

SERVICE COORDINATION SOUTIEN (SCS) POUR LES PERSONNES AYANT UNE DÉFICIENCE INTELLECTUELLE			
Chapitre : 7.	PRESTATION DE SERVICES	Numéro	7.5.03
Section : 5.	CONFIDENTIALITÉ ET DOSSIERS	Date d'émission	2012-11-14
Sujet : .03	VIE PRIVÉE ET CONFIDENTIALITÉ	Date d'entrée en vigueur	2012-12-04
Autorisation :		Date de révision	2022-01-24
		Remplace	7.5.02
POLITIQUE ET PROCÉDURE			

Le nom de notre agence juridique est *Coordination des Services pour les personnes ayant des déficiences intellectuelles*. Toutefois, aux fins de nos politiques et procédures, nous utilisons notre nom commercial *Service Coordination Soutien pour les personnes ayant une déficience intellectuelle (SCS)*.

Veillez noter que ce document seront affichées dans les deux langues officielles sur le site Web de SCS.

1. DÉFINITIONS

- 1.1. **Renseignements personnels** : Renseignements permettant d'identifier une personne, notamment son nom, son adresse, sa date de naissance, son numéro de téléphone, son adresse courriel, son genre, sa nationalité, sa situation financière et son état de santé.
- 1.2. **Système DSCIS** (Système d'information centralisé sur les services aux personnes ayant une déficience intellectuelle) : Une base de données à l'échelle de la province, accessible aux membres du personnel travaillant à Services de l'Ontario pour les personnes ayant une déficience intellectuelle. Cette base de données est sécurisée et est uniquement accessible après avoir entré un mot de passe et un code identificateur sélectionné au hasard dans le dispositif de déverrouillage du système propre à une personne. Le ministère des Services à l'enfance et des Services sociaux et communautaires de l'Ontario peut accéder à tous les renseignements dans le DSCIS. Les autres organismes bénéficiant de paiements de transfert devront utiliser un portail Web relié au DSCIS pour les fonctions de jumelage et liaison, intervention d'urgence, transfert de dossiers de Passeport et établissement de priorité.
- 1.3. **Base de données ETO (efforts à l'atteinte des objectifs)** : Une base de données accessible aux membres du personnel de SCS pour les personnes ayant une déficience intellectuelle et des Services de l'Ontario pour les personnes ayant une déficience intellectuelle de la région de l'Est (SPODIRE). Cette base de données est sécurisée et consultable seulement après avoir entré un mot de passe.
- 1.4. **Dossiers** : Un ensemble de renseignements connexes traités comme un tout, à propos d'une personne qui a reçu ou qui reçoit à l'heure actuelle des services. Cela comprend des notes de cas, des courriels et des notes de service où le nom de la personne est inscrit, cité ou mentionné en référence.

Atteinte à la vie privée : Il y a atteinte à la vie privée lorsque des renseignements personnels sont recueillis, conservés, utilisés ou divulgués de façon contraire aux dispositions des *Lois*, par exemple, la divulgation de renseignements personnels sans autorisation.

2. POLITIQUE ET BUT

SCS pour les personnes ayant une déficience intellectuelle (SCS) respecte toutes les lignes directrices établies par la loi sur la protection des droits de toutes les personnes, comme

Indiqué dans la *Loi sur les services à l'enfance, à la jeunesse et à la famille* et la *Loi de 2008 sur les services et soutiens favorisant l'inclusion sociale des personnes ayant une déficience intellectuelle*. SCS respecte également la *Loi sur la protection des renseignements personnels sur la santé* et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), même si SCS n'est pas un dépositaire de renseignements sur la santé, conformément à l'article 3 de la LPRPS.

Le but de la présente politique est de protéger tous les renseignements personnels et de veiller à ce qu'ils soient traités de manière confidentielle et privée par tous les employés, membres du conseil d'administration et les autres organismes qui ont des relations de travail avec SCS. Les renseignements sont partagés avec d'autres organismes avec consentement et selon les conditions et l'interprétation de la présente politique sur la protection de la vie privée et la confidentialité.

