S-103 CONFIDENTIALITÉ ET PROTECTION DE LA VIE PRIVÉE

Dans le but d'alléger le texte du présent document, le genre masculin est utilisé pour toute personne.

Version 6 approuvée le 16 janvier 2025 (auparavant DG-05)

Politique

Valoris s'engage à respecter les législations en matière de protection de la vie privée et de la confidentialité des informations, et prendre des mesures raisonnables pour protéger les renseignements personnels, dont nous avons la garde ou le contrôle, contre le vol, la perte et tout accès, utilisation, divulgation, duplication, modification ou élimination non autorisée.

L'organisation prend les mesures nécessaires pour protéger les renseignements personnels ou confidentiels dont elle est responsable.

Les employés sont responsables de respecter les consignes de protection des renseignements personnels pour minimiser le risque d'un bris de la confidentialité et d'atteinte à la vie privée.

Toute personne pouvant potentiellement accéder à de l'information personnelle ou confidentielle à Valoris est informée de ses responsabilités en termes de maintien de la confidentialité et la protection de la vie privée à son embauche. Chacun doit certifier avoir compris et s'engager à respecter les paramètres entourant les renseignements personnels et confidentiels avant de pouvoir être exposés à ceux-ci. Cet engagement moral et légal se poursuit à la fin de l'association avec l'agence; il a un caractère perpétuel.

Si une atteinte à la vie privée a lieu, des suivis et des corrections seront apportés pour réduire l'impact négatif de l'atteinte, ainsi que pour minimiser le risque que ceci ne se reproduise; tel qu'exigé par le Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP).

Procédure

1. **Respect de la confidentialité et de la vie privée**
   Le document ***Déclaration de respect de la confidentialité et de la protection de la vie privée*** doit être signé par toute personne pouvant avoir accès à des renseignements personnels en vertu de son association avec Valoris comme employé, bénévole, stagiaire ou consultant externe au début de son association avec Valoris.

2. **Avis aux clients**
   Sauf exception prévue à la loi, on obtient le consentement de toute personne à propos de laquelle on va recueillir des renseignements personnels avant de le faire. On informe la personne concernée de l'objet de la collecte ainsi que de l'utilisation prévue des

renseignements. L'employé doit aussi informer l'individu qu'il peut demander accès à ses renseignements personnels et qu'il peut demander que certaines corrections y soit faites.

L'employé doit aviser le client qu'il peut trouver plus d'informations au sujet de la collecte, l'utilisation et la divulgation de ses renseignements personnels sur le site web de Valoris ou celui du Commissaire à l'information et la protection de la vie privée au www.ipc.on.ca.

3. Comportements et attitudes professionnels

Tout employé, étudiant, bénévole ou stagiaire ayant accès à des informations personnelles ou confidentielles est tenu de respecter la confidentialité de tous, tel que prévu dans le code d'éthique. Un individu qui consulte un dossier client pour des raisons autres que dans le cadre de ses fonctions, commet une atteinte à la vie privée et s'expose à des sanctions disciplinaires pouvant aller jusqu'au congédiement, ou la fin de son association avec l'agence.

On ne doit pas mentionner d'information personnelle, confidentielle ou identificatoire dans les lieux publics ou dans toute autre circonstance où l'information pourrait être entendue ou interceptée par des personnes non autorisées. Des mesures doivent être prises pour prévenir le vol ou la perte de renseignements confidentiels en cours de transport ou d'entreposage. Par exemple, les documents physiques doivent être transportés et entreposés sous clé, alors que les documents électroniques doivent être protégés par de l'encryption, un mot de passe, une clé biométrique ou d'autres technologies approuvées.

Les personnes concernées doivent s'abstenir de mentionner des informations personnelles ou confidentielles dont Valoris est le gardien en présence de personnes non autorisées même si elles croient que la situation est connue des personnes non-autorisées ou du grand public.

Les informations personnelles entreposées sur des médias physiques doivent être entreposées de manière sécuritaire sous clé. Seules les personnes autorisées ont accès à ces locaux. Les mesures appropriées doivent être prises pour éviter l'accès par les personnes non-autorisées.

