Politique de confidentialité et de protection des renseignements personnels

Mise à jour et adoptée lors du conseil d'administration de la Clinique SPOT le 16 juin 2025

TABLE DES MATIÈRES

1. INTRODUCTION

SPOT Clinique communautaire de santé et d'enseignement (« SPOT ») accorde une importance primordiale à la protection de la vie privée et des renseignements personnels de toutes les personnes avec qui elle est en relation, incluant notamment les personnes utilisatrices, les membres de son équipe et ses partenaires.

SPOT s'engage à respecter les exigences de la Loi sur la protection des renseignements personnels dans le secteur privé (Loi 25) et à mettre en place les mesures nécessaires pour protéger les renseignements qu'elle collecte, utilise, conserve ou communique.

Cette politique vise à préciser :

- les renseignements collectés,
- les finalités de leur utilisation,
- les mesures de protection mises en place,
- les droits des personnes concernées.

2. RESPONSABLE DE LA PROTECTION DES DONNÉES PERSONNELLES ET COORDONNÉE POUR NOUS JOINDRE

La coordination de la Clinique SPOT assume la responsabilité de la mise en œuvre de cette politique. Pour toute question ou demande relative à la protection des renseignements personnels, il est possible de contacter la coordination générale :

Courriel : coordo@cliniquespot.org
Téléphone : 418-781-2668, poste 112

3. PRINCIPES DIRECTEURS

1. **Principe de responsabilité :** Chaque membre de l'organisation est responsable de la protection des renseignements personnels dont il ou elle a la charge, en respectant la présente politique et les directives de l'équipe de coordination.
2. **Principe de limitation des données :** Les renseignements personnels doivent être collectés uniquement dans la mesure où ils sont nécessaires pour l'exécution des tâches et responsabilités, et en lien avec les fins identifiées.
3. **Principe de consentement :** Le consentement libre, éclairé et manifeste des personnes concernées est requis pour la collecte, l'utilisation et la communication de leurs renseignements personnels, sauf exception prévue par la loi.
4. **Principe de non-divulgation :** Les renseignements personnels ne doivent pas être divulgués ni discutés à des tiers non autorisés, à l'intérieur ou à l'extérieur de

l'organisation, sauf si la personne concernée y a consenti explicitement ou si une obligation légale claire l'exige.

5. **Principe de non-discussion** : Il est interdit d'accepter ou de tolérer que des partenaires ou des tiers divulguent des renseignements personnels sans le consentement de la personne concernée. Toute discussion impliquant des données sensibles doit être encadrée et autorisée.
6. **Principe de sécurité des données** : Des mesures de sécurité appropriées doivent être mises en place pour protéger les renseignements personnels contre tout accès non autorisé, divulgation, altération ou destruction.
7. **Principe de notification** : Toute situation susceptible de compromettre la sécurité ou la confidentialité des renseignements personnels doit être signalée immédiatement à l'équipe de coordination.
8. **Principe de respect des droits :** Les droits des personnes concernées en matière de vie privée, notamment l'accès, la rectification, le retrait du consentement, doivent être respectés.

4. COLLECTE ET UTILISATION DES RENSEIGNEMENTS PERSONNELS

SPOT collecte certains renseignements personnels dans le cadre de ses activités, notamment auprès des personnes utilisatrices, des membres de l'équipe et des partenaires.

Les renseignements personnels collectés peuvent inclure, sans s'y limiter :

- Nom et prénom
- Date de naissance
- Adresse postale et adresse électronique
- Numéro de téléphone
- Numéro d'assurance maladie ou d'assurance sociale
- Informations médicales, psychosociales, socioéconomiques ou administratives
- Informations relatives à l'emploi et à la formation
- Informations financières (relevés bancaires, informations fiscales, etc.)
- Autres renseignements pertinents selon les besoins, en lien avec les services rendus ou la gestion de la clinique

Ces renseignements sont recueillis, notamment aux fins de :

- La prestation des soins et services offerts et la gestion des dossiers des personnes utilisatrices
- La communication avec les personnes concernées par les activités de la clinique
- La gestion des dossiers du personnel et des relations d'emploi
- Le respect des obligations légales, fiscales et contractuelles
- Le développement, le fonctionnement et la reddition de comptes liés aux services et aux partenariats
- La recherche et l'évaluation en lien avec la mission, les soins ou les activités

Seuls les renseignements nécessaires à la réalisation des objectifs précisés ci-dessus sont collectés, en conformité avec les obligations légales en vigueur.

