PLAN DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ

Médiation familiale &
services sociaux

Family Mediation &
Social Services

SHERBROOOKE, QC

Procédure de conservation, de destruction et d’anonymisation des renseignements personnels

1. Aperçu

Il est important de mettre en place une procédure de conservation, de destruction et d'anonymisation des renseignements personnels pour garantir la protection de la vie privée des individus, se conformer aux lois sur la protection des renseignements personnels, prévenir les incidents de confidentialité impliquant des renseignements personnels et les atteintes à la sécurité, maintenir la confiance des clients et protéger la réputation de l'organisation.

2. Objectif

Le but de cette procédure est de garantir la protection de la vie privée des individus et de se conformer aux obligations légales en matière de protection des renseignements personnels.

3. Portée

La portée de cette procédure devrait couvrir l'ensemble du cycle de vie des renseignements personnels, depuis leur collecte jusqu'à leur destruction. Elle concerne tous les employés et parties prenantes impliquées dans la collecte, le traitement, la conservation, la destruction et l'anonymisation des renseignements personnels conformément aux exigences légales et aux bonnes pratiques en matière de protection de la vie privée.

4. Définitions

- **Renseignements personnels :** toute information permettant d'identifier, directement ou indirectement, une personne physique.
- **Conservation :** stockage sécurisé des renseignements personnels pendant la durée requise.
- **Destruction :** suppression, élimination ou effacement définitif des renseignements personnels.
- **Anonymisation :** processus de modification des renseignements personnels de manière à ne plus permettre en tout temps et de façon irréversible l'identification, directe ou indirecte, des individus concernés.
- **Incident de confidentialité** : Un incident de confidentialité désigne toute situation où des renseignements personnels sont consultés, utilisés ou communiqués sans autorisation, y compris, sans s’y limiter :

- l'accès non autorisé à des données confidentielles concernant un client ;
- la perte, le vol ou l'égarement de dossiers physiques ou électroniques contenant des renseignements personnels ;
- le partage ou l'exposition involontaire de renseignements personnels.

5. Procédure

5.1 Durée de conservation

Selon les normes de l'OTSTCFQ en matière de tenue de dossiers et de pratiques professionnelles, la Norme IV : Conservation et archivage des dossiers exige que les travailleurs sociaux et les thérapeutes conjugaux et familiaux conservent les dossiers des clients de manière sécuritaire afin d'en assurer la confidentialité. Ces dossiers doivent être conservés pendant au moins cinq ans après la dernière intervention. Après ce délai, ils peuvent être détruits de manière à préserver leur caractère confidentiel.

5.2 Méthodes de conservation sécuritaire

5.2.1 - Les renseignements personnels sont conservés aux endroits suivants : Owl Practice – logiciel de gestion de pratique clinique, ainsi que sur l'ordinateur personnel de Theresa Gagnon, TS/médiatrice familiale.

5.2.2 Le degré de sensibilité de chacun de ces emplacements de stockage a été établi.

5.2.3 Ces lieux de conservation, qu'ils soient papier ou numériques, sont adéquatement sécurisés.

5.2.4 L'accès à ces installations de stockage est restreint à Theresa Gagnon, TS/médiatrice familiale.

5.3 Destruction des renseignements personnel

5.3.1 Les renseignements personnels sur support papier doivent être détruits par déchiquetage complet.

5.3.2 Les renseignements personnels sous forme numérique doivent être supprimés de façon complète des appareils (ordinateurs, téléphones, tablettes, disques durs externes), des serveurs et des outils infonuagiques.

5.3.3 Un calendrier de destruction fondé sur la période de conservation établie pour chaque catégorie de renseignements personnels doit être élaboré. Les dates de destruction prévues doivent être consignées.

5.3.4 Il doit être assuré que la destruction est effectuée de manière à ce que les renseignements personnels ne puissent être récupérés ni reconstitués.

