Fellice stratégies humaines
5 septembre 2023

POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Cette Politique vise à informer les clientèles visées sur la collecte, l'utilisation ou la divulgation de renseignements personnels, et à clarifier les pratiques en la matière aux fins du bon fonctionnement de Fellice stratégies humaines (FSH).

La présente Politique est régie par les lois de la province de Québec et les lois du Canada qui s'y appliquent, notamment par les lois sur la protection des renseignements personnels et par les lois et règlements encadrant la pratique des professionnels concernés chez FSH.

1. Collecte des renseignements personnels

Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier.

Les informations personnelles sur tout client peuvent être recueillies à des fins légitimes en relation avec les mandats qui lui sont confiés par un individu ou une organisation.

À cet effet, il est possible de recueillir des informations personnelles avant même la première rencontre de tout client, aux fins d'obtenir les renseignements sur les besoins, la situation personnelle et professionnelle, dont notamment mais sans limiter la généralité de ce qui précède, afin d'obtenir ses coordonnées et de communiquer avec lui.

Les renseignements personnels concernant les clients sont recueillis dans le cadre de diverses communications avec une personne de FSH, notamment lors de toute communication écrite, téléphonique ou électronique et de toute rencontre de tout client.

Des renseignements sont aussi recueillis auprès de tiers payeurs avec lequel il doit transiger, notamment les employeurs et les collègues.

2. Nature des renseignements personnels colligés

Dans le cadre des activités et services offerts, différents types de renseignements personnels sur l'identité, l'éducation, l'emploi et la santé sont recueillis, incluant les renseignements énumérés ci-dessous :

- Des coordonnées, tels les noms et prénoms, l'adresse postale, l'adresse courriel, le numéro de téléphone, la date de naissance des personnes qui consultent ;
- Des renseignements relatifs aux services rendus et aux rendez-vous ;
- Des informations relatives aux transactions et aux paiements, comme le mode de paiement utilisé, la date et l'heure, le montant du paiement et autres informations connexes ;

- Des renseignements que le client choisit de fournir ou de transmettre, comme des formulaires, des questionnaires, un curriculum vitae ;
- Des renseignements recueillis automatiquement lors de la passation de tests ou d'outils d'évaluation en ligne.

Les renseignements personnels collectés sont recueillis au travers de formulaires et grâce à l'interactivité établie entre le client et la personne de FSH. Ces renseignements sont recueillis pour plusieurs raisons :

- Pour correspondre avec le client ;
- Pour orienter les services ;
- Pour prendre les rendez-vous ;
- Pour repérer les clients et les dossiers associés ;
- Pour communiquer avec les clients au besoin (p. ex., changements apportés aux rendez-vous) ;
- Pour des fins administratives et comptables, y compris le recouvrement des paiements et la facturation aux tiers payeurs ;
- Pour consigner et faciliter l'élaboration et la prise en charge d'une évaluation, d'un diagnostic, d'un traitement, d'une continuité d'interventions appropriées.

3. Consentement du client

Le consentement du client est obtenu à travers le formulaire de consentement à la première séance. Par la suite, en continuant de participer à l'évaluation, à l'intervention ou à la thérapie, le client continue à donner son consentement à la collecte, à l'utilisation et à la divulgation des renseignements personnels pour les fins du traitement ou de sa démarche. Certaines informations peuvent, toutefois, être partagées avec le tiers payeur lorsque requis pour l'intervention ou sa continuité.

4. Utilisation des renseignements personnels

- Les renseignements personnels ne sont pas utilisés, divulgués ou conservés pour des fins autres que celles pour lesquelles ils ont été recueillis, à moins que le client n'ait donné son consentement à cet effet.
- Les renseignements personnels collectés sont conservés dans un environnement sécurisé. Les personnes travaillant pour FSH sont tenues de respecter la confidentialité des informations.
- Certains renseignements personnels peuvent être divulgués sans le consentement du client si la loi l'exige ou l'autorise (voir les *Limites de la confidentialité*).
- Certains renseignements personnels requis afin d'assurer le paiement ou la continuité des services sont uniquement divulgués aux tiers payeurs au besoin, le cas échéant.
- Tous les efforts sont déployés pour veiller à l'exactitude des renseignements personnels.
- Les renseignements personnels, sous format papier et électronique, sont conservés en toute sécurité.

5. Limites de la confidentialité :

En matière d'exception à la règle de confidentialité, un membre d'un ordre professionnel de la santé mentale et des relations humaines a l'obligation légale de :

- Prévenir une victime potentielle qu'un client a l'intention de lui causer un préjudice ;
- Prévenir les autorités et les professionnels de la santé compétents lorsqu'il a un motif raisonnable de croire qu'un danger imminent de mort ou de blessures graves menace une personne ou un groupe de personnes identifiables (ex. suicide, homicide) ;
- Communiquer le dossier d'un client lorsqu'il est exigé par un tribunal ;
- Répondre, sous serment, aux questions posées par la Cour en tant que témoin devant un tribunal ;
- Répondre à toutes les questions de l'ordre professionnel concerné si le comportement éthique d'un intervenant fait l'objet d'une enquête ;
- Signaler aux autorités compétentes tout cas d'abus ou d'exploitation d'un enfant, d'une personne âgée ou d'une personne handicapée ;
- Signaler un cas d'abus ou d'exploitation d'un client ou d'un patient par un professionnel de la santé.

