sponsoring agency, school or institution; termination of contract, and/or immediate dismissal. Additional consequences include notification of affected persons, fines, prosecutions, or lawsuits. Refer to the *Incidents and Serious Occurrences Reporting policy* to more detail.

Procedures**Principle 1: Accountability for Personal Health Information (PHI)**

1. All staff, students, consultants and volunteers having access to confidential information will complete and acknowledge the *Oath of Confidentiality and Privacy of Information*, at the time of joining the Organization. Client information is only discussed with those who need to know, based on their involvement in the services being provided to the client. Client personal information can only be shared through the formal channels of communication of the Organization (e.g., case conferences). E-mail correspondence will only include non-identifying client information (e.g., initials, first name only, first name and last initial).
2. All staff, students, consultants and volunteers will be informed of the policies regarding the privacy of client information and confidentiality by the appropriate supervisor before access to clients and records is permitted. This information will be included in the orientation and training program of the Organization.
3. All staff, students, consultants and volunteers will protect client privacy and confidentiality by ensuring that any material with personal information is locked when not being used, whether in the office, in the community or when working remotely.
4. At the time of closing the office at the end of each day, any materials left in printers or unclaimed faxes that contain client personal information will be placed in the mailbox of the staff. Those that are not identifiable will be shredded.

Principle 2: Purpose for Collecting PHI

5. Staff and students are responsible for ensuring that their access to a client record is limited to only those clients where they are providing direct service or related administrative service. The Director or designate will approve access to client files for others who are not providing direct service on a "need-to-know" basis. Official representatives of government funders have the authority to examine records pertaining to their programs. Accreditation site reviewers may access client files during their review of the Organization.
6. Access to records may be granted for teaching purposes. Identities will be disguised in any client records used for external training. The requirements for the protection of client personal information are part of the authorization process as determined by the Organization, in accordance with relevant legislation.
7. Access to records for research purposes will follow policies and procedures noted in the Research policy.

Principle 3: Consent for Collection and Use of a Lockbox

8. The following is the process for releasing health records to a third-party health care or service provider or organization relying on a client's express consent:
 - Record the date of the request in the client record
 - Advise the Program Manager/Supervisor, Senior Manager or Director of the request
9. If release of information to the third-party organization is authorized by a Manager/Supervisor,

Policy Title: Privacy and Confidential Personal Health Information

Policy Number: III, 1.5

Senior Manager or Service Director:

- Select and photocopy/print specific information requested
- Do not photocopy/print the entire client record unless required
- Prepare an official cover letter that will accompany the released information
- Courier or arrange for pick up by the client requesting the information
- Scan the letter of request, client's consent, and a copy of the covering letter and save in the client's record

10. If the request is incomplete, unclear or contains invalid consent or is otherwise not authorized by the Manager/Supervisor, Senior Manager or Director:
 - Inform the client who made the request of the problem in writing (or in person or by phone as appropriate), such as:
 - The request is not sufficient to identify the client
 - The request is unclear or unspecific
 - The request does not have the required consent.
11. Document the date, time of the call, name of the person with whom contact was made, a brief summary of the conversation and comments made by the requester.

Implied Consent -- Circle of Care

12. Strides may also release information to a client's other health care providers and organizations for health care purposes (within the "circle of care") without the express written consent of the client if it is reasonable in the circumstances to believe that the client wants the information shared with other health care providers and organizations. However, no information will be released to other health care providers and organizations if a client has stated they do not want the information shared.
13. The following is the process for releasing health records to a third-party health care provider relying on a client's implied consent:
 - Record the date of the request in the health record
 - Advise the Program Manager/Supervisor, Senior Manager or Director of the request
 - If release of information to the third-party health care provider is authorized by Manager/Supervisor, Senior Manager or Director:
 - Select and photocopy or print specific information requested
 - Do not photocopy/print the entire health record unless required
 - Prepare an official cover letter that will accompany the released information
 - Courier or arrange for pick up by the client requesting the information.
 - Record the verbal request for information
 - If the request is incomplete, unclear or Strides has been advised by the client not to disclose relying on implied consent, or the request is otherwise not authorized by the Manager/Supervisor, Senior Manager or Director:
 - Inform the person who made the request of the problem in writing (or in person or by phone, as appropriate), such as:
 - The request is not sufficient to identify the client
 - The request is unclear or unspecific
 - The request does not have the required consent
 - Document the date, time of the call, name of the person with whom contact was made, a brief summary of the conversation and comments made by the requester.

