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 5 approuvée le 19 février 2020 (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 au sujet de la clientèle, et prendre des mesures raisonnables pour protéger les renseignements personnels, dont nous avons la garde ou le contrôle, contre le vol, la perte et toute utilisation, divulgation, duplication, modification ou élimination non autorisée.

L'organisation s'assure de gérer une partie du risque lié à la protection des renseignements personnels qui se trouvent pour la plupart dans des bases de données web par le biais d'une infrastructure technologique sécuritaire et assure des vérifications régulières pour en garantir la sécurité.

Les employés qui utilisent les outils technologiques et qui offrent des services autant dans des lieux publics que les bureaux de Valoris sont responsables de respecter les consignes de protection des renseignements personnels et ainsi 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 confidentielle et des renseignements personnels à Valoris est informée de ses responsabilités en termes de maintien de la confidentialité et la protection de la vie privée à son embauche. Chacune doit certifier avoir compris et s'engager à respecter les paramètres entourant les renseignements personnels et confidentiels avant de pouvoir être exposée à ceux-ci. Son engagement moral et légal ne cesse pas 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 le risque que ceci ne se reproduise pas tel qu'exigé par le Commissaire à l'information et la protection de la vie privée (CIPVP).

Procédure

1. **Respect de la confidentialité et de la vie privée**
   Le document ***Respect de la confidentialité et 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

L'employé doit aviser le client qu'il va collecter, utiliser et même parfois divulguer ses renseignements personnels avec ou sans son consentement si une loi l'autorise; autrement, ses renseignements personnels resteront confidentiels. L'employé doit aussi informer le client 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 ou stagiaire ayant accès à la base de données client 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 un bris de la confidentialité et s'expose à des sanctions disciplinaires pouvant aller jusqu'au congédiement, ou la fin de son association avec l'agence.

Toutes les personnes concernées doivent s'abstenir d'identifier une personne ou de discuter de faits qui pourraient l'identifier dans des lieux publics (de l'agence ou extérieurs) ou par des moyens accessibles à tous tels que restaurants, salle d'attente, cafétéria, interphone. Elles doivent prendre toutes les mesures pour prévenir le vol ou la perte de renseignements confidentiels en cours de transport ou à domicile : notes d'intervention, ordinateurs portables, agendas, dossiers. De plus, leurs conversations au téléphone cellulaire ne doivent jamais mentionner d'information pouvant mener à l'identification d'une personne.

Les personnes concernées doivent s'abstenir de faire des commentaires en public même si elles croient que la situation d'un client a été commentée dans les médias et est connue du public.

Dans chaque centre de services, les dossiers physiques de la clientèle doivent être entreposés dans un local à l'épreuve du feu et de l'eau. Celui-ci doit être verrouillé après les heures d'ouverture du bureau. Seules les personnes autorisées ont accès à ces locaux.

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 à l'extérieur des centres de services à moins de le faire dans un contenant verrouillé.

4. Approche multidisciplinaire (de service intégré)

En raison de notre modèle multiservice intégré, un même dossier de client peut contenir 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 notre agence regroupe 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 est souhaitable, quoique non nécessaire 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 communication instantanées ne doivent pas être utilisées 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 des renseignements de santé personnels. 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.

Des renseignements personnels peuvent être communiqués par courriel entre adresses de courriel internes seulement.

Dans les circonstances où un client ne peut être joint que par ces médias de communication non confidentiels (courriel, SMS, 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.

Le personnel prend les précautions nécessaires pour assurer la confidentialité des informations affichées à l'écran de l'ordinateur : déconnexion du réseau lors d'absences (réunions, salle de bain, imprimante, etc.), utilisation d'un économiseur d'écran avec mot de passe. Les documents acheminés par télécopieur sont identifiés « confidentiels ».

Les dossiers d'enfants ayant reçu des services de santé mentale ou autres, maintenant devenus adultes, ne doivent pas être consultés lors de situations de protection à l'enfance, sans leur consentement.