6. Stockage et sécurité

Tous les renseignements personnels fournis sont conservés sur des serveurs sécurisés, à accès restreint au personnel de Fellice stratégies humaines.

FSH utilise les moyens techniques raisonnables pour assurer un environnement sécuritaire et protéger les renseignements personnels, tels que : barrières coupe-feu, usage d'antivirus, gestion des accès, détection des intrusions, copie de sauvegarde régulière.

Cependant, étant donné la nature même du réseau public qu'est l'internet, les clients reconnaissent et acceptent que la sécurité des transmissions via internet ne puisse être garantie. En conséquence, FSH ne peut garantir ni n'assume aucune responsabilité pour toute violation de confidentialité, piratage, virus, perte ou altération des données transmises par Internet.

7. Conservation

FSH utilise et conserve les renseignements personnels pour la durée nécessaire à l'objet de la collecte des renseignements.

Toutefois, Fellice stratégies humaines se réserve le droit de détenir, pour une durée raisonnable, certains renseignements personnels pour être en règle avec la Loi, prévenir la fraude, collecter des frais dus, résoudre une réclamation ou certains autres problèmes s'y rattachant, coopérer à une enquête et pour tout autre acte permis ou requis par la loi, notamment les règlements professionnels sur la conservation des dossiers.

À l'expiration de ces délais, les renseignements personnels seront délestés des serveurs de FSH.

8. Droits du client

- Les clients ont le droit de savoir pourquoi leurs renseignements personnels sont recueillis, comment ils sont utilisés et à qui ils sont communiqués.
- Les clients ont le droit de demander un accès approprié à leurs renseignements personnels. Des frais peuvent s'appliquer pour traiter cette demande d'accès.
- Les clients ont le droit de contester l'exactitude et l'exhaustivité de leurs renseignements et de demander une modification à ceux-ci.
- Un droit d'opposition et de retrait quant aux renseignements personnels peut être exercé.
- Pour toute demande d'accès aux renseignements personnels, ou pour exercer les droits prévus, les clients doivent s'adresser à la personne responsable des renseignements personnels.

9. Incidents de confidentialité

Un incident de confidentialité correspond à un accès non autorisé par la Loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.

Le responsable de la protection des renseignements personnels, s'il a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient, doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

Le responsable de la protection des renseignements personnels procède à l'évaluation du préjudice selon la procédure prévue à l'Annexe 1.

Le responsable de la protection des renseignements personnels tient un registre des incidents de confidentialité (Annexe 2) et, sur demande de la Commission d'accès à l'information, lui en transmet une copie.

Les renseignements contenus au registre des incidents de confidentialité doivent être tenus à jour et conservés pendant une période minimale de cinq ans après la date ou la période au cours de laquelle le responsable a pris connaissance de l'incident.

Personne responsable de la protection des renseignements personnels :

La personne responsable de la protection des renseignements personnels et qui veille à assurer le respect et la mise en œuvre de la loi est **Diane Fellice**, présidente de Fellice stratégies humaines.
Diane Fellice
dfellice@fellice.com
(514) 207-3036

ANNEXE 1

SERMENT DE DISCRÉTION DU PERSONNEL DE FELLICE STRATÉGIES HUMAINES

Sous réserve des dispositions relatives à l'accès à l'information et à la protection des renseignements personnels, toute personne agissant au nom de Fellice Stratégies humaines est tenue à la discrétion – obligation qui implique notamment de ne pas communiquer une information confidentielle – sur ce dont elle a connaissance dans l'exercice de ses fonctions et en lien avec celles-ci.

Je reconnais que pendant la durée de mon mandat chez Fellice stratégies humaines, j'aurai accès à des renseignements de nature confidentielle et/ou exclusive concernant la vie privée, les intérêts ou les droits des clients et de l'entreprise elle-même. Ces renseignements peuvent se rattacher notamment aux données personnelles et financières des clients, aux documents relatifs à la gestion financière, administrative ou technique de FSH, à ses liens avec des organisations, etc.

Je reconnais également que ces informations ne doivent pas être divulguées sans l'autorisation de FSH ou des personnes concernées, sauf si la loi l'exige ou le permet.

Aussi, je consens à ne jamais utiliser, ni publier, ni divulguer lesdites informations pendant ou suivant mon mandat chez FSH, et je prendrai toutes les mesures raisonnables pour protéger la nature restreinte de cette information à moins que celle-ci ne devienne disponible au public ou soit légalement obtenue d'une tierce partie en dehors de la portée de la présente entente.