Policy Title: Privacy and Confidential Personal Health Information

Policy Number: III, 1.5

Third Party Requests for Release of Information (to Non-Health Care Providers)

14. Should a client wish their lawyer, insurance company, employer, landlord or other such persons or agencies to have access to the client record, the client must provide a written statement of consent to this effect, which will be written to Strides Toronto and then directed to the relevant Director, Senior Manager, or Manager/Supervisor. Strides will not process verbal third-party requests for release of information to anyone who is not a health care provider. These requests must be in writing. No information will be released without the express consent from the client or the authorized person (unless permitted or required by law). See below "Permitted or Mandatory Release of Information". Third-party requests not accompanied by appropriate consent will be returned with an official letter, outlining proper and complete consent requirements.
15. Any third-party request for release of information shall include:
 - The name, address and telephone number of person/agency requesting the information
 - The full name, address and date of birth of the person about whom the information relates
 - A specific description of the type and amount of information to be released
 - A consent for release of information form signed by the client (or client's authorized person)
16. The following is the process for releasing client records to a third party with the consent of the individual client:
 - Record the date of the request in the health record
 - Advise the Program Manager, Senior Manager or Director of the request
 - If release of information to the third party is authorized by a Manager, Senior Manager or Director:
 - Select and photocopy/print specific information requested
 - Do not photocopy/print the entire client record unless required
 - Prepare an official cover letter that will accompany the released information
 - Send out/mail-out requested information
 - Scan the letter of request, consent, and a copy of the covering letter and save in the client's record
 - If the request is incomplete, unclear or contains an invalid consent or is otherwise not authorized by a Manager, Senior Manager or Director:
 - Inform requester of the problem in writing (or in person or by phone as appropriate), such as:
 - The request is not sufficient to identify the client
 - The request is unclear or unspecific
 - The request does not have the required consent
 - If the date the client's consent was signed is not recent; while legally still accurate, you may ask why it has taken a length of time for it to be provided.
 - Document the date, time of the call, name of the person with whom contact was made, a brief summary of the conversation and comments made by the requester.

Permitted or Mandatory Release of Information

17. Strides may release personal health information or other personal information to a third party if "permitted or required by law". A list of mandatory disclosures is included at the end of this document.
18. Any time a mandatory disclosure is considered, the Program Manager/Supervisor, Senior Manager or Director will be informed PRIOR to releasing the information. Consultation with the organization's Privacy Officer and/or Legal advice may be sought.

Policy Title: Privacy and Confidential Personal Health Information

Policy Number: III, 1.5

Police/OPP/RCMP

19. The fact that a client is suspected of being a victim of a crime or suspected of having committed a crime is not a recognized reason for breaching the client's right to confidentiality. However, there is a recognized exception ("discretion to warn") to client confidentiality where there is a significant risk of serious bodily harm to someone (either the client or someone else) **and if it is genuinely believed that disclosing information to police could eliminate or reduce that risk.**
20. Otherwise, personal information will only be released to police upon the presentation of one of the following documents:
 - A consent for release of information form signed by the client or authorized person
 - A valid court order (or other legal document) requiring the release of information to the police
 - A coroner's writ requiring the release of information to the police
21. Each document must be reviewed carefully before information may be disclosed to the police (to ensure the disclosure is **permitted or required** by law). This review should be done by appropriate staff, such as the Privacy Officer or Director, before any information is released. The documentation from the client, police, court or coroner will be scanned into the client record. Legal advice should be sought as necessary.

Children's Aid Societies (CAS)

22. Everyone has a mandatory duty to report a "child in need of protection" to the CAS under the *Child, Youth and Family Services Act, 2017*. Information may be sent to the CAS to explain the reason for the report.
23. Any documentation from CAS claiming authority to release information to the CAS must be reviewed carefully before information may be disclosed (see the section of the legislation giving the legal authority that the release of information is **permitted or required** by law). This review should be done by the Privacy Officer before any information is released. The documentation from CAS will be scanned into the client record. Strides will seek legal advice as appropriate.
24. When clients ask to restrict, limit, exclude, shield, block their information from others, they may want a lockbox, and their worker help the client complete a Client Lockbox Request form and receive a Client Lockbox Information Brochure.
25. The Privacy Officer or delegate will review the request, consider if there are any reasons to deny the request and respond to the client. The client will be informed if the request is denied and may make a complaint to the Privacy Commissioner of Ontario.
26. The process of creating a lockbox is managed by the Manager, Information Technology.
27. Lockboxes can be broken to access the information. Consultation should take place with their supervisor.

