SERVICE COORDINATION SUPPORT (SCS) FOR PEOPLE WITH DEVELOPMENTAL DISABILITIES			
Chapter: 7	**SERVICE DELIVERY**	**Number:**	**7.5.02**
Section: 5	**CONFIDENTIALITY AND RECORDS**	**Issue Date:**	**2012-11-14**
Subject: 02	**PRIVACY AND CONFIDENTIALITY**	**Effective Date:**	**2012-12-04**
Authorized:		**Revised Date:**	**2026-05-30**
		Replaces:	**7.5.02**
POLICY AND PROCEDURE			

Please note that this document is available in both official languages on the SCS website.

1. DEFINITIONS

1.1. Personal Information: Any identifying information about a person including but not limited to name, address, contact information, date of birth, identification numbers, and family or social circumstances.

1.2. Personal Health Information (PHI): Information related to an individual's physical or mental health, developmental status, diagnosis, functional abilities, care needs, supports, or services received.

1.3. Client \ Participant: An individual who seeks or receives services from SCS.

1.4. Informed (Knowledgeable) Consent: The individual must understand the purpose of the collection use or disclosure and that they can give or withhold consent. Consent must specifically relate to the personal health information being collected, used, or disclosed. Consent provided by client or their legally authorized substitute decisionmaker for the collection, use, or disclosure of their personal or Personal Health information. Consent must be given **freely**, without coercion or misrepresentation. Verbal consent will be accepted to engage but consent forms must be completed before any support is provided.

1.5. DSCIS (Developmental Services Consolidated Information System)**:** A province wide database accessible to staff members working at Developmental Service Ontario (DSO). This database is secured using Microsoft Account integration. The Ontario Ministry of Children, Community and Social Services (MCCSS) can access all information in DSCIS. Other Transfer Payment Agencies will have access to a web portal linked to DSCIS for the purpose of matching and linking, urgent response, Passport transfer of files and prioritization functions.

1.6. ETO (Efforts to Outcomes): A Bonterra database accessible to staff members working at SCS and DSO Ontario Eastern Region. This database is secured and only accessible using Microsoft Account integration.

1.7. Records: A collection of related information treated as a unit, about a person who has received or is currently receiving services. This includes case notes, emails and memos where the individual is named, referenced or cited.

1.8. Privacy Breach: A privacy breach occurs when personal information is collected, retained, used or disclosed in ways that are not in accordance with the provisions of the *Acts*, for example, the disclosure of personal information without authority.

2. POLICY AND PURPOSE

SCS follows all legislated requirements protecting the rights and privacy of the people we support, including those set out in the *Child, Youth and Family Services Act* and the *Services and Supports to Promote the Social Inclusion of Persons with Developmental Disabilities Act, 2008*. Although SCS is not a Health Information Custodian (HIC) under PHIPA, the organization recognizes the sensitivity of the information it collects and voluntarily applies PHIPA-aligned standards to ensure a high level of privacy protection.

The purpose of this policy is to set out how SCS collects, uses, shares, stores, and protects personal and confidential information relating to the people we support. SCS is committed to ensuring that all such information is handled in a confidential, secure, and respectful manner that recognizes individuals' rights to privacy and choice.

This policy applies to employees, board members, students, volunteers, contractors, and partner organizations who may have access to this information in the course of their work or relationship with SCS.

Information is only shared with other organizations or individuals with appropriate consent and in accordance with this policy and applicable legislation.

This policy applies to:
- Personal and confidential information about people supported by SCS
- Related information about family members, caregivers, or others acting on their behalf, where collected for service delivery or support purposes

This policy does **not** apply to:
- Job applicants and employee candidates
- Employees in their employment capacity
- Board recruitment processes
- Donors, website users, or members of the general public
- Other individuals, except where they are also receiving services from SCS

SCS gathers and has access to personal and confidential information about the people it serves, their families, and those representing their interests. SCS respects the right to privacy and confidentiality and recognizes that individuals have the right to choose with whom they share their personal information.