Les personnes autorisées ne consultent les dossiers (physiques ou électroniques) que lorsqu'elles en ont besoin pour exercer leurs fonctions; elles retournent les dossiers aux endroits désignés dans les plus brefs délais. Toute personne accédant à un dossier physique ou électronique est responsable d'en assurer la confidentialité (par exemple, en verrouillant son ordinateur lorsque l'employé n'est pas en train de s'en servir, ou en ne laissant jamais un dossier physique non verrouillé sans surveillance directe). Le personnel ne peut pas transporter des documents physiques comportant des renseignements personnels (incluant des agendas, cahiers de notes, formulaires, ou autres documents contenant des noms ou des informations personnelles, confidentielles ou identificatoires) à l'extérieur des centres de services à moins de le faire dans un contenant verrouillé (p. ex. dans les pochettes de transport verrouillables fournies par Valoris).

4. Approche multidisciplinaire (de service intégré)

En raison de notre modèle multiservice intégré, un même client peut nous fournir différents types d'informations personnelles régis par des lois différentes.

Par exemple, le service intégré d'un client peut exiger que nous travaillions avec lui en tant qu'organisation offrant des soins de santé et en tant que pourvoyeur de services liés à la protection de l'enfance. Dans un tel cas, certaines informations au(x) dossier(s) sont soumise(s) aux règles de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (mieux connue par son acronyme anglais PHIPA – *Personal Health Information Protection Act*) alors que d'autres informations sont protégées par la Partie X de la *Loi de 2017 sur les services à l'enfance, à la jeunesse et à la famille* (*LSEJF*).

Puisque Valoris offre plusieurs types de services, l'approche intégrée exige parfois le partage d'informations au sujet de clients par différents professionnels internes. Seules les informations pertinentes et nécessaires au but du partage seront divulguées. Le consentement du client à ce partage est nécessaire sauf dans certaines circonstances spécifiées dans les lois en vigueur.

Étant donné le risque d'un bris de la confidentialité, le courriel, les SMS (« textos ») et autres formes de communications instantanées ne doivent pas être utilisés pour communiquer avec ou à propos des clients de Valoris pour la prestation de services ni pour communiquer ou recevoir du client des renseignements personnels ou de santé. Ces méthodes de communication instantanées peuvent cependant être utilisées pour fixer, confirmer ou annuler des rendez-vous ou pour envoyer des informations générales à propos des services offerts à Valoris ou à l'externe.

La transmission d'informations personnelles ou confidentielles par moyens électroniques n'est permise qu'en utilisant les technologies approuvées par Valoris en raison de leur standard d'encryption et de sécurité rencontrant les normes nécessaires.

Des renseignements personnels peuvent être communiqués par courriel entre adresses de courriel internes uniquement, en raison de l'encryption, présente automatiquement sur tous les documents qui demeurent à l'intérieur de l'infrastructure informatique de l'agence.

Dans les circonstances où un client ne peut être joint que par ces médias de communication non confidentiels (courriel, SMS, snap chat, etc.), on informe le client du risque que présente l'usage de ces technologies pour la communication avec Valoris. Si le client consent à utiliser ces technologies malgré les risques, on documente le consentement du client au dossier. Le personnel de Valoris fait preuve de jugement dans l'utilisation de ces technologies de communication pour minimiser le risque d'atteinte à la vie privée de la clientèle.

Toute personne prend les précautions nécessaires pour assurer la confidentialité des informations affichées aux écrans de leurs appareils (ordinateurs, téléphones, etc.) : verrouillage de l'appareil lors d'absences (réunions, salle de bain, imprimante, etc.), utilisation de filtres de protection de la vie privée sur certains écrans, etc. Les documents acheminés par télécopieur sont identifiés « confidentiels ».

La destruction des documents de nature confidentielle est faite en respectant les lois applicables et notre calendrier de conservation (politique A-102 Gestion des documents et archives).