Regulatory Colleges

28. Under the Regulated Health Professions Act, 1991 and other health profession specific legislation, regulatory colleges may have the authority to review client records as part of investigations or quality assurance practices. Any documentation from a regulatory college claiming legal authority to release information to the college must be reviewed carefully before information may be disclosed (for the section of the legislation giving the legal authority that the release of information is permitted or

Policy Title: Privacy and Confidential Personal Health Information**Policy Number: III, 1.5**

required by law). This review should be done by the affected clinician and/or the Privacy Officer before any information is released. The documentation from the regulatory college will be scanned into the client record.

Other Authorities

29. Certain legislation gives government agencies and others authority to review client records (such as immigration, the Ministry of Health, workplace safety and insurance and others). Any documentation from an agency claiming legal authority to release information to the agency must be reviewed carefully before information may be disclosed (review the legislation giving the legal authority that the release of information is permitted or required by law). This review should be done by the Privacy Officer before any information is released. The documentation from the agency will be scanned into the client record.

Lawyers

30. Most lawyers' letters require client consent for the release of information to a lawyer. Staff should not release information to a lawyer without client consent unless they have some other documentation to state that Strides Toronto is required by law to disclose the information. Any documentation from a lawyer claiming legal authority to release information to the lawyer must be reviewed carefully before information may be disclosed (in most cases the lawyer is asking for the record, not advising Strides Toronto that it is required by law to release the record). This review should be done by the Privacy Officer before any information is released. The documentation from the lawyer will be scanned into the client record.

Principle 4: Limiting Collection of PHI

31. Client information is only gathered to inform service delivery based on the Recording Standards and Expectations *policy* and discussed with those that need to know.

Principle 5: Limiting Use and Disclosure of PHI

32. Provide clients with the information sheet on the Collection, Use and Disclosure of Information found in the Client Welcome Package.

Principle 6: Accuracy of PHI

33. Program Assistants will review each file at closing to check demographic accuracy.

Principle 7: Safeguards to Protect Client Information

34. Refer to the Acceptable Use of Information Technology policy for more specifics on features in place to protect client information.

Principle 8: Openness About Client Information

35. Provide clients with a copy of the Client Complaint Information process found in the Client Welcome Package and review this information sheet at the start of service.

Principle 9: Client Access to Client Information

36. By law, Strides Toronto is required to give clients' access to their records of personal health information or personal information or seek an extension up to 30 days with notice to the client.

37. Corrections are made in the following ways:

- Striking out the incorrect information in a manner that does not obliterate the record or

Policy Title: Privacy and Confidential Personal Health Information

Policy Number: III, 1.5

38. If striking out is not possible:

- Labelling the information as incorrect, severing it from the record, and storing it separately with a link to the record that enables Strides to trace the incorrect information, or
- Ensuring there is a practical system to inform anyone who sees the record or receives a copy that the information is incorrect and directing that person to the correct information.

39. The record will not be corrected if:

- The record was not originally created by a Team Member, and Strides does not have the knowledge, expertise or authority to correct the record, or
- The record consists of a professional opinion which was made in good faith.

40. Where Strides chooses not to correct a record, the client must be informed in writing. The client will have the choice to submit a statement of disagreement. If the client submits such a statement, it will be scanned onto the client's record and released any time the information that was asked to be corrected is released.

41. Where Strides chooses not to correct a record, clients have a right to complain to the Information and Privacy Commissioner of Ontario.

Principle 10: Privacy Breaches

42. All privacy complaints, incidents and actual or potential breaches must be reported immediately to the Privacy officer using the Privacy Breach form. If the breach was a "near miss" then the Privacy Officer is also informed.

43. The Privacy Officer responds immediately by following privacy breach protocol:

- Containment: Identify the scope of the potential breach and take steps to contain it
- Clarify the facts
- Notify those individuals whose privacy has been breached and notify them of the breach
- Investigate and Remediate
- Document and keep a record of all complaints, incidents and breaches including investigations, notifications, and remedial action taken.

The Privacy Officer will refer to the "*Privacy Breaches*" document noted under Cross References for more specific information.

Cross References

Policy I, 1.4 Research

Policy I, 2.6 Feedback and Formal Complaints

Policy I, 2.8 Incident and Serious Occurrence Reporting

Policy I, 2.9 Record Retention

Policy III, 2.1 Consent to Service

Policy III, 2.2 Recording Standards and Expectations

Policy VI, 1.2 Cyber Risk and Security

Policy VI, 1.1 Acceptable Use of Information Technology Resources

Oath of Confidentiality

Client Lockbox Information Brochure

Lockbox Request form

Privacy Breaches

Policy Title: Privacy and Confidential Personal Health Information

Policy Number: III, 1.5

Appendices

N/A