5. CONSENTEMENT

SPOT collecte, utilise et communique des renseignements personnels avec le consentement des personnes concernées, sauf si la loi permet ou exige de procéder autrement.

Le consentement peut être :

- Explicite, par exemple lorsqu'une personne signe un formulaire ou donne son accord verbalement ;
- Implicite, lorsqu'une personne fournit volontairement des renseignements dans un contexte où leur usage est évident (ex. : demande de service).

Le consentement peut être retiré en tout temps, sous réserve des obligations légales ou contractuelles. SPOT informe les personnes concernées des conséquences possibles d'un tel retrait (ex. : on ne pourra plus les rejoindre).

6. DESTRUCTION DES DONNÉES

Les renseignements personnels sont conservés aussi longtemps que nécessaire pour la réalisation de la mission et le respect des obligations légales.

Lorsqu'ils ne sont plus requis, les renseignements personnels doivent être détruits de manière à empêcher toute récupération, reconstitution ou lecture non autorisée.

Documents papier :

- Broyage croisé, déchiquetage ou incinération à l'interne ou par un prestataire certifié.
- Aucun document contenant des renseignements personnels ne doit être jeté aux ordures ou au recyclage sans traitement préalable.

Fichiers numériques :

- Suppression permanente des fichiers à l'aide d'outils sécurisés (ex. : effacement multiple ou logiciel conforme).
- Suppression des sauvegardes, métadonnées ou copies redondantes.
- Si un appareil (ordinateur, disque dur, clé USB, etc.) est mis hors service, il doit être formaté en profondeur ou physiquement détruit.

L'organisme s'engage à revoir périodiquement les documents, qu'ils soient sur support papier ou numérique, contenant des renseignements personnels, afin d'identifier ceux devant être détruits, et à procéder à leur destruction de manière appropriée.

7. CLAUSE DE CONFIDENTIALITÉ

Tous les membres de l'équipe, incluant les personnes contractuelles, étudiantes, en services externes, bénévoles et membres du conseil d'administration, sont liés par une clause de confidentialité. Toute information obtenue dans le cadre des activités de SPOT ne peut être divulguée sans autorisation ou consentement préalable.

8. DIVULGATION À DES TIERS

Les renseignements personnels détenus par SPOT ne sont jamais communiqués à des tiers sans le consentement de la personne concernée, sauf dans les cas prévus par la loi.

En vertu de la Loi sur les services de santé, de la Loi sur la protection des renseignements personnels dans le secteur privé et des principes déontologiques applicables dans les professions de la santé et des services sociaux, la règle est la suivante :

Le secret professionnel est la règle. La divulgation est l'exception.

Certaines situations peuvent justifier ou exiger la communication de renseignements personnels sans consentement préalable, notamment :

- **Urgence vitale ou risque grave et imminent**
  Lorsque la vie, la santé ou la sécurité d'une personne (ou d'autrui) est menacée.
  Exemple : risque de suicide, de violence grave imminente

- **Ordonnance judiciaire ou mandat**
  Une communication écrite peut être exigée si une autorité judiciaire l'ordonne.
  Exemple : la police doit présenter un mandat écrit ou une ordonnance de la cour valide pour obtenir des renseignements.

- **Exigence légale claire**
  Lorsque la loi oblige à communiquer certains renseignements
  Exemple : Déclaration obligatoire de certaines maladies, signalement à la Direction de protection de la jeunesse (DPJ), enquête en santé publique.

- **Suivi d'une plainte par une autorité compétente**
  Lorsqu'une instance responsable de la qualité de l'acte professionnel (Ex. ordre professionnels, commissaires aux plaintes, protecteur du citoyen) demande des renseignements dans le cadre du traitement d'une plainte.
  Exemple : un ordre professionnel exige un dossier clinique pour examiner une plainte contre un·e intervenant·e.

- **Collaboration clinique**
  Dans certains cas, des renseignements personnels peuvent également être communiqués à des partenaires qui collaborent directement à la prestation des soins.