SCS veillera à ce que tous les renseignements recueillis demeurent privés et confidentiels. SCS recueille des renseignements de nature personnelle et confidentielle à propos des personnes auxquelles elle offre des services, de leur famille et de ceux qui représentent leurs intérêts, et a accès à ces renseignements. SCS respecte le droit à la vie privée et à la confidentialité et reconnaît que les personnes choisissent les personnes avec lesquelles elles veulent partager leurs renseignements personnels. SCS protège tous les dossiers des clients contre le vol, la perte, l'accès non autorisé, la divulgation, la copie et/ou l'utilisation. Toutes les atteintes à la sécurité seront documentées et signalées à l'agent du service de protection de la vie privée de SCS (voir la section 3.10).

Tous les employés de SCS doivent signer un « code de confidentialité » indiquant qu'ils ont lu et compris cette politique et qu'ils acceptent de la respecter. Les employés reconnaissent également que toute violation de la présente politique et de ses procédures entraînera des mesures disciplinaires pouvant même aller jusqu'au congédiement. De façon similaire, tous les renseignements liés aux affaires de SCS, de l'organisme et de ses employés ou les renseignements liés aux affaires internes ou externes doivent être traités de manière confidentielle et demeurer confidentiels en tout temps. Tous les documents sont entièrement la propriété de SCS.

3. PROCÉDURE

Les pratiques en matière de protection et de divulgation des renseignements personnels de SCS sont orientées par les 10 principes du Code type sur la protection des renseignements personnels de l'Association canadienne de normalisation. Tant la *Loi sur la protection des renseignements personnels sur la santé* que la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) sont fondées sur ce code, comme indiqué ci-dessous :

3.1. Responsabilité

Les gestionnaires de cas, les coordonnateurs de ressources et les évaluateurs/navigateurs (et tous les autres membres du personnel qui travaillent avec les renseignements sur les clients) sont responsables de veiller à conserver un dossier pour chaque personne qui présente une demande de services et à assurer la qualité et la sécurité de ces dossiers. Il est strictement interdit de discuter de renseignements personnels dans des endroits publics. Cette directive s'applique à tous les employés de SCS ou à toute autre partie qui a accès à ces renseignements. Cela inclut l'échange de renseignements au moyen de n'importe quel appareil électronique ou système de communication (p. ex. ordinateur, télécopieur, téléphone, etc.) SCS dispose d'un agent de la protection de la vie privée qui fournit des conseils sur la confidentialité des informations et remplit certaines fonctions lors d'une atteinte à la vie privée ou d'une plainte. La responsabilité sur la confidentialité incombe à chaque personne de SCS et remonte dans la structure hiérarchique.

3.2. Fins de la collecte des renseignements

Les renseignements personnels sont recueillis à des fins particulières et SCS documentera la raison de la collecte des renseignements. L'identité des personnes qui reçoivent les services et des autres personnes sera protégée. Des dossiers de cas pour établir les priorités, à des fins de recherche ou d'enseignement, seront préparés (masqués/caviardés) de manière à ce que toutes les personnes concernées ne puissent être identifiées.

