Politique sur la vie privée, la confidentialité, la protection de l'information et protocole en cas d'atteinte à la vie privée

Politique

Agilec respecte la confidentialité de ses clients et de ses employés. Nous sommes engagés à traiter tous vos renseignements personnels conformément à la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) et les dix principes de la confidentialité.

Nous appliquons cette politique en observant nos pratiques de confidentialité.

Responsabilité

Agilec a nommé un agent de la protection de la vie privée qui est responsable d'établir et de mettre en œuvre notre politique et nos pratiques de confidentialité.

> **Agent de la protection de la vie privée :**
> Brian Martin
> 905 443 1001, poste 2300
> bmartin@agilec.ca

Les responsabilités entières de l'agent de la protection de la vie privée sont expliquées ci-dessous dans la section sur l'imputabilité de nos pratiques de confidentialité.

L'agent de la protection de la vie privée est appuyé par une équipe de protection de la vie privée composée de chaque chef d'équipe d'Agilec. L'équipe de protection de la vie privée est responsable de prodiguer la formation sur la confidentialité à l'équipe locale, à superviser l'application locale des pratiques de confidentialité d'Agilec et de s'assurer que les problèmes de confidentialité qui surviennent au niveau local sont communiqués à l'agent de la protection de la vie privée.

Chaque employé d'Agilec est responsable de l'application uniforme de nos pratiques de confidentialité. Les employés adhèrent aussi au Code d'éthique de

l'Association canadienne de réadaptation professionnelle, qui contient des principes pour le traitement éthique des renseignements personnels des clients.

Pratiques de confidentialité

Introduction
Nous comprenons l'importance de protéger les renseignements personnels que nous recueillons de nos clients. Nous sommes engagés à recueillir, utiliser, divulguer et conserver les renseignements personnels d'une manière responsable. Nous nous efforçons d'être aussi ouverts et transparents que possible à propos de la manière dont nous traitons les renseignements personnels. Afin d'assurer l'exhaustivité de nos pratiques de confidentialité, nous les avons organisées en fonction des dix principes de la confidentialité.

Principe 1 : Imputabilité
Agilec comprend et accepte sa responsabilité pour les renseignements personnels qu'elle recueille directement ou qu'elle reçoit d'autres sources dans le cadre de ses activités d'affaires.

Un agent de la protection de la vie privée a été nommé par Agilec pour superviser notre approche en matière de confidentialité et pour assurer la conformité à la LPRPDE et à nos pratiques de confidentialité. Cela comprend :

- Le suivi des données concernant nos pratiques de confidentialité, comme le nombre de demandes, de plaintes, d'infractions, etc.
- L'évaluation de l'efficacité de notre système, ainsi que de l'efficacité des améliorations apportées au système.
- La révision des pratiques de confidentialité d'Agilec et l'assurance qu'elles sont actualisées en fonction des changements applicables de la loi et du milieu (incluant la technologie de l'information).

Vous trouverez dans notre cadre sur la conformité en matière de confidentialité les détails sur la manière dont nous surveillons notre adhérence aux lois et à nos pratiques sur la protection de la vie privée.

Agilec reconnaît que sa responsabilité en matière de confidentialité comprend les renseignements personnels qui ont été transférés à une tierce partie. Nous utilisons des moyens contractuels et autres afin d'assurer un niveau comparable de protection des renseignements accessibles et/ou traités par des tiers.

Principe 2 : Identification des motifs pour la collecte de renseignements

Avant de recueillir des renseignements personnels, Agilec expliquera toujours clairement à tous pour quelle raison nous le faisons.

Afin de satisfaire à ce principe :

- Nous nous assurerons que les employés qui recueillent des renseignements personnels sont capables de clairement expliquer pour quelle raison ils le font et la manière dont l'information sera utilisée.
- Les formulaires que nous utilisons pour recueillir des renseignements personnels comprendront une description des buts de la collecte.
- Afin d'éviter de recueillir des renseignements dont nous n'avons pas besoin, nous nous efforcerons d'être aussi exacts que possible quant à nos buts pour chaque élément d'information recueilli.
- Si nous savons que des renseignements personnels seront partagés avec d'autres à l'extérieur d'Agilec, nous l'expliquerons au moment de la collecte.
- Nous n'utiliserons pas les renseignements recueillis à de nouvelles fins qui n'ont pas été expliquées aux clients à moins d'obtenir leur consentement pour ces nouvelles fins.

Principe 3 : Consentement

Agilec obtient le consentement informé pour la collecte, l'utilisation et la divulgation de renseignements personnels, sauf s'il serait inapproprié de demander le consentement et sous réserve de certaines exceptions stipulées dans la loi.