À la fin de mon mandat, je purgerai mes dossiers (papiers et électroniques) de tous renseignements personnels obtenus dans le cadre de mon mandat, après avoir transféré l'ensemble des informations, dossiers, et/ou renseignements, auprès FSH lorsque requis tout en conservant les informations exigées en vertu des règlements sur la conservation des dossiers de mon ordre professionnel.

Je, _____, déclare avoir reçu et pris connaissance des obligations applicables en matière de confidentialité et m'engage à les respecter.

_____ _____

Signature du mandataire Date

ANNEXE 2

PROCÉDURE A SUIVRE EN CAS D'INCIDENT DE CONFIDENTIALITÉ

Les étapes qui suivent peuvent être réalisées simultanément.

1. **Évaluer la situation.** Le responsable qui a des raisons de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient doit notamment :
   a. Établir les circonstances de l'incident ;
   b. Identifier les renseignements personnels impliqués ;
   c. Identifier les personnes concernées ;
   d. Trouver le problème, que ce soit une erreur, une vulnérabilité, etc. Cette évaluation doit se poursuivre tant que tous les éléments n'ont pas été identifiés.

2. **Diminuer les risques.** Le responsable doit prendre rapidement les mesures raisonnables qui s'imposent afin de diminuer les risques qu'un préjudice, qu'il soit sérieux ou non, ne soit causé et pour éviter que de nouveaux incidents de même nature ne surviennent, par exemple :
   a. Cesser la pratique non autorisée ;
   b. Récupérer ou exiger la destruction des renseignements personnels impliqués ;
   c. Corriger les lacunes informatiques.

3. **Identifier la nature du préjudice**. L'objectif consiste à déterminer s'il faut aviser la Commission d'accès à l'information (CAI) et les personnes concernées ainsi qu'établir les mesures à mettre en place pour diminuer les risques notamment :
   a. Inscrire une note dans les dossiers visés par un risque de vol d'identité ;
   b. Exiger des vérifications supplémentaires.

4. **Évaluer le préjudice.** Lors d'un incident de confidentialité, le responsable doit évaluer s'il en découle un risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné. Il doit alors considérer plusieurs facteurs, dont :
   - La sensibilité des renseignements personnels tels un renseignement financier ou un renseignement d'identité ;
   - Les conséquences appréhendées de l'utilisation de ces renseignements ;
   - La probabilité que ces renseignements puissent être utilisés à des fins préjudiciables.

   Un préjudice sérieux correspond à un acte ou à un événement susceptible de porter atteinte à la personne ou à ses biens et de nuire à ses intérêts de manière non négligeable. Il peut conduire, par exemple :

   - À l'humiliation ;
   - À une atteinte à la réputation ou à la vie privée ;
   - À une fraude ou à une perte financière ;
   - À un vol d'identité ;
   - À des conséquences négatives sur un dossier de crédit ;
   - À une perte d'emploi.

5. **Inscrire l'incident au registre, que le risque de préjudice soit qualifié ou non de sérieux.**

6. **S'il y a un risque de préjudice sérieux, le responsable doit :**

   a. Aviser la Commission d'accès à l'information dès que possible, même s'il n'a pas colligé l'ensemble des informations relatives à l'incident, et remplir la déclaration par la suite. Il peut ainsi aviser la Commission de l'incident et, plus tard, confirmer le nombre de personnes concernées.

   b. Aviser toute personne dont un renseignement personnel est concerné par l'incident, à moins que cet avis ne soit susceptible d'entraver une enquête. Un délai peut s'appliquer entre le moment où le responsable prend connaissance de l'incident et celui où il en avise les personnes concernées. Ce délai peut être nécessaire afin, par exemple, d'identifier les renseignements personnels impliqués, les personnes concernées, la faille de sécurité et pour colmater celle-ci ou pour éviter d'entraver une enquête en cours.

   Ces avis sont obligatoires.

7. **S'il y a un risque de préjudice sérieux, le responsable peut** :

   Aviser toute personne ou tout organisme susceptible de diminuer ce risque. À cette fin, il ne peut lui communiquer que les renseignements personnels qui sont nécessaires à la poursuite de cet objectif.

   L'obtention du consentement de la personne concernée par les renseignements transmis n'est pas requise. Toutefois, la personne responsable de la protection des renseignements personnels doit enregistrer la communication pour garder des traces documentaires de celle-ci comme :

   - À qui ces renseignements sont communiqués ;
   - Dans quelles circonstances ;
   - Quels renseignements ont été transmis ;
   - Quels sont les objectifs de cette démarche.

ANNEXE 3

REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

INCIDENT			PERSONNES CONCERNÉES		CAI	MESURES PRISES	
Date	**Renseignements**	**Circonstances**	**Nombre**	**Date de l'avis**	**Date de l'avis**	**Date de la connaissance**	**Mesures prises**