5.4 Anonymisation des renseignements personnels

5.4.1 Les renseignements personnels ne doivent être anonymisés que lorsque l'organisation souhaite les conserver et les utiliser à des fins sérieuses et légitimes.

5.4.2 La méthode privilégiée d'anonymisation des renseignements personnels consiste à effacer toute trace permettant d'identifier la personne concernée.

5.4.3 Des mesures doivent être prises afin de s'assurer que les renseignements

résiduels ne permettent plus, de façon irréversible, l'identification directe ou indirecte des personnes concernées. Il convient également d'évaluer régulièrement le risque de réidentification des données anonymisées, notamment au moyen de tests et d'analyses visant à en assurer l'efficacité.

Veuillez noter qu'au moment de la rédaction du présent document, l'anonymisation des renseignements personnels à des fins sérieuses et légitimes n'est pas possible. Un règlement gouvernemental doit être adopté afin d'en déterminer les critères et les modalités.

6. Formation et sensibilisation

Il est nécessaire de s'assurer que le ou la praticienne reçoit une formation régulière aux procédures relatives à la conservation, à la destruction et à l'anonymisation des renseignements personnels, ainsi qu'aux risques liés aux atteintes à la vie privée. Cette formation doit également inclure une sensibilisation aux bonnes pratiques en matière de sécurité des données et à l'importance de respecter les procédures établies.

Procédure de demande d'accès aux renseignements personnels et de traitement des plaintes

1. Aperçu

Étant donné qu'une personne peut demander l'accès aux renseignements personnels qu'une organisation détient à son sujet, ou formuler une plainte, il est important de disposer de lignes directrices prédéfinies pour répondre à ce type de demande.

2. Objectif

La présente procédure vise à assurer que toutes les demandes d'accès soient traitées de manière confidentielle, diligente et exacte, dans le respect des droits des personnes concernées.

3. Champ d'application

La présente procédure s'applique aux personnes internes responsables du traitement des demandes d'accès et de la gestion des plaintes, ainsi qu'aux personnes souhaitant accéder à leurs propres renseignements personnels.

4. Procédure

4.1 Soumission de la demande

4.1.1 Toute personne souhaitant accéder à ses renseignements personnels doit soumettre une demande écrite à Theresa Gagnon, travailleuse sociale. La demande peut être transmise par courriel ou par la poste (Postes Canada).

4.1.2 Theresa transmettra ensuite un formulaire en ligne, indiquant clairement qu'il s'agit d'une demande d'accès à des renseignements personnels, et demandera les informations nécessaires pour identifier la personne et les renseignements visés.

4.1.3 Ces informations peuvent inclure le nom, l'adresse et tout autre renseignement pertinent permettant d'identifier de manière fiable la personne qui formule la demande.

4.2 Réception de la demande

4.2.1 Une fois la demande reçue, un accusé de réception est transmis à la personne afin de

confirmer que la demande a bien été prise en compte.

4.2.2 La demande doit être traitée dans un délai de trente (30) jours suivant sa réception.

4.2.3 Si ce délai ne peut être respecté, la personne requérante doit être informée de l'état d'avancement du traitement tout au long du processus.

4.3 Vérification de l'identité

4.3.1 Avant de traiter la demande, l'identité de la personne doit être vérifiée de manière raisonnable. Cette vérification peut se faire par la demande d'informations supplémentaires ou par une vérification en personne.

4.3.2 À titre d'exemples, les informations supplémentaires demandées peuvent inclure des détails concernant la dernière collaboration, le montant de la dernière facture, etc.

4.3.3 Si l'identité ne peut être vérifiée de manière satisfaisante, Theresa Gagnon, travailleuse sociale, peut refuser de communiquer les renseignements personnels demandés.

4.4 Réponse aux demandes incomplètes ou excessives

4.4.1 Si une demande d'accès est incomplète ou excessive, la personne responsable de la protection des renseignements personnels communiquera avec la personne afin d'obtenir des précisions ou des informations supplémentaires.