3.3. Obtenir un consentement à la collecte, à l'utilisation et à la divulgation de renseignements

- 3.3.1. La personne qui reçoit des services ou son mandataire légal doit signer des formulaires d'autorisation (formulaires de consentement de SCS/des Services de l'Ontario pour les personnes ayant une déficience intellectuelle de la région de l'Est [SOPDIRE]) avant de divulguer des renseignements contenus au dossier. Un témoin doit également assister à la signature. Il est essentiel de déployer tous les efforts pour aider la personne à connaître et à comprendre les renseignements qui sont divulgués, pour quelles raisons et quel est le but de la divulgation des renseignements.
- 3.3.2. Il est interdit de produire des documents audio et audiovisuels sans le consentement écrit de la personne qui reçoit les services. Les gens doivent également être informés du fait qu'il existe des risques à consentir à la communication électronique/par courriel. La personne doit être informée du fait que l'information électronique peut être interceptée, envoyée au mauvais destinataire et être à risque dans le domaine public (c.-à-d. Google, Yahoo, etc.) avant qu'elle donne son consentement à la communication par courriel.
- 3.3.3. Les renseignements à propos de la personne qui reçoit des services ne peuvent être partagés qu'avec les personnes au sein de SCS ou les personnes externes ayant droit de consulter ces renseignements et auxquelles le consentement a été accordé.
- 3.3.4. Le consentement électronique est disponible sur Billboard < Forms – Applications < Consents modified for e-version folder.
- 3.3.5. Il est acceptable d'envoyer un consentement électronique à l'individu ou à son parent/tuteur par courriel dans une pièce jointe, leur demander de taper leur nom sur le formulaire électronique (et leur demander de cocher la case de consentement) et leur demander de le renvoyer **par courriel** dans une pièce jointe. Ceci est considéré comme étant un consentement écrit.
- 3.3.6. Si une personne ou un parent/tuteur éprouve des difficultés à taper leur nom sur le consentement électronique ou à l'enregistrer sur leur appareil afin de pouvoir le renvoyer dans une pièce jointe, il est acceptable pour eux de fournir leur consentement écrit dans le corps du courriel **s'il provient de leur adresse courriel**. Comme nous devons télécharger les formulaires de consentement dans notre base de données, le personnel doit enregistrer une copie du courriel (avec le consentement écrit dans le corps du courriel) dans « Supplemental forms » dans notre base de données. S'il y a une vérification de la conformité sur des dossiers, c'est dans « Supplemental forms » que nous vérifierons s'il y a un consentement écrit au dossier, et non dans les notes de cas (case notes).
- 3.3.7. **Obligation d'avertir** : Conformément à la *Loi sur la protection des renseignements personnels sur la santé*, les divulgations liées aux risques sont autorisées s'il existe des motifs raisonnables de croire que la divulgation est nécessaire pour éliminer ou réduire un risque important de lésions corporelles graves pour une personne ou un groupe de personnes.
-

3.3.3.1. En tant que dépositaire des informations sur la santé, SCS peut envisager la divulgation sans consentement s'il existe un risque potentiel qui pourrait nuire à un fournisseur de services ou autres.

3.3.3.2 SCS fait l'équilibre entre la nécessité de maintenir la confidentialité et la nécessité de fournir aux agences des informations suffisantes pour évaluer leur capacité à fournir des services de haute qualité qui favorisent la sécurité de tous. Ceci est reflété dans le consentement de SCS nous permettant de recueillir, utiliser et divulguer des informations, qui est alors signé par tous les individus recevant des services de SCS.

3.3.3.3 À l'aide du formulaire d'évaluation des risques sur l'obligation d'avertir, SCS déterminera la nécessité de divulguer des informations et ne le fera qu'en cas de risque réel pour la sécurité. Ces risques comprennent les situations où :

- **Un individu a des comportements posant une menace** – ceci fait référence à une menace ou un risque connu, qui n'est pas reflété dans les évaluations de SOPDIRE, dans le plan d'intervention en comportements ou dans d'autres documents d'un individu, ou lorsqu'un individu a spécifiquement interdit à SCS de partager des informations sur ces risques avec des agences qui fournissent des services.
- **Un individu a un casier judiciaire tel que :**
 - Adultes ayant un casier judiciaire – tout ce qui contient des informations sur des antécédents criminels personnels. Ceci comprend toutes les condamnations pour lesquelles un pardon n'a pas été accordé, toutes les accusations, peu importe la décision, les mandats et les accusations en suspens, toutes les ordonnances judiciaires et autres informations susceptibles de déclencher une enquête policière.
 - Jeune avec un casier judiciaire – Dans tous les cas impliquant un jeune avec un casier judiciaire scellé, les renseignements sur la personne ne peuvent être divulgués sans son consentement, sauf pour les cas suivants :
 - Le jeune a été reconnu coupable de meurtre, ou;
 - La personne a commis une infraction après avoir atteint l'âge de 18 ans, mais que la période d'accès pour une infraction juvénile antérieure était encore en vigueur.

3.3.3.4 En fonction des réponses au formulaire d'évaluation de l'obligation d'avertir, SCS devrait avoir une base factuelle pour prendre une décision éclairée quant à l'obligation de divulguer un risque particulier à un organisme de services directs. Les employés veilleront à ce que les divulgations ne soient faites que lorsqu'il existe un risque réel pour la sécurité du public, des fournisseurs de services ou des personnes vulnérables en examinant les critères de risque.