SCS is committed to:
- Protecting personal information from theft, loss, unauthorized access, use, disclosure, or copying
- Ensuring information is collected, used, and shared only as necessary for service delivery and support
- Maintaining secure storage and handling practices for all records and files

All privacy and security breaches must be documented and reported promptly to the SCS Privacy Officer.

All employees are required to sign an employment agreement that includes confidentiality obligations and a Code of Confidentiality confirming that they have read, understood, and will comply with privacy expectations.

All individuals covered by this policy must:
- Maintain the confidentiality of client information at all times
- Use and access information only as required for their role
- Ensure that any sharing of information is done with proper consent and in accordance with this

policy
Breaches of this policy may result in disciplinary action, up to and including dismissal.

In addition, all information related to SCS operations—including internal and external matters, agency business, and documentation—is to be treated as confidential and remains the property of SCS.

All breaches of privacy or confidentiality, including suspected breaches, must be:
- Documented
- Reported immediately to the SCS Privacy Officer
- Addressed in accordance with SCS procedures

3. PROCEDURE

SCS's privacy and disclosure practices are guided by the 10 Principles of the Canadian Standard's Association's Model Code for the Protection of Personal Information. The Personal Health Information Protection Act (PHIPA) is based on this code, as listed below:

3.1. Accountability

We are responsible for ensuring that client files are kept for each person applying for services and for the quality and security of these files. Discussions of confidential information in any public places are strictly prohibited. This applies to all employees of SCS or any other party who has access to this information. This includes any exchange of information by any electronic devices or communication systems. SCS has an assigned Privacy Officer, who provides guidance regarding privacy of information, and completes certain functions during a breach or a complaint. The responsibility for confidentiality lies with each person at SCS and flows up the reporting structure.

3.2. What we Collect

The organization may collect the following types of information including but not limited to; Identifying and contact information, eligibility and intake information, developmental, functional, and support needs information, case notes and service records, information required by funders or oversight bodies, emergency contact and substitute decision maker information.

3.3. Purpose and Information Collection

Personal and Personal Health Information is collected for these reasons but not limited to;
Confirm eligibility for services, plan, coordinate, and evaluate services and supports, maintain accurate case records, meet contractual, funding, reporting, and legal obligations, support client safety and continuity of care. SCS will document thereason for collecting information. The identity of the person being served and other persons will be protected. Case material for prioritization, research or teaching purposes will be prepared (blinded/redacted) so that all persons involved cannot be identified.

3.4. Informed (Knowledgeable) Consent

SCS and DSOER obtain informed, voluntary, and documented consent for the collection, use, and disclosure of personal information, except where permitted or required by law.
Consent forms (SCS/DSOER Consent Forms) must be signed by the person receiving services or their legal designate before any information is collected or any information contained in the file is released. The signature must also be witnessed. It is essential that every effort be made to assist the individual in knowing and understanding what information is being released, why it is being collected, how it will be used, to whom it will be released, and what purpose is to be achieved by releasing the information.

Where a client lacks capacity, consent is obtained from a legally authorized substitute decision-maker. Clients may withdraw or limit consent at any time, subject to legal or contractual restrictions.
Recording audio and video must not be made without the consent of the person being served. People must also be informed that there are risks associated to providing consent with electronic communication/emails. The person must be informed that electronic information sharing can be intercepted, sent to the wrong recipient and is at risk in public domain (i.e. Google, Yahoo etc...) before providing consent to using email communication.

It is acceptable practice to send an e-consent to the individual or their parent/guardian by email in an attachment, ask them to type their name on the electronic form (and have them check the consent box) and have them resend it **through their email** in an attachment. This is considered a signed written consent.

If an individual or a parent/guardian is having issues typing their name on the electronic form, or saving it on their device so that they can send it back in an attachment, it is an acceptable practice for them to provide their written consent in the body of the email **if it comes from their email address**. As we are directed to save consent forms in supplemental documents in ETO, staff should save a copy of the email (with the written consent in the body of the email) in the Supplemental forms' touchpoint in ETO. If files get audited, this is where we will verify that there is a consent on file, and not in case notes.

3.5. Use and Disclose Information

Information about the person receiving services may only be shared with persons within SCS or external persons who have the right to see this information and to whom consent has been granted.