4.4.2 Avant de divulguer l'ensemble des renseignements personnels détenus, il est recommandé de vérifier avec la personne si l'accès à l'ensemble des informations est réellement requis ou si une liste sommaire des catégories de renseignements personnels détenus serait suffisante.

4.4.3 Theresa Gagnon, travailleuse sociale, se réserve le droit de refuser une demande lorsqu'elle est manifestement abusive, excessive ou injustifiée.

4.5 Traitement de la demande

4.5.1 Une fois l'identité vérifiée, la personne responsable du traitement des demandes d'accès procède à la collecte des renseignements personnels demandés.

4.5.2 Les dossiers pertinents sont consultés afin de recueillir les renseignements demandés, dans le respect des restrictions légales applicables.

4.6 Révision des renseignements

4.6.1 Avant toute communication, les renseignements personnels sont soigneusement

examinés afin de s'assurer qu'ils ne contiennent pas de renseignements concernant des tiers ou d'informations susceptibles de porter atteinte aux droits d'autrui.

4.6.2 Lorsque des renseignements concernant des tiers sont présents, une analyse est effectuée afin de déterminer s'ils peuvent être dissociés ou s'ils doivent être exclus de la communication.

4.7 Communication des renseignements

4.7.1 Une fois le processus de vérification complété, les renseignements personnels sont communiqués à la personne dans un délai raisonnable, conformément aux exigences légales applicables.

4.7.2 Les renseignements peuvent être transmis par voie électronique, par courrier postal sécurisé ou en personne, selon la préférence de la personne et les mesures de sécurité appropriées.

4.8 Suivi et documentation

4.8.1 Chaque étape du traitement d'une demande d'accès doit être documentée de façon complète et rigoureuse.

4.8.2 Les éléments suivants doivent être consignés dans un registre dédié aux demandes d'accès :

- la date de réception de la demande ;
- la date d'envoi de l'accusé de réception ;
- la date de vérification de l'identité ;
- la méthode utilisée pour la vérification de l'identité ;
- la décision rendue concernant la demande (acceptée ou refusée) ;
- la date de communication des renseignements, le cas échéant.

4.9 Protection de la confidentialité

4.9.1 Theresa Gagnon, travailleuse sociale, en tant que seule personne responsable du traitement des demandes d'accès aux renseignements personnels, doit respecter des obligations strictes de confidentialité et se conformer aux protocoles de protection des données. Cette obligation est renforcée par le code de déontologie et les responsabilités professionnelles applicables.

4.10 Gestion des plaintes et recours

4.10.1 Toute personne insatisfaite de la réponse à sa demande d'accès doit être informée

des procédures de plainte et des recours possibles auprès de la Commission d'accès à l'information.

4.10.2 Les plaintes sont traitées conformément aux politiques et procédures établies en matière de gestion des plaintes, lesquelles sont détaillées à la section suivante.

5. Procédure de traitement des plaintes

5.1 Réception des plaintes

5.1.1 Les plaintes peuvent être transmises par écrit, par téléphone, par courriel ou par tout autre moyen de communication officiel. Toutes les plaintes sont consignées dans un registre centralisé, accessible uniquement à Theresa Gagnon, travailleuse sociale.

5.1.2 En cas de plainte, Theresa Gagnon, travailleuse sociale, informera la personne de la possibilité de s'adresser à l'Ordre des travailleurs sociaux et des thérapeutes conjugaux et familiaux du Québec (OTSTCFQ) pour la suite des démarches.

5.1.3 L'OTSTCFQ est responsable de la réception, de l'analyse, de l'enquête et de la détermination des mesures ou sanctions applicables. Pour plus d'informations, il convient de se référer aux lignes directrices de l'OTSTCFQ en matière de protection du public.

