SERVICE COORDINATION SUPPORT (SCS)			
Chapter: 7.	**SERVICE DELIVERY**	**Number:**	**7.5.03**
Section: 5.	**CONFIDENTIALITY AND RECORDS**	**Issue Date:**	**2012-11-14**
Subject: .03	**PRIVACY AND CONFIDENTIALITY**	**Effective Date:**	**2012-12-04**
Authorized:		**Revised Date:**	2018-12-07
		Replaces:	7.5.02
POLICY AND PROCEDURE			

Please note that sections of this document will appear in both official languages on SCS website.

1. DEFINITIONS

1.1. Personal Information: Any identifying information about a person including their name, address, date of birth, phone number, email address, gender, nationality, financial status and funding, health status.

1.2. DSCIS (Developmental Services Consolidated Information System)**:** A province wide database accessible to staff members working at Developmental Service Ontario. This database is secured and only accessible after inputting a password and a randomly selected identifier code on the system's corresponding person specific key fob. 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.

1.3. ETO (Efforts to Outcomes): A database accessible to staff members working at SCS and Developmental Service Ontario Eastern Region. This database is secured and only accessible after inputting a password.

1.4. 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.

1.5. Privacy Breach: 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 guidelines protecting the rights of all individuals, as outlined in the *Child and Family Services Act* and the *Services and Supports to Promote the Social Inclusion of Persons with Developmental Disabilities Act, 2008*. As well, SCS complies with the *Personal Health Information Protection Act (PHIPA*) and the *Personal Information and Electronic Documents Act (PIPEDA).*

The purpose of this policy is to protect and ensure that all personal information is handled in a confidential and private manner by all employees, board members, and other organizations who have working relationships with SCS. Information shared with other organizations is done so with consent and within the terms and understanding of this privacy and confidentiality policy.

SCS will ensure that all information gathered remains private and confidential. SCS gathers and has access to information of a personal and confidential nature about the people they serve, their families and those representing their interests. SCS respects the right to privacy and confidentiality and recognizes that people choose whom they would like to share their personal information with. SCS protects all individual files from theft, loss, unauthorized access, disclosure, copying and/or use. All breaches in security will be documented and reported to the SCS Privacy Officer (see section 3.11).

All SCS employees are required to sign an employment agreement, which includes a "Code of Confidentiality" indicating that they have read and understood confidentiality expectations. Employees also acknowledge that disciplinary action leading up to, and including, dismissal will result from any violation of this policy and its procedures. In like manner all information related to SCS business, the agency and its employees or information related to internal or external matters is to be treated as, and is to remain, confidential at all times. All documentation is solely the property of SCS.

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. Both the Personal Health Information Protection Act (PHIPA) and the Personal Information and Electronic Documents Act (PIPEDA) are based on this code, as listed below:

3.1. Accountability

SCS has an assigned Privacy Officer who is accountable for all privacy related matters. Case Managers, Resource Coordinators and Assessor/ Navigators are responsible for ensuring that individual 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 (i.e.: computers, facsimiles, telephones etc.)

3.2. Purpose and Information Collection

Personal information is gathered for specific purposes and SCS will document the reason 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.

3.3. Obtaining Consent to Collect, Use and Disclose Information

3.3.1. Consent forms (SCS/DSOER Consent Forms) must be signed by the person receiving services or their legal designate before 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 released, and what purpose is to be achieved by releasing the information.

3.3.2. Audio and audio visual records must not be made without the written 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.

3.3.3. **Duty to warn;** As per PHIPPA, 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.

3.3.3.1. As a custodian of health information, SCS may consider disclosure without consent if there as a potential risk that could harm a third party service provider or others.

3.3.3.2 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.

3.3.3.3 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 and 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.

3.3.3.4 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.

3.3.3.5 The documentation supporting this decision must be noted on file and authorized by a Director

3.3.3.6 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.