Client information is used only by authorized personnel and only for purposes directly related to service delivery, administration, quality improvement, or legal compliance.

Information may be disclosed in the following circumstances: with the consent of the client or substitute decision-maker; to service partners, funders, or regulatory bodies, where required; to prevent a serious risk of harm, as permitted by law; or where disclosure is legally required (e.g., by court order or mandatory reporting).

SCS does **not sell or trade client information**.

3.6. Duty to Warn

As per PHIPA, disclosures related to risks are permitted if there are reasonable grounds to believe that the disclosure is necessary to eliminate or reduce a significant risk of serious bodily harm to a person or a group of persons.
SCS may consider disclosure without consent if there is a potential risk that could harm a third-party service provider or others.

SCS balances the need to maintain confidentiality with the need to provide agencies with sufficient information to assess their ability to provide high quality services that promote safety and security for all. This is reflected in the SCS Consent to Collect, Use and Disclose Information, which is signed by all people served at SCS.

Using the Duty to Warn Risk Assessment Form, SCS will determine the need to disclose information and will only do so where there is a genuine safety risk. Such risks include situations where;

- **An individual has behaviours posing a threat-** this refers to a known threat or risk, which is not

reflected in an individual's DSOER package, behavioural intervention plan or other documents or where an individual has specifically restricted SCS from sharing information about these risks with service agencies.

- **An individual has a criminal record such as;**
  - Adults with a criminal record- anything that contains information about a personal criminal history. Includes all convictions for which a pardon has not been granted, all charges regardless of disposition, outstanding warrants, charges, all judicial orders and other information that might be of interest to police investigations
  - Youth with a criminal record- In all cases involving a person with a sealed Youth Criminal Justice Record, information about the person served will not be disclosed without consent, except where;
    - The youth was convicted of murder, or;
    - The person committed an offence after they turned 18, but while the access period for a previous youth offence remained open.

Based on the responses of the Duty to Warn Risk Assessment Form, SCS should then have a factual basis to make an informed decision about whether there is a duty to disclose a particular risk to a direct service agency. Employees will ensure disclosures are only made where there is a genuine safety risk to the public, service providers or vulnerable persons by reviewing the risk criteria.

The documentation supporting this decision must be noted on file and authorized by a director.

In all cases, disclosure will be made only if there is an actual risk of serious harm that could arise from the failure to disclose certain information. The information disclosed will be restricted to the minimum amount of information required to help minimize the risk.

3.7. Limiting Collection

The amount and type of information collected is limited to what is necessary for the identified purposes. Examples of information include but are not limited to demographic information, case notes, service information, consent forms, eligibility documentation, Application for Developmental Services and Supports (ADSS), Support Intensity Scale Assessment (SIS).

3.8. Retention of Client Information

Information provided to SCS or a designate (family/guardian) will only be kept for the duration it is needed.

Client records are retained in accordance with legislative, contractual, and best-practice retention requirements.
When no longer required, records are securely destroyed to prevent unauthorized access or reconstruction.

3.9. Accuracy

Information will be kept as accurate, complete and up to date as new information is provided and as necessary for the purpose for which it was collected.

3.10. Using appropriate safeguards

SCS will protect personal information with the appropriate physical, administrative, and technical safeguards put in place.

Administrative Safeguards Include but are not limited to; privacy training for all staff and volunteers, confidentiality agreements, role-based access controls, clear breach reporting procedures

Physical Safeguards Include but not limited to; restricted access areas, secure shredding of paper records.

Technical Safeguards Include but not limited to; 2 Factor Password protected systems, Encryption where available, Regular system updates and access review

3.7.1 No information is to be left in any place where it could be accessed by persons who do not have a legitimate right to this information.
3.7.2 Information being reviewed during daily operations is to be maintained confidential at all times.
3.7.3 All employees will lock computers when moving away from their workstation to protect the privacy and security of electronic files.
3.7.4 All employees follow the Safety and Security Policy and will adhere to rules related to the identification and monitoring of visitors within the SCS office in order to protect the privacy of personal information.
3.7.5 All staff will adhere to SCS Policies and procedures regarding security

3.11. Transparency

Privacy practices are openly communicated to clients.