Procédure de demande de désindexation et de suppression des renseignements personnels

1. Aperçu

La présente procédure vise à répondre aux préoccupations liées à la protection de la vie privée et à la confidentialité concernant le traitement des renseignements personnels.

2. Objectif

L'objectif de cette procédure est d'établir un processus clair pour la gestion des demandes des clients relatives à la désindexation et à la suppression de leurs renseignements personnels.

3. Champ d'application

La présente procédure s'applique à la personne responsable du traitement des demandes de désindexation et de suppression des renseignements personnels. Elle couvre l'ensemble des renseignements personnels publiés sur des plateformes en ligne, incluant les sites web, les applications mobiles, les bases de données ou tout autre média numérique.

4. Définitions

Suppression des renseignements personnels : Retrait complet et permanent des données, de manière à ce qu'elles ne soient plus accessibles ni récupérables.

Désindexation des renseignements personnels : Processus visant à retirer des renseignements des index des moteurs de recherche, réduisant leur visibilité tout en demeurant accessibles directement à partir de leur source.

5. Procédure

5.1 Réception des demandes

5.1.1 Les demandes de désindexation et de suppression de renseignements personnels doivent être soumises à la personne responsable de la protection des renseignements personnels.

5.1.2 Les demandes peuvent être transmises par courriel ou par courrier postal.

5.2 Vérification de l'identité

5.2.1 Avant le traitement de la demande, l'identité de la personne doit être vérifiée de manière raisonnable. Cette vérification peut inclure la demande d'informations supplémentaires ou une vérification en personne.

5.2.2 À titre d'exemples, les informations supplémentaires demandées peuvent inclure des détails concernant la dernière collaboration, le montant de la dernière facture ou tout autre renseignement permettant de confirmer l'identité.

5.2.3 Si l'identité de la personne ne peut être vérifiée de façon satisfaisante, la demande peut être refusée.

5.3 Évaluation des demandes

5.3.1 La personne responsable examine attentivement chaque demande ainsi que les renseignements personnels visés afin d'évaluer leur admissibilité à la désindexation ou à la suppression.

5.3.2 Les demandes doivent être traitées de manière confidentielle et dans les délais prescrits, soit dans un délai de trente (30) jours suivant leur réception.

5.4 Motifs de refus

5.4.1 Une demande peut être refusée pour des motifs valables, notamment :

- la nécessité de conserver les renseignements afin de poursuivre la prestation de biens ou de services à la personne concernée ;
- des obligations légales liées au droit du travail ;
- des exigences légales en lien avec un litige en cours.

5.5 Désindexation ou suppression des renseignements personnels

5.5.1 La personne responsable prend les mesures appropriées afin de procéder à la désindexation ou à la suppression des renseignements personnels, conformément aux demandes approuvées.

5.6 Suivi et communication

5.6.1 La personne responsable communique avec la personne requérante tout au long du processus, notamment pour accuser réception de la demande et fournir des mises à jour sur l'état d'avancement.

5.6.2 Tout délai ou difficulté rencontrée dans le traitement de la demande doit être

communiqué clairement, accompagné des explications appropriées.

5.7 Suivi et documentation

5.7.1 L'ensemble des étapes liées au traitement des demandes de désindexation et de suppression des renseignements personnels doit être documenté de façon complète et rigoureuse.

5.7.2 Les dossiers doivent inclure les détails des demandes, les actions posées, les dates pertinentes ainsi que les résultats des mesures prises.

Bonnes pratiques et outils en ligne pour la protection des renseignements personnels

Utiliser des mots de passe robustes
Utilisez des mots de passe de 16 à 20 caractères, composés d'une combinaison de lettres, de chiffres et de caractères spéciaux. Évitez toute information personnelle évidente et utilisez un mot de passe différent pour chaque compte.

Gestionnaires de mots de passe
Utilisez un gestionnaire de mots de passe tel que Dashlane, Bitwarden, NordPass, KeePass ou 1Password pour générer, stocker et gérer vos mots de passe de manière sécurisée.