3.3.3.5 Les documents à l'appui de cette décision doivent être versés au dossier et autorisés par un directeur.

3.3.3.6 Dans tous les cas, la divulgation ne sera faite que s'il y a un risque réel de préjudice grave qui pourrait découler du défaut de divulguer certains renseignements. Les renseignements divulgués seront limités à la quantité minimale de renseignements nécessaires pour aider à réduire le risque.

3.3.3.7 La décision de communiquer ces renseignements revient au directeur général.

3.4. Limitation de la collecte

La quantité et la nature des renseignements se limitent à ceux qui sont nécessaires aux fins

déterminées. Tous les employés de SCS et des SOPDIRE doivent inclure dans le dossier d'une personne, à tout le moins, un formulaire de consentement, un exemplaire de la demande de services et de soutiens pour les personnes ayant une déficience intellectuelle de la personne et de son évaluation de l'échelle d'intensité de soutien (ÉIS) (le cas échéant). Le personnel des SOPDIRE doit s'assurer que les données de la trousse de demande de services sont réunies, entreposées et tenues à jour de façon rigoureuse et uniforme, et satisfont aux normes du programme de formation des évaluateurs et d'assurance de la qualité du MESSC.

3.5. Limitation de l'utilisation, de la communication et de la conservation des renseignements personnels

Les renseignements fournis à SCS ou à une partie désignée (famille/tuteur) seront conservés uniquement pendant la durée au cours de laquelle ils sont nécessaires. Lorsqu'on ferme le dossier d'une personne de plus de 18 ans qui ne reçoit plus de services actifs de gestion des cas et que le premier contact a eu lieu lorsque cette personne avait plus de 18 ans, les dossiers seront conservés, sécurisés, pendant une période de sept ans. Voir Appendix A – Privacy and Confidentiality Policy and Procedure

- 3.5.1. Les dossiers des adultes seront conservés pendant sept ans lorsque le client est décédé et que le dernier contact a eu lieu lorsqu'il avait plus de 18 ans.
- 3.5.2. Les dossiers des enfants de moins de 18 ans qui ne reçoivent plus de services actifs de gestion des cas seront conservés pendant une période de 20 ans.
- 3.5.3. Après sept ans et avant la destruction du dossier, les documents suivants doivent être numérisés par balayage et téléchargés à la base de données sur la gestion des relations avec les clients;
 - 3.5.3.1 L'admissibilité après 2016 est entrée directement dans la base de données sur la gestion des relations avec les clients;
 - 3.5.3.2 L'évaluation psychologique;
 - 3.5.3.3 Tous les échanges de courriers avec le ministère des Services à l'enfance et des Services sociaux et communautaires et tous les signalements d'incidents graves.
- 3.5.4. L'accès aux dossiers sera accordé à des représentants du ministère des Services à l'enfance et des Services sociaux et communautaires qui réalisent un examen, une étude ou un audit officiel et ont été identifiés comme tels par le directeur général.

3.6. Exactitude

Les renseignements personnels seront aussi exacts, complets et à jour à mesure de que de nouveaux renseignements sont recueillis et que l'exigent les fins pour lesquelles ils ont été recueillis.

3.7. Utilisation des mesures de sécurité appropriées

SCS protégera les renseignements personnels en utilisant des mesures de sécurité appropriées, des mesures de protection matérielles et électroniques.

- 3.7.1 Il ne faut pas laisser des renseignements dans des endroits accessibles à des personnes qui n'ont pas un droit légitime d'obtenir ces renseignements.
 - 3.7.2 En tout temps, il faut assurer la confidentialité des renseignements écrits examinés pendant les activités quotidiennes et conserver tous les dossiers dans des classeurs verrouillés lorsque les employés quittent le travail.
 - 3.7.3 Tous les employés verrouilleront leur ordinateur lorsqu'ils s'éloignent de leur poste de travail afin de protéger la vie privée et la sécurité des dossiers électroniques.
-

- 3.7.4 Tous les employés suivront la politique sur la sécurité et respecteront les règles liées à l'identification et à la surveillance des visiteurs au sein du bureau de SCS afin de protéger les renseignements personnels.
- 3.7.5 En règle générale, tous les dossiers, documents et logiciels contenant des renseignements personnels doivent demeurer au bureau. Cependant, lorsque des renseignements doivent être utilisés en dehors du bureau, ils sont conservés de manière sécuritaire de façon à assurer la vie privée et à protéger les renseignements contre le vol, la perte ou les dommages.