3.12. Granting Individual Access

Clients have the right to access the personal information contained in their record, and to have this information corrected or amended. The following information is provided by the Information and Privacy Commissioner (IPC):

If an individual believes that his or her personal health information is not accurate or complete, the individual has the right to make a request to have it corrected. The correction request should be made in writing, directly to SCS, via the Personal Records – Request for Access, Correction or Complaint Form.

3.12.1. If a correction request is denied by SCS, SCS must explain why the request was refused. Individuals have the right to attach a statement to their record of personal health information conveying disagreement. Please note that SCS must correct an incomplete or inaccurate record but is not required to change professional opinions or correct records that were not created by SCS.

3.12.2. Individuals have the right to file a complaint to the IPC if his or her correction request to SCS is denied, by completing the Access/Correction Complaint Form.

It is also their right to change or remove their consent.
To do so, they must contact their SCS assigned Staff or the Privacy Officer at SCS and make a formal request via the Personal Records- Request for Access, Correction or Complaint Form.

SCS permits the reasonable right of access and review of personal information collected about a client and will endeavour to provide the information in question within a reasonable time frame, generally no later than 30 days following the request. Where information will not or cannot be disclosed within the 30 days or at all, the individual making the request will be provided with the reasons for non-disclosure.

SCS cannot charge clients who request verification or corrections to their personal information (not

including case notes); however, there will be a minimal charge imposed if copies of records are requested. SCS must provide an estimate for any anticipated charge of $25 or more. To accommodate individuals, SCS is prepared to waive the first $100 of fees.

The following fees represent a breakdown of the costs that will be charged to accommodate the request and will be used to calculate charges.

Action	Fees
Change in Personal Information	No fee required
Photocopies and computer printouts	$0.20 per page
USB KEY	$25 each
Manually searching for a record	$30 per hour ($7.50 for each 15 minute spent by any person
Preparing a record for disclosure, including severir part of the record	$30 per hour ($7.50 for each 15 minute spent by any person
Miscellaneous costs incurred to locate, retrieve, process, and copy record(s) as specified in an invoice received by SCS	actual costs

Note:
Every record requested must be reviewed and will incur a preparation charge.
Every effort will be made to provide a fee estimate when the fees for processing your request are expected to exceed $25.
Fees may be charged for goods and services for which SCS must pay in order to respond to your information request.
SCS may require the requester to pay 50% of the total estimated fee in advance if it is anticipated to exceed $100. The remainder of the fee must be paid upon receipt of the material.
SCS will refund any deposit paid if the request for information is withdrawn.
SCS will endeavor to keep fees reasonable.

4. Privacy and\or Confidentiality Breach

Breaches occur when personal health information is collected, retained, used or disclosed in ways that are not in accordance with the provisions of the Act and/ or when unauthorized disclosure of PHI occurs, such as; PHI that may be lost (a file is misplaced within the organization), stolen or lost computer, laptop or work cell phone, information inadvertently disclosed through human error (a letter addressed to person A is actually mailed to person B).

5. All breaches in security will be immediately reported to the SCS Privacy Officer.

Breaches are logged in a breach log and reported to a director. As per the Privacy Breach Protocol Guidelines, plans to manage breaches should include the following;

Containment

If an employee is notified of a breach or breaches of an individual's information or is the cause of the privacy breach(es) they will report the breach to the SCS privacy officer immediately and follow up with details in writing and copy their supervisor and Director.

The SCS Privacy officer will meet with the employee and their Direct Report/Director to assist with collecting the details of the breach in order to mitigate risks to the person(s) involved and ensure privacy is not further compromised. This includes:

- determining where or how the breach occurred and
- securing the information to prevent further breaches,
- *retrieving the hard copies of any PHI that has been disclosed;*
- ensuring that no copies of the PHI have been made or retained by the individual who was not authorized to receive the information and obtain the individual's contact information in the event that follow-up is required; and
- determine whether the privacy breach would allow unauthorized access to any other PHI (e.g., an electronic information system) and take whatever necessary steps are appropriate (e.g., change passwords, identification numbers and/or temporarily shut down a system).