Activer l'authentification à deux facteurs
Activez l'authentification à deux facteurs (2FA) lorsque cela est possible. Cette mesure ajoute une couche de sécurité supplémentaire en exigeant une deuxième preuve d'identité lors de la connexion.

Faire preuve de vigilance face aux messages suspects
Soyez attentif aux courriels, messages instantanés et appels téléphoniques non sollicités demandant des renseignements personnels. Ne cliquez pas sur des liens suspects et n'ouvrez pas de pièces jointes provenant de sources inconnues.

Mettre à jour régulièrement les logiciels
Maintenez vos systèmes d'exploitation, applications et logiciels antivirus à jour en installant les mises à jour et correctifs de sécurité. Une gestion proactive des mises à jour logicielles et matérielles réduit considérablement les risques de sécurité.

Limiter les renseignements personnels partagés en ligne
Évitez de publier des renseignements sensibles tels que votre adresse, votre numéro de téléphone ou vos informations financières sur les réseaux sociaux ou d'autres plateformes en ligne.

Utiliser des réseaux Wi-Fi sécurisés
Évitez d'utiliser des réseaux Wi-Fi publics pour effectuer des transactions sensibles ou accéder à des renseignements confidentiels. Privilégiez les réseaux protégés par mot de passe ou l'utilisation d'un VPN presque en tout temps.

Supprimer les cookies
Utilisez les outils de nettoyage du système d'exploitation pour supprimer les cookies de suivi et les données de navigation stockées sur vos appareils.

VPN (réseau privé virtuel)

Utilisez un VPN afin de chiffrer votre connexion Internet et de protéger votre vie privée en ligne. Des services comme NordLayer, ExpressVPN ou CyberGhost offrent des fonctionnalités de protection de la confidentialité.

Extensions de navigateur axées sur la confidentialité
Installez des extensions telles que Privacy Badger, uBlock Origin ou HTTPS Everywhere afin de bloquer les traceurs publicitaires, les publicités intrusives et de forcer les connexions sécurisées.

Chiffrement des communications
Utilisez des services de messagerie chiffrés comme Signal, WhatsApp (avec le chiffrement de bout en bout activé) ou Telegram (avec les discussions secrètes activées) pour protéger la confidentialité de vos échanges.

Prudence avec les paiements en ligne
Lors d'achats en ligne, assurez-vous d'utiliser des sites sécurisés et fiables. Vérifiez la présence d'un cadenas dans la barre d'adresse et privilégiez des moyens de paiement sécurisés comme PayPal ou des cartes de crédit protégées.

Chiffrement des fichiers
Utilisez des outils de chiffrement pour protéger vos fichiers sensibles. Des logiciels comme VeraCrypt, AxCrypt ou BitLocker permettent de chiffrer des fichiers individuels ou de créer des conteneurs chiffrés.

Navigation privée
Utilisez le mode de navigation privée ou incognito de votre navigateur afin de limiter la collecte de données et de cookies durant vos sessions. Ce mode empêche également l'enregistrement de l'historique de navigation.

Vérifier les paramètres de confidentialité
Examinez et ajustez les paramètres de confidentialité de vos comptes en ligne, notamment sur les réseaux sociaux, les services de messagerie et les applications, afin de limiter le partage de renseignements personnels et de restreindre l'accès à vos données.

Supprimer les données personnelles inutiles
Supprimez régulièrement les données personnelles inutiles ou sensibles stockées sur vos appareils, telles que les anciens courriels, fichiers temporaires, caches de navigation et historiques de recherche.

Sensibilisation à la cybersécurité
Familiarisez-vous avec les bonnes pratiques en cybersécurité en suivant des formations en ligne, en consultant des ressources fiables et en demeurant informé des menaces et techniques d'attaque émergentes.