5. Responsable de l'information et la protection de la vie privée

Valoris nomme un membre de l'équipe de leadership comme responsable de l'information et de la protection de la vie privée (privacy officer). Cette personne joue le rôle de personne-ressource pour toutes les questions liées au bon usage de l'information personnelle dont Valoris est dépositaire selon les différentes lois en vigueur. Ses fonctions incluent :

a) Faciliter l'observation des lois sur la protection des renseignements personnels par Valoris (le dépositaire).
b) Veiller à ce que tous les employés mandataires soient adéquatement informés des obligations que leur imposent les lois sur la protection des renseignements personnels.
c) Répondre aux demandes de renseignements du public au sujet des pratiques relatives aux renseignements qu'a adoptées Valoris (le dépositaire).
d) Recevoir les plaintes du public par courriel au PVPO@valorispr.ca au sujet d'une contravention aux lois sur la protection des renseignements personnels qu'aurait commise Valoris (le dépositaire) et en aviser le bureau du Commissaire à l'information et à la protection de la vie privée, au besoin.

Le personnel peut rejoindre la personne responsable de l'information et de la protection de la vie privée à travers l'adresse de courriel vieprivee_privacy@valorispr.ca.

6. Atteinte à la vie privée

Des exemples de bris de confidentialité et d'atteintes à la vie privée sont :

1) *Vol de renseignements personnels* (ex. piratage d'un ordinateur donnant accès à ses fichiers);
2) *Perte de renseignements personnels* (ex. perte d'un formulaire identifiant un client);
3) *Utilisation non autorisée de renseignements personnels* (ex. utiliser sans consentement des données sur l'orientation sexuelle des clients ou employés pour les cibler directement avec de la publicité d'un groupe communautaire offrant des services aux communautés LGBTQ);
4) *Divulgation non autorisée de renseignements personnels* (ex. envoi d'un courriel à la mauvaise adresse).

Dès qu'une personne est mise au courant d'une atteinte potentielle à la vie privée, on enclenche la procédure suivante :

1. La personne à l'origine du bris potentiel, ou la première personne à le découvrir avise immédiatement son supérieur immédiat de la situation;
2. La personne à l'origine du bris potentiel, ou la première personne à le découvrir, ainsi que son superviseur immédiat avisent le responsable de l'information et de la protection de la vie privée en envoyant un courriel à (vieprivee_privacy@valorispr.ca)
3. La personne à l'origine du bris potentiel, ou une personne nommée par le superviseur immédiat prend les mesures nécessaires pour évaluer et maîtriser l'atteinte potentielle à la vie privée :

a. On détermine les renseignements personnels qui sont en cause
b. On prend des mesures correctives, par exemple :
    i. S'assurer que le destinataire qui n'était pas autorisé à recevoir des renseignements personnels ne les a pas conservés, et demander la confirmation qu'ils ont été détruits. S'il s'agit de documents physiques (lettres, dossier papier, etc.), on s'assure de les récupérer.
    ii. On s'assure que les renseignements qui ont été partagés par erreur ne donnent pas accès à d'autres renseignements (par exemple : s'il s'agissait de nom d'usager et mot de passe). Dans l'affirmative, on prend les étapes nécessaires pour fermer ces chemins d'accès vers d'autres données non-autorisées (par exemple en changeant les mots de passe, bloquant des accès, etc.)
    iii. Dans l'éventualité où l'information personnelle non-autorisée a été accédée volontairement par un employé, on considère s'il est nécessaire de suspendre ses droits d'accès.

4. La personne à l'origine de l'atteinte à la vie privée, ou une personne nommée par son superviseur immédiat avise les personnes concernées par l'atteinte à la vie privée dans les plus brefs délais. La notification doit être directe, c'est-à-dire par téléphone, lettre ou courriel, ou en personne. La notification indirecte est acceptable dans les situations où on ne peut raisonnablement recourir à la notification directe, lorsque les coordonnées des personnes concernées sont inconnues ou lorsque l'atteinte à la vie privée touche un grand nombre de personnes. L'avis aux personnes concernées doit :
    a. indiquer la portée de l'atteinte à la vie privée et décrire les renseignements personnels en cause;
    b. indiquer les mesures qui ont été ou seront prises pour rectifier la situation, tant dans l'immédiat qu'à long terme;
    c. fournir les coordonnées d'une personne de chez Valoris qui pourra fournir des renseignements et de l'aide supplémentaires et répondre aux questions;
    d. préciser que la personne a le droit de porter plainte au CIPVP et comment s'y prendre pour le faire.
5. Dans le cas où la situation est jugée grave selon les lignes directrices publiées par le Commissaire de l'information et la protection de la vie privée (CIPVP), la direction générale est informée de la situation tel que prévu à la politique A-203 *Situations à communiquer au directeur général.*
6. Selon le cas, le responsable de l'information et la protection de la vie privée avisera le CIPVP, l'assureur de Valoris ou les corps policiers.
    a. Les circonstances principales à rapporter au CIPVP sont les suivantes :
        i. Valoris détermine que l'atteinte est importante après avoir évalué la sensibilité, le volume, le nombre de personnes touchées ainsi que le nombre de fournisseurs de services impliqués.
        ii. Les renseignements personnels ont été utilisés ou divulgués à une personne qui savait ou aurait dû savoir qu'on le faisait sans autorisation.