Notification - a plan will be developed to:

- Identify those individuals whose privacy were breached
- Within 3 business days, notify the individuals whose privacy was breached
- Provide details of the extent of the breach and the specifics of the PHI at issue;
- If financial information or information from government-issued documents are involved, include a detailed notice
- Advise of the steps that have been taken to address the breach, both immediate and long-term;
- Provide contact information for someone within your organization who can provide additional information, assistance and answer questions (i.e. Privacy Officer and/or Director); and
- Advise that the IPC will be contacted to ensure that all obligations under the Act are fulfilled and, where appropriate, provide information about how to complain to the IPC
- Complete a Serious Occurrence form for any breach for which the IPC has been notified

Investigation – Within one week of the breach, the Privacy Officer will;

- Meet with the staff responsible for breach with supervisor/director to evaluate the breach and determine a plan to address the breach if applicable and make recommendations to prevent further breaches.
- Inform the Executive Director of the plan.
- Inform the IPC registrar when appropriate[2] and will work in collaboration with the IPC and the staff to resolve and prevent further breaches. The determination of risk will be determined within the risk management framework.
- Conduct an internal investigation
- Document all recommendations
- Review adequacy of existing policies and procedures and make recommendations
- Cooperate in any further investigation into the incident undertaken by IPC.

Remediation – the Privacy Officer will:

- Within each 90-day period, follow up with the families engaged in the breach to provide an update on containment.
- Ensure that the immediate requirements of containment and notification have been met.
- Review the circumstances surrounding the breach.
- Review the adequacy of SCS existing policies and procedures in protecting personal health information.
- Ensure all staff are appropriately educated and trained with respect to compliance with the privacy

protection provisions of PHIPA.[3]

- Notify the families when the file is considered closed.

[2] https://www.ipc.on.ca/wp-content/uploads/Resources/hprivbreach-e.pdf - The IPC does not define the "appropriate" time to advise of a breach, but we suggest we advise the IPC when breaches impact multiple families or are intentional. See last two paragraphs of page 1.
[3] https://www.ipc.on.ca/health/breach-reporting-2/privacy-breach-protocol/

6. Challenging Compliance

All people have a right to file a complaint against SCS if they feel that the organization has failed to comply with one or more of the privacy protection provisions of the *Acts*, or that his or her privacy has been compromised. If you have any questions regarding SCS's privacy policies, access to your records, correction of information, or if you believe any of your privacy rights have been violated in any way, you may contact our Privacy Officer:

Privacy Officer
Service Coordination Support for People with Developmental Disabilities
1400 St Laurent Rd., Suite 507
Ottawa, ON K1K 4H4
Phone: 613-748-1788 ext. 245
Fax: 613-748-1018
Privacy@scsonline.ca

You may also make requests for file complaints via Personal Records - Request for Access, Correction or Complaint Form. The Privacy Officer will investigate all complaints and take all reasonable steps to resolve the issue, generally no later than 30 days following the request. If SCS's Privacy Officer has not resolved your concerns to your satisfaction, you have a right to file a complaint with the Information and Privacy Commissioner/ Ontario (IPC). As well, upon learning of a possible privacy breach, the IPC may itself initiate a complaint in the absence of an individual complainant. The Information and Privacy Commissioner (IPC) may be reached at:

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Phone: 416-326-3333 or 1-800-387-0073
Online: https://www.ipc.on.ca/

7. ATTACHMENTS / APPENDIX

8. REFERENCES AND RELATED POLICY AND PROCEDURE

8.1 Quality Assurance Measures, Regulation 299/10.
8.2 Personal Health Information Protection Act.
8.3 Children, Youth and Family Services Act
8.4 Personal Records - Request for Access, Correction or Complaint Form

9. REVISION DATES

DOCUMENT REVISION HISTORY		
Date	**Author**	**Revision**
September 24, 2020	N Tardif	Added sections 3.3.4 to 3.3.6 regarding electronic consents.
January 24, 2022	N Tardif	Revision of language re: HIC
May 30, 2026	A Staltari	Revision of definitions, purpose and guiding principles