3.3.3.7 The decision to release such information rests with the Executive Director.

3.4. Limiting Collection

The amount and type of information collected is limited to what is necessary for the identified purposes. All SCS and DSOER employees must include in the person's record, at a minimum, consent forms, a copy of the person's eligibility documentation, Application for Developmental Services and Supports (ADSS) and their Support Intensity Scale (SIS) assessment (if applicable). DSOER staff must ensure that the Application Package is collected, stored and maintained accurately and consistently and meets the quality standards required by the MCCSS as set out by the Assessor Training and Data Quality Assurance program.

3.5. Limiting use, disclosure and retention of personal information

Information provided to SCS or a designate (family/guardian) will only be kept for the duration it is needed. When an individual file is closed and the person over 18 years of age is no longer receiving active services, and the first contact occurred over the age of 18, files will be securely kept for a period of 7 years. See Appendix A – Privacy and Confidentiality Policy and Procedure

3.5.1. Adult files will be kept for 7 years where the individual is deceased and last contact occurred over the age of 18 years.

3.5.2. Children who are under the age of 18 and are no longer receiving active case management services will have their files kept for a period of 20 years.

3.5.3. After 7 years and before the destruction of the file, the following documents must be scanned and uploaded to the client relationship management database;

3.5.4. Access to files will be given to representatives from the MCCSS who are conducting an official review, audit or study, and who have been identified as such by the Executive Director.

3.6. Accuracy

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

3.7. Using appropriate safeguards

SCS will protect personal information with the appropriate security measures, physical safeguards and electronic precautions.

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 at all times and all files are to be kept in locked filing cabinets when employees leave the workplace.
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 files, materials or software containing personal information is to remain at the office, however, when information is required for use outside of the office, it will be stored in a safe and secure way that ensures privacy and protects the information from theft, loss or damages.

This includes logging off the ETO database when work is completed or moving away from the workstation. When sending personal information via email (with informed consent obtained) all private information or documents must be encrypted (password protected).

3.8 Disclosure

The people served and their families or designated parties protecting their interests must be aware that records are kept and that they can access their files. They may also request full disclosure of their record at any time.

3.9 Granting Individual Access

Individuals 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):

3.9.1 If an individual believes that his or her personal health information is not accurate or complete, Ontario's health privacy legislation, the Personal Health Information Protection Act (PHIPA), gives the individual the right to make a request to have it corrected. The correction request should be made in writing, directly to SCS. "This Request to Correct Personal Health Information Form can be used for this purpose."[1]
3.9.2 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.

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

[1] https://www.ipc.on.ca/resource/request-to-correct-personal-health-information-phipa/

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

3.9.4 SCS permits the reasonable right of access and review of personal information collected about an individual, whether staff or 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.

3.9.5 SCS cannot charge individuals 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 minutes) spent by any person
Preparing a record for disclosure, including severing part of the record	$30 per hour ($7.50 for each 15 minutes) 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.

3.9.6 All fees are in line with information provided by the Ontario Information and Privacy Commissioner. For more information, see https://www.ipc.on.ca/access/

To guard against fraudulent requests for access, SCS may require additional information to confirm that the person making the request is authorized to do so before granting access or making corrections.

SCS reserves the right to decline to provide access to personal information where the information requested:

3.9.6.1 Would disclose (i) personal information, including opinions, about another individual or about a deceased individual; or (ii) business confidential information that may harm SCS or the competitive position of a third party;
3.9.6.2 Would interfere with contractual or other negotiations of SCS or a third party;
3.9.6.3 Is subject to solicitor-client, litigation or other legal privilege;
3.9.6.4 Is not readily retrievable and the burden or cost of providing would be disproportionate to the nature or value of the information;
3.9.6.5 Does not exist, is not held, or cannot be found by SCS;
3.9.6.6 Could reasonably result in (i) serious harm to the treatment or recovery of the individual concerned, (ii) serious emotional harm to the individual concerned or another individual, or (iii) serious bodily harm to another individual;
3.9.6.7 May harm or interfere with law enforcement activities and other investigative or regulatory functions of a body authorized by law to perform such functions; or
3.9.6.8 May be withheld or is requested to be withheld under applicable legislation.