Cette communication s'effectue dans le respect du secret professionnel et toujours dans la limite de ce qui est strictement requis pour assurer les soins.

- **Réorganisation ou transfert d'activités**
  Des renseignements personnels peuvent être communiqués dans le cadre d'une réorganisation, d'un transfert de services ou d'une fusion, lorsque cela est nécessaire à la poursuite de la mission de la clinique et que des engagements de confidentialité sont mis en place.

- **Protection de la sécurité de l'organisation**
  SPOT peut divulguer certains renseignements personnels si elle estime, en toute bonne foi, qu'une telle communication est nécessaire pour assurer la sécurité de ses activités, prévenir une menace ou se conformer à une exigence liée à une enquête légitime.

Dans tous les cas, seule l'information strictement nécessaire et explicitement demandée est transmise.

9. TRANSFERT À L'EXTÉRIEUR DU QUÉBEC

Lorsqu'un renseignement personnel doit être transmis à l'extérieur du Québec, SPOT s'assure, dans la mesure du possible, que le pays ou le territoire de destination offre des protections similaires à celles prévues par la Loi 25.

Toutefois, dans les cas d'urgence ou de nécessité — notamment dans certaines situations de soins, comme lorsqu'une personne accouche ou reçoit des traitements à l'étranger — le transfert de renseignements peut être requis, même si le pays ne garantit pas une protection équivalente.

Dans ces cas, SPOT privilégie de remettre les renseignements directement à la personne concernée (plutôt que de les transmettre à un tiers), afin qu'elle puisse les communiquer elle-même au professionnel de son choix.

10. ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE (ÉFVP)

Lorsqu'un projet implique une nouvelle technologie ou de nouvelles pratiques qui modifient la gestion des renseignements personnels au sein de l'organisme, SPOT procède à une ÉFVP afin d'évaluer les risques pour la vie privée et de déterminer les mesures de protection appropriées.

L'ÉFVP inclut notamment :

- une description du projet ou de la situation visée ;
- les renseignements personnels concernés ;
- les risques potentiels pour la vie privée ;

- les mesures prévues pour limiter ces risques (ex. : accès restreint, chiffrement, entente de confidentialité).

Cette évaluation est réalisée par écrit, par la coordination générale ou par toute autre personne désignée, et peut être documentée de façon simple.

11. MESURES DE SÉCURITÉ

SPOT met en place des mesures organisationnelles, technologiques et physiques pour assurer la confidentialité, l'intégrité et la sécurité des renseignements personnels.

Ces mesures incluent notamment :

- **Gestion des accès** : seuls les membres du personnel autorisés peuvent accéder aux renseignements personnels, selon leur rôle et les besoins liés à leurs fonctions.
- **Choix des lieux et contextes de soin** : SPOT applique le principe de coresponsabilité dans le choix des lieux d'intervention afin d'assurer la confidentialité des échanges :
    - L'équipe de coordination oriente les pratiques et favorise la mise en place d'espaces et contextes de soins adéquats permettant de respecter au maximum la confidentialité, tout en adoptant une approche de proximité;
    - Chaque intervenant·e ou soignant·e demeure responsable d'évaluer le contexte de soins et services (espace, intimité, niveau de confidentialité) et d'adapter sa manière d'intervenir pour protéger la vie privée des personnes.
- **Sauvegarde et protection des systèmes** : des solutions de stockage sécurisé et de sauvegarde sont en place pour prévenir les pertes accidentelles ou les atteintes à l'intégrité des données, tant sur support papier que numérique.
- **Gestion des incidents** : des procédures sont prévues pour détecter, signaler et gérer les incidents de sécurité ou de confidentialité.
- **Sensibilisation** : les personnes impliquées à Spot sont formées et encadrées afin de respecter les politiques internes de confidentialité et leurs obligations légales.
- **Gestion des partenaires** : tout partenaire ayant accès à des renseignements personnels est tenu de respecter des engagements de confidentialité, de sécurité, de limitation d'usage et de gestion des incidents de confidentialité.