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 le directeur de la qualité et des systèmes d'information comme 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) Acheminer vers l'équipe légale les demandes de particuliers qui désirent avoir accès aux dossiers de renseignements personnels sur la santé les concernant, et dont le dépositaire a la garde ou le contrôle, ou les faire rectifier.
e) 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.

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. parler d'un dossier dans une aire ouverte et publique);
4) *Divulgation non autorisée de renseignements personnels* (ex. envoi d'un courriel à la mauvaise adresse).

Dès qu'un employé est mis au courant d'une atteinte potentielle à la vie privée, un avis initial est donné au supérieur immédiat et un courriel est acheminé à PVPO@valorispr.ca l'informant de la situation. Le supérieur ou l'employé doit noter l'atteinte à la vie privée au dossier. Toutes ces actions doivent avoir lieu dès que possible, mais pas plus tard que 24 heures suivant la connaissance de l'atteinte à la vie privée.

Le superviseur avise le directeur de service qui informe le directeur général de la situation tel que prévu à la politique A-203 *Situations à communiquer au directeur général.* Selon le cas, le responsable de l'information et la protection de la vie privée avisera le Commissaire de l'information et la protection de la vie privée, l'assureur de Valoris et le corps policier. Selon le bris de la confidentialité, un incident grave sera complété et envoyé au ministère, tel que décrit dans les lignes directrices.

Il est à noter que si l'atteinte à la vie privée est accidentelle et occasionnelle, par exemple, envoyer des renseignements par erreur au mauvais destinataire, l'employé, en consultation avec son supérieur, informera par courriel le responsable de la protection de la vie privée au PIPV@valorispr.ca et avisera dès que possible les personnes visées par le bris de la confidentialité et expliquera les mesures prises pour corriger la situation. L'employé notera le tout au dossier du client. Il n'est pas nécessaire de signaler ceci au

CIPVP à moins que cette atteinte nous laisse croire que l'information a été utilisée ou copiée sans permission.

Les circonstances principales à rapporter au CIPVP sont les suivantes :

1) 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.
2) Les renseignements personnels ont été utilisés ou divulgués à une personne qui savait ou aurait dû savoir qu'on le faisait sans autorisation.
3) Valoris a des motifs raisonnables de croire que les renseignements personnels ont été volés.
4) 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.
5) Un employé a démissionné ou a été congédié, suspendu ou sanctionné en raison de l'atteinte.

Au 5e jour ouvrable, suivant l'avis initial, le supérieur ou l'employé doivent remettre les informations suivantes à PVPO@valorispr.ca :

1) La nature de l'atteinte à la vie privée (renseignement volé, perdu ou utilisé ou divulgué sans autorisation).
2) Les circonstances (comment les renseignements personnels ont été volés, perdus, utilisés sans autorisation ou divulgués sans autorisation et la date que ceci a eu lieu).
3) Combien de particuliers sont visés et comment et quand l'atteinte à la vie privée a été découverte.
4) Les mesures prises pour maitriser la situation (par exemple, les mesures prises pour récupérer les renseignements personnels) et la correction prévue.

Dans les 7 jours ouvrables, suivant l'avis initial, le responsable de l'information et la protection de la vie privée enverra une lettre pour aviser les personnes visées de la situation et de leur droit de porter plainte au Commissaire de l'information et la protection de la vie privée.

Si jugé nécessaire ou utile, le responsable de l'information et la protection de la vie privée fera une enquête interne afin de déterminer comment cette atteinte à la vie privée pourrait être évitée à l'avenir. Il émettra ensuite des recommandations face à des changements de procédures.

7. Médias publics

L'agence s'engage à protéger la confidentialité des informations relatives à la clientèle dans tous ses contacts avec les médias publics. Lorsqu'un client fait des déclarations aux médias et dévoile sa relation avec l'agence, nous continuons à respecter notre engagement de confidentialité même dans une situation où l'information donnée par le client 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 rectification
- 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 Autorisation et utilisation des systèmes informatiques et des sources de données de Valoris