Cela inclut la fermeture de la session de la base de données sur les efforts à l'atteinte des objectifs lorsque le travail est achevé ou lorsqu'on est éloigné du poste de travail. Au moment d'envoyer des renseignements personnels par courriel (avec le consentement éclairé), tous les renseignements privés ou les documents doivent être chiffrés (protégés par mot de passe).

3.8 Divulgation

Les personnes qui reçoivent des services et leur famille ou les parties désignées pour protéger leurs intérêts doivent savoir que des dossiers sont conservés et qu'elles peuvent y avoir accès. Elles peuvent également demander la divulgation de tous les renseignements contenus dans leur dossier en tout temps.

3.9 Permettre l'accès aux renseignements personnels

Les personnes ont le droit d'avoir accès aux renseignements personnels contenus dans leur dossier et de faire corriger ou modifier ces renseignements. Les renseignements suivants sont fournis par le commissaire à l'information et à la protection de la vie privée (CIPVP) :

- 3.9.1 Si une personne croit que ses renseignements personnels sur la santé ne sont pas exacts ou complets, la loi de l'Ontario sur la protection des renseignements personnels sur la santé, soit la *Loi sur la protection des renseignements personnels sur la santé*, donne à la personne le droit de présenter une demande pour les faire corriger. La demande de rectification doit se faire par écrit, directement à SCS, au moyen du Dossier personnel – Formulaire de demande d'accès, de correction ou de plainte de renseignements personnels.
- 3.9.2 Si une demande de rectification est rejetée par SCS, l'organisme doit expliquer les raisons du refus. Les personnes ont le droit de joindre à leur dossier de renseignements personnels sur la santé une déclaration faisant part du désaccord. Veuillez noter que SCS doit rectifier des renseignements incomplets ou inexacts, mais l'organisme n'est pas tenu de changer des avis d'experts ou corriger des renseignements contenus dans des dossiers qui n'ont pas été créés par SCS.
- 3.9.3 Les personnes ont le droit de déposer une plainte auprès du CIPVP si leur demande de rectification adressée à SCS est rejetée, en remplissant le Formulaire de demande d'accès, de correction ou de plainte de renseignements personnels.

Elles ont également le droit de changer ou de retirer leur consentement. Pour ce faire, elles doivent communiquer avec l'agent de la protection de la vie privée de SCS et présenter une demande officielle en remplissant le [Formulaire de demande d'accès, de correction ou de plainte de renseignements personnels](#).
- 3.9.4 SCS accorde le droit raisonnable à l'accès et à l'examen des renseignements personnels recueillis sur une personne, que ce soit un employé ou un client, et s'efforcera de fournir l'information en question dans des délais raisonnables, généralement au plus tard 30 jours après la demande. Lorsque des renseignements ne peuvent ou ne doivent pas être divulgués dans les 30 jours ou pas du tout, les raisons de la non-divulgation seront données à la personne faisant la demande.
- 3.9.5 SCS ne réclamera pas aux personnes des frais pour vérifier ou pour corriger leurs renseignements personnels (à l'exclusion des notes de cas)); toutefois, il peut y avoir des frais minimes si les personnes demandent des copies des dossiers. SCS doit fournir une estimation du montant de tous frais prévus de 25 \$ ou plus. Pour répondre aux besoins des

clients, SCS est prêt à renoncer aux premiers 100 \$ de frais. Le tableau suivant représente une ventilation des frais qui seront réclamés pour répondre aux demandes, et sera utilisé pour calculer les frais.