iii. Valoris a des motifs raisonnables de croire que les renseignements personnels ont été volés.
iv. Valoris a des motifs raisonnables de croire que les renseignements personnels auxquels on a porté atteinte ont été ou seront vraisemblablement encore utilisés, divulgués sans autorisation ou on remarque une répétition d'atteintes similaires.
v. Un employé a démissionné ou a été congédié, suspendu ou sanctionné en raison de l'atteinte.

7. Selon le type de bris de la confidentialité, un incident grave sera complété et envoyé au ministère, tel que décrit dans les lignes directrices

7. Médias

L'agence s'engage à protéger la confidentialité des informations personnelles et confidentielles dans tous ses contacts avec les médias. Lorsqu'une personne fait des déclarations aux médias et dévoile sa relation avec l'agence, Valoris continuera de respecter notre engagement de confidentialité même dans une situation où l'information donnée par la personne est erronée.

Définition

***Renseignement personnel et confidentiel* :**

Tout renseignement que nous avons à propos d'un individu auquel nous offrons un service, ou qui pourrait ultimement mener à l'identification de l'individu à partir de ce renseignement. L'unique fait de confirmer ou infirmer que nous offrons des services à cet individu est aussi un renseignement personnel et confidentiel. Cette information peut être sous forme papier, électronique, audio digitale, photo, vidéo, etc. Des exemples de renseignements personnels sont :

- La race, l'origine nationale ou ethnique, la couleur, la religion, l'âge, le genre, l'orientation sexuelle ou l'état matrimonial ou l'état familial du particulier.
- Les antécédents médicaux, psychiatriques, psychologiques, criminels ou professionnels du particulier.
- Tout numéro, symbole ou autre détail identificatoire attribué au particulier (ex. carte santé ou permis de conduire).
- L'adresse, le numéro de téléphone, les empreintes digitales ou le groupe sanguin du particulier.
- Les lettres que nous avons reçues par le particulier qui est implicitement ou explicitement d'une nature privée ou confidentielle et les réponses à cette correspondance qui divulgueraient le contenu de la correspondance initiale.
- Les opinions ou points de vue personnels du particulier, sauf s'ils se rapportent à une autre personne.
- Les points de vue ou les opinions d'une autre personne au sujet du particulier.
- Le nom du particulier lorsqu'il figure parmi d'autres renseignements personnels qui le concernent ou lorsque la divulgation du nom révélerait d'autres renseignements personnels à son sujet.

Annexe

- Formulaire Respect de la confidentialité et protection de la vie privée.

Références

- *Loi de 2004 sur la protection des renseignements personnels sur la santé*
- *Loi de 2017 sur les services à l'enfance, à la jeunesse et à la famille (LSEJF), partie X*
- *Loi de 2002 sur le système de justice pénale pour les adolescents*
- *Loi de 2008 sur les services et soutiens favorisant l'inclusion sociale des personnes ayant une déficience intellectuelle*
- *S-102 Accès aux renseignements personnels des particuliers et rectifications*
- *S-104 Collecte, utilisation et divulgation des renseignements personnels et le consentement*
- *S-105 Plaintes de la clientèle*
- *A-101 Les communications*
- *A-102 Gestion des documents et archives*
- *RH-116 Sanctions disciplinaires*
- *A-301 Gestion et utilisation de la technologie et des systèmes*