3.10 Reporting a Privacy and Confidentiality Breach

Breaches occur when personal 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 personal information occurs, such as;

- Personal information 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).

3.11 All breaches in security will be immediately reported to the SCS Privacy Officer. Breaches are logged in breach log, and reported to the Executive Director on a scheduled basis. As per the Privacy Breach Protocol Guidelines, plans to manage breaches should include the following;

3.11.1 Containment

3.11.1.1 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.

3.11.1.2 Any risks related to the breach will be immediately reported to the Executive Director to ensure Risk Mitigation strategies are in place through the Operations team.

- 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 personal information that has been disclosed;*
- ensuring that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information and obtain the individual's contact information in the event that follow-up is required; and
- determine whether the privacy breach would allow unauthorized access to any other personal information (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).

3.11.2 Notification - a plan will be developed to:

3.11.2.1 Identify those individuals whose privacy were breached and, barring exceptional circumstances, notify those individuals accordingly

3.11.2.2 Within 3 business days, notify the individuals whose privacy was breached, by telephone and then in writing;

3.11.2.3 Provide details of the extent of the breach and the specifics of the personal information at issue;

3.11.2.4 If financial information or information from government-issued documents are involved, include a detailed notice

3.11.2.5 Advise of the steps that have been taken to address the breach, both immediate and long-term;

3.11.2.6 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

3.11.2.7 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

3.11.2.8 Complete a Serious Occurrence form for any breach for which the IPC has been notified

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

3.12.1 Meet with the staff responsible for breach/supervisor/Director to evaluate the breach and determine a plan to address the breach if applicable and make recommendations to prevent further breaches.

3.12.2 Inform the Executive Director of the plan.

3.12.3 Inform the IPC registrar when appropriate[2] and will work in collaboration with the IPC staff to resolve and prevent further breaches. The determination of risk will be determined within the risk management framework.

3.12.4 Conduct an internal investigation

3.12.5 Document all recommendations

[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.

3.12.6 Review adequacy of existing policies and procedures and make recommendations
3.12.7 Cooperate in any further investigation into the incident undertaken by IPC.

3.13 Remediation – the Privacy Officer will:

3.13.1 Within each 90-day period, follow up with the families engaged in the breach to provide an update on containment.
3.13.2 Ensure that the immediate requirements of containment and notification have been met.
3.13.3 Review the circumstances surrounding the breach.
3.13.4 Review the adequacy of your existing policies and procedures in protecting personal health information.
3.13.5 Ensure all staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of PHIPA.[3]
3.13.6 Notify the families when the file is considered closed.

3.14 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 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 (SCS)
507-1400 St Laurent Blvd.
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 the 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 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/

[3] https://www.ipc.on.ca/health/breach-reporting-2/privacy-breach-protocol/

4.0 ATTACHMENTS / APPENDIX

Appendix 1- Plain Language Privacy and Confidentiality Statement
Plain Language Privacy and Confidentiality Statement

Any information about you is nobody else's business. The only way we can share information about you is if you say "YES" we can tell somebody else.

There are some people who have access to your information who help you pay for the services you get in your home, school, day program or job. These people do not tell anybody else about you. They keep your information private.

If any of the people who are paid to help you tell someone information about you that is private, they can lose their job.

5. REFERENCES AND RELATED POLICY AND PROCEDURE

5.1 Orientation and Mandatory Training
5.2 Quality Assurance Measures, Regulation 299/10.
5.3 Personal Health Information Protection Act.
5.4 Children, Youth and Family Services Act
5.5 Request for Access/Correction or Complaint From
5.6 Safety and Security Policy
5.7 SCS Consent to Collect and Disclose (pink)
5.8 SCS Consent for Release (yellow)
5.9 Orientation and Mandatory Training