¹ <https://www.ipc.on.ca/resource/request-to-correct-personal-health-information-phia/>

Acte	Frais
Modification aux renseignements personnels	Aucuns frais
Photocopies et imprimés d'ordinateur	0,20 \$ la page
Clé USB	25 \$ chacune
Recherche manuelle d'un dossier	30 \$ l'heure (7,50 \$ pour chaque 15 minutes) qu'une personne y consacre
Préparer un dossier en vue de la divulgation, incluant la séparation de pièces du dossier	30 \$ l'heure (7,50 \$ pour chaque 15 minutes) qu'une personne y consacre
Frais divers encourus pour localiser, récupérer, traiter et copier des dossiers indiqués dans une facture reçue par SCS	Frais réels

Remarques:

- Chaque dossier demandé doit être examiné et entraînera des frais de préparation.
- Tous les efforts seront déployés pour présenter une estimation lorsque les frais liés au traitement du dossier demandé devraient dépasser 25 \$.
- Des frais peuvent être réclamés pour des biens et services pour lesquels SCS doit payer afin de répondre à votre demande de renseignements.
- SCS peut exiger du demandeur de payer d'avance 50 % du montant estimé des frais s'il est prévu que ce montant dépasse 100 \$. Le reste doit être payé après la réception du ou des documents.
- SCS remboursera tout acompte versé si la demande de renseignements est retirée.
- SCS s'efforcera de réclamer des frais raisonnables.

3.9.6 Tous les frais sont conformes aux renseignements fournis par le CIPVP/Ontario. Pour obtenir de plus amples renseignements, consultez le site <https://www.ipc.on.ca/access/>

En vue de bloquer les demandes d'accès frauduleuses et avant d'accorder l'accès ou d'apporter les corrections, SCS peut demander des renseignements supplémentaires pour confirmer que la personne faisant la demande est autorisée à le faire.

SCS se réserve le droit de refuser l'accès à des renseignements personnels dans les cas suivants :

- 3.9.6.1 Les renseignements révéleraient (i) des renseignements personnels, y compris des opinions, sur une autre personne ou un défunt; (ii) des secrets commerciaux ou d'autres renseignements commerciaux confidentiels pouvant nuire à SCS ou à la position concurrentielle d'une tierce partie;
- 3.9.6.2 Les renseignements pourraient interférer avec des négociations contractuelles ou autres de SCS ou d'une tierce partie;
- 3.9.6.3 Les renseignements sont assujettis au secret professionnel de l'avocat, au privilège relatif au litige ou à un autre aspect juridique;

- 3.9.6.4 Les renseignements ne sont pas facilement accessibles et le fardeau de travail ou le coût pour les offrir serait disproportionné par rapport à la nature ou à la valeur des renseignements;
- 3.9.6.5 Les renseignements n'ont jamais existé, n'ont pas été conservés ou ne peuvent pas être trouvés par SCS;
- 3.9.6.6 Les renseignements pourraient à juste titre être la cause (i) d'une nuisance importante au traitement ou au rétablissement de la personne en cause; (ii) d'un problème émotionnel pour la personne visée ou pour une autre; (iii) d'un préjudice corporel grave pour une autre personne;
- 3.9.6.7 Les renseignements risqueraient de nuire ou d'interférer lors d'activités axées sur l'application de la loi ou sur d'autres fonctions liées à une enquête ou à une réglementation d'un organisme autorisé par la loi à assumer de telles fonctions; ou
- 3.9.6.8 Les renseignements peuvent être retenus ou il y a une demande de les retenir en vertu d'une loi applicable.

3.10 **Signalement d'une atteinte à la vie privée et à la confidentialité**

Il y a atteinte à la vie privée lorsque des renseignements personnels sont recueillis, conservés, utilisés ou divulgués de façon contraire aux dispositions des Lois et/ou en cas de divulgation non autorisée des renseignements personnels, par exemple;

- Des renseignements personnels peuvent être perdus (lorsqu'un dossier est égaré au sein de l'organisation);
- Un ordinateur, un portable ou un téléphone cellulaire de travail volé ou perdu;
- Des renseignements sont divulgués par inadvertance à la suite d'une erreur humaine (une lettre adressée à la personne A est envoyée en fait à la personne B).