12. ACCÈS, RECTIFICATION, PORTABILITÉ ET RETRAIT DU CONSENTEMENT

Toute personne peut demander :

- L'accès à ses renseignements personnels
- Leur rectification en cas d'erreur
- Le retrait de son consentement à tout moment
- La portabilité de ses renseignements personnels, c'est-à-dire leur transmission dans un format technologique structurant, couramment utilisé, pour les transmettre à un autre organisme ou fournisseur de services, lorsque techniquement possible

SPOT s'engage à répondre à toute demande dans un délai raisonnable.

13. UTILISATION DE TÉMOINS (COOKIES) ET LIEN VERS D'AUTRES SITES

Le site Web de SPOT peut utiliser des témoins de navigation pour des fins de fonctionnement ou d'analyse. Il est possible de configurer son navigateur pour les refuser.

Le site Web de SPOT peut contenir des liens vers des sites tiers. SPOT n'est pas responsable des pratiques de ces sites. Il est recommandé de consulter leur politique de confidentialité.

14. MODIFICATIONS À LA POLITIQUE

SPOT se réserve le droit de modifier cette politique en tout temps. La version la plus récente et mise à jour sera rendue disponible sur le site Web de l'organisation.

15. CONCLUSION ET COORDONNÉES POUR NOUS JOINDRE

La Clinique SPOT accorde une grande importance à la protection de la vie privée et au respect des renseignements personnels des personnes avec qui elle est en lien. Elle s'engage à traiter ces renseignements avec rigueur, sensibilité et en conformité avec les lois en vigueur.

Malgré toutes les mesures mises en place, SPOT ne peut garantir l'impossibilité absolue d'un incident de sécurité, mais s'engage à réagir promptement à toute situation compromettante.

16. ANNEXES

ANNEXE A : PROCÉDURE DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ

Cette procédure vise à réagir rapidement et efficacement à tout incident pouvant compromettre la confidentialité des renseignements personnels détenus par la Clinique SPOT.

1. Détection d'un incident

Toute personne liée à SPOT (employé·e, stagiaire, bénévole, administrateur·trice, etc.) doit signaler immédiatement à la coordination générale toute situation suspecte, perte de données, accès non autorisé ou autre incident lié à des renseignements personnels.

2. Évaluation de l'incident

La coordination générale (ou une personne désignée) évalue rapidement :

- les renseignements touchés et leur degré de sensibilité ;
- le nombre de personnes concernées ;
- les risques possibles (fraude, atteinte à la vie privée, etc.).

L'incident est classé selon sa gravité :

- Mineur : sans conséquence réelle pour les personnes ;
- Modéré : peut causer un inconfort ou une difficulté pour les personnes ;
- Majeur : risque sérieux de préjudice (ex. : vol d'identité, stigmatisation, exploitation).

3. Prise en charge et soutien externe

La coordination générale prend en charge l'incident en mettant en place les mesures nécessaires pour limiter les conséquences et en appliquant les correctifs appropriés. Cela peut inclure : désactiver un accès, corriger une erreur, renforcer une mesure de sécurité, etc.

Si l'incident dépasse l'expertise disponible à l'interne ou présente un risque important, elle en informe le conseil d'administration et peut recommander de faire appel à un·e expert·e externe.

4. Avis aux personnes concernées et à la Commission d'accès à l'information (CAI)

Si l'incident peut causer un préjudice sérieux (ex. : vol d'identité, fraude), SPOT doit :

- aviser les personnes concernées le plus rapidement possible ;

- aviser la Commission d'accès à l'information (CAI), comme l'exige la loi.

L'avis comprend ce qui s'est passé, ce qui a été fait et comment se protéger.

Commission d'accès à l'information
525, boulevard René-Lévesque Est, Bur. 2.36
Québec (Qc) G1R 5S9
Téléphone : 418 528-7741 – Sans frais : 1 888 528-7741 – Télécopieur : 418 529-3102
Courrier électronique : cai.communications@cai.gouv.qc.ca

5. Suivi et amélioration

Après l'incident, la coordination générale fait le point sur ce qui s'est passé et propose, au besoin:

- des ajustements aux pratiques,
- de la formation supplémentaire,
- ou une mise à jour de la politique.

6. Registre des incidents

Chaque incident est noté dans un registre confidentiel, avec :

- ce qui s'est passé ;
- les personnes touchées ;
- les mesures prises ;
- les notifications effectuées ;
- les recommandations de suivi.