3.11 **Toutes les atteintes à la sécurité seront immédiatement signalées à l'agent du service de protection de la vie privée de SCS.** Les atteintes sont inscrites au registre des atteintes et signalées au directeur général à intervalles réguliers. Conformément au Protocole en cas de violation de la vie privée, les plans pour gérer les infractions devraient inclure ce qui suit :

3.11.1 **Maîtrise de la situation**

- Si un employé est informé d'une atteinte ou d'atteintes aux renseignements d'un client ou est la cause de l'atteinte à la vie privée, il doit immédiatement signaler l'atteinte à l'agent du service de protection de la vie privée de SCS et envoyer les détails par écrit en transmettant une copie à son superviseur et à son directeur.
- Tout risque lié à l'atteinte sera immédiatement signalé au directeur général pour veiller à la mise en place de stratégies d'atténuation des risques.
- L'agent du service de protection de la vie privée de SCS rencontrera l'employé et son superviseur/directeur afin de recueillir les détails de l'atteinte dans le but d'atténuer les risques à la personne concernée et veiller à ce que la confidentialité ne soit pas compromise davantage. Cela inclut ce qui suit :
 - Déterminer l'endroit et la cause de l'atteinte;
 - Sécuriser les renseignements afin de prévenir d'autres atteintes;
 - *Récupérer les copies papier des renseignements personnels qui ont été divulgués;*
 - S'assurer que le particulier qui n'était pas autorisé à recevoir les renseignements n'en a conservé aucune copie, et obtenir ses coordonnées au cas où il serait nécessaire de communiquer à nouveau avec lui;
 - Déterminer si l'atteinte à la vie privée pouvait entraîner un accès non autorisé à d'autres renseignements personnels (p. ex., système d'information électronique) et prendre les mesures nécessaires (p. ex.,

remplacer les mots de passe ou les numéros d'identification, ou mettre le système hors service temporairement).

3.11.2 Notification – un plan sera élaboré afin de :

- Déterminer les personnes concernées par l'atteinte à la vie privée et les informer de la situation, sauf dans des circonstances exceptionnelles;
- Dans un délai de trois jours ouvrables, informer les personnes concernées par téléphone ou par écrit;
- Indiquer la portée de l'atteinte à la vie privée et décrire les renseignements personnels en cause;
- Si des renseignements financiers ou des renseignements provenant de documents délivrés par le gouvernement sont en cause, inclure un message détaillé;
- Informer les personnes concernées des mesures qui ont été ou seront prises pour rectifier la situation, tant dans l'immédiat qu'à long terme;
- Fournir les coordonnées d'une personne de l'organisation qui pourra fournir des renseignements et de l'aide supplémentaires et répondre aux questions (agent du service de protection de la vie privée et/ou directeur);
- Préciser que l'organisation fera appel au CIPVP pour s'assurer que toutes les obligations sont remplies en vertu de la Loi et, le cas échéant, fournir des renseignements sur la manière de déposer plainte auprès du CIPVP;
- Remplir un rapport d'incident grave concernant toute atteinte à la vie privée pour laquelle le CIPVP a été informé.

3.12 Enquête – Dans un délai d'une semaine après l'atteinte à la vie privée, l'agent du service de protection de la vie privée :

- Rencontrera le personnel responsable de l'atteinte/le superviseur/le directeur afin d'évaluer l'atteinte et de déterminer un plan pour la régler, s'il y a lieu, et formuler des recommandations pour empêcher d'autres atteintes;
- Informera le directeur général du plan;
- Informera le registraire du CIPVP au moment opportun² et collaborera avec le personnel du CIPVP pour résoudre l'atteinte et empêcher les atteintes futures. La détermination du risque se fera selon le cadre de gestion des risques;
- Mènera une enquête interne;
- Documentera toutes les recommandations;
- Examinera la suffisance des politiques et procédures existantes et formulera des recommandations;
- Collaborera dans le cadre de toute enquête que le CIPVP pourrait mener sur l'incident.

3.13 Mesures correctives – L'agent du service de protection de la vie privée :

- Dans chaque période de 90 jours, assurera le suivi avec les familles concernées par l'atteinte pour faire le point sur la maîtrise de la situation.
- Veillera à ce que les exigences immédiates liées à la maîtrise de la situation et à la notification soient satisfaites.
- Examinera les circonstances entourant l'atteinte à la vie privée.
- Examinera la suffisance des politiques et procédures existantes pour protéger les renseignements personnels sur la santé.
- Veillera à ce que tout le personnel soit sensibilisé et formé concernant la conformité aux dispositions sur la protection de la vie privée de la *Loi sur la protection des renseignements personnels sur la santé*.³
- Avisera les familles lorsque le dossier est considéré comme clos.

² <https://www.ipc.on.ca/wp-content/uploads/Resources/hprivbreach-f.pdf> – le CIPVP ne définit pas le moment

« opportun » d'informer au sujet de l'atteinte à la vie privée, mais nous suggérons d'informer le CIPVP lorsque plusieurs familles sont touchées ou lorsque l'atteinte est délibérée. Voir les deux derniers paragraphes de la page 1

³<https://www.cipvp.ca/>

3.14 Contester la conformité

Toutes les personnes ont le droit de déposer une plainte contre SCS si elles estiment que l'organisation n'a pas respecté une ou plusieurs dispositions des Lois en matière de protection de la vie privée ou que leur vie privée a été compromise. Si vous avez des questions concernant les politiques de la protection de la vie privée de SCS, l'accès à votre dossier, la correction de renseignements ou si vous croyez que vos droits à la protection des renseignements personnels n'ont pas été respectés d'une quelconque façon, vous pouvez communiquer avec notre agent de la protection de la vie privée :

Agent de la protection de la vie privée

SCS pour les personnes ayant une déficience intellectuelle

507 – 1400 boul. St Laurent

Ottawa, ON K1K 4H4

Téléphone : 613-748-1788, poste 245

Télécopieur : 613-748-1018

Privacy@scsonline.ca

Vous pouvez également présenter une demande de soumission d'une plainte au moyen du [Formulaire de demande d'accès, de correction ou de plainte de renseignements personnels](#).

L'agent de la protection de la vie privée étudiera toutes les plaintes et prendra toutes les mesures raisonnables pour régler le problème, généralement au plus tard 30 jours après la demande. Si l'agent de la protection de la vie privée de SCS n'a pas réglé votre problème à votre satisfaction, vous avez le droit de déposer une plainte auprès du commissaire à l'information et à la protection de la vie privée/Ontario (CIPVP). En outre, s'il apprend qu'il y a eu atteinte possible à la vie privée, le CIPVP peut porter plainte lui-même si personne d'autre ne l'a fait. Vous pouvez communiquer avec le commissaire à l'information et à la protection de la vie privée à l'adresse suivante :

Commissaire à l'information et à la protection de la vie privée/Ontario

2, rue Bloor Est, bureau 1400

Toronto (Ontario) M4W 1A8

Téléphone : 416-326-3333 or 1-800-387-0073

En ligne : <https://www.cipvp.ca>

4.0 PIÈCES JOINTES / ANNEXE

Annexe 1– Déclaration en langage claire sur la protection de la vie privée et de la confidentialité.

Vos renseignements ne concernent que vous. La seule façon pour nous de divulguer des renseignements vous concernant est que vous dites OUI au partage de renseignements avec d'autres.

Certaines personnes qui vous aident à payer les services que vous obtenez à la maison, à l'école, dans les programmes de jour ou au travail ont accès à vos renseignements personnels. Ces personnes ne donnent aucun renseignement sur vous à quiconque. Elles gardent vos renseignements privés.

Si une personne payée pour vous aider fournit à un tiers des renseignements personnels vous concernant, elle peut perdre son emploi.

5. RÉFÉRENCES ET POLITIQUES ET PROCÉDURES CONNEXES

- 5.1 [Orientation et formation obligatoire](#)
- 5.2 [Mesures d'assurance de la qualité, Règlement 299/10.](#)
- 5.3 [Loi sur la protection des renseignements personnels sur la santé.](#)
- 5.4 [Loi sur les services à l'enfance et à la famille](#)
- 5.5 [Formulaire de demande d'accès, de correction ou de plainte de renseignements personnels](#)
- 5.6 [Politique en matière de sécurité](#)
- 5.7 [Consentement de SCS à la cueillette et à la divulgation \(rose\)](#)
- 5.8 [Consentement de SCS à la diffusion \(jaune\)](#)
- 6.0 [Consentement à recevoir des communications électroniques](#)

5. DATES DE RÉVISION

HISTORIQUE DE RÉVISION DU DOCUMENT		
Date	Auteur	Révision
Le 24 septembre 2020	N Tardif	Ajout des sections 3.3.4 à 3.3.6 concernant les consentements électroniques.