Ce principe exige que nous expliquions nos buts pour l'information (en respectant le Principe 2) et que nous soyons certains que la personne comprend. Afin de faciliter la compréhension, nos explications utiliseront un langage simple et concis.

Le consentement peut être donné de plusieurs manières. En général, nous appliquons les lignes directrices ci-dessous afin d'augmenter la rigueur du consentement à mesure que la sensibilité, l'ampleur et la complexité de l'utilisation des renseignements augmentent.

- Le consentement lié aux renseignements personnels les plus simples (p. ex., nom et coordonnées qui ne sont pas partagés avec d'autres hors d'Agilec) peut être obtenu verbalement et n'a pas besoin d'être documenté.
- Le consentement concernant des renseignements personnels plus détaillés qui seront utilisés exclusivement à l'interne par Agilec peut être obtenu verbalement. Il faut noter au dossier du cas que le consentement informé verbal a été donné.
- Le consentement concernant des renseignements personnels qui seront partagés avec des tiers (y compris des agences de recommandation)

doit être obtenu par écrit, habituellement au moyen d'une signature sur un formulaire de consentement.

Le consentement doit être renouvelé si les détails du but ou de la divulgation devaient changer.

Une personne peut retirer son consentement en tout temps. Dans ces cas, nous avisons la personne des implications possibles du retrait du consentement.

Principe 4 : Limite de la collecte de renseignements personnels
Agilec ne recueille que les renseignements qui sont nécessaires aux fins indiquées et communiquées au moment de la collecte

Cela signifie :

- Que nous exposons clairement nos buts avant de recueillir des renseignements (voir Principe 2).
- Que nos formulaires pour l'obtention des renseignements sont conçus de manière à ne recueillir que les renseignements nécessaires.
- Que nous n'enregistrons ou ne documentons aucun renseignement personnel non essentiel qui est présenté lors des conversations avec les clients.

Dans la pratique : Nous devons être prudents de ne pas recueillir d'information basée sur des suppositions par rapport au déboucher éventuel des services. Par exemple, nous ne devrions pas demander le NAS d'un candidat avant d'avoir établi si cette personne utilisera des services où le NAS est requis.

Principe 5 : Limite de l'utilisation, de la divulgation et de la rétention
Agilec n'utilisera ou ne divulguera pas des renseignements personnels à d'autres fins que celles pour lesquelles l'information a été recueillie, sauf avec le consentement exprès ou en conformité avec la loi.

Utilisation :

Si nous prévoyons utiliser des renseignements personnels à une fin différente de celle exprimée au moment de la collecte, nous devons d'abord obtenir et documenter le consentement à cette nouvelle fin.

Divulgation des renseignements :

Au sein d'Agilec

Au moment de la collecte, nous avisons les clients que leurs renseignements personnels peuvent être partagés avec d'autres employés d'Agilec qui jouent un rôle dans la réalisation des fins identifiées. Cela permet aux chefs d'équipes, au service financier, aux pairs (pour des conférences sur des cas ou le remplacement lors de congés, par exemple) et à d'autres d'y accéder si c'est nécessaire pour accomplir leurs tâches. Cependant, les renseignements personnels ne seront pas partagés ou rendus accessibles à des employés d'Agilec qui ne sont pas concernés par le cas du client.

À l'extérieur d'Agilec
Nous ne divulguerons aucun renseignement personnel à quiconque à l'extérieur d'Agilec à moins que la personne ou l'organisme recevant cette information soient spécialement autorisés par le consentement par écrit du client. Cela comprend des membres de la famille ou d'autres agissant au nom d'une personne.

Cette pratique s'applique aux formes de divulgation écrites, électroniques et verbales.

Exceptions aux exigences relatives au consentement
La LPRPDE contient certaines exceptions concernant l'obligation d'obtenir le consentement avant la divulgation. Des situations justifiant ces exceptions ne se produisent que rarement. Celles qui sont les plus probables de survenir auprès d'Agilec sont :

- lorsque nous sommes obligés de nous conformer à un mandat, l'ordonnance d'un tribunal, d'une assignation à témoigner ou à la loi;
- lorsqu'un organisme gouvernemental (p. ex., la police) demande les renseignements afin de pouvoir appliquer la loi. (Remarque : dans de tels cas, nous exigeons de la police de d'abord obtenir un mandat avant de divulguer les renseignements demandés);
- lorsque nous avons des motifs raisonnables de croire que les renseignements se rapportent à une activité illégale et nous pouvons alors les communiquer aux autorités sans attendre qu'elles nous les demandent;
- dans une situation d'urgence qui menace la vie, la santé ou la sécurité d'une personne.

Dans la pratique : Si une de ces situations se produit, au moins deux dirigeants d'Agilec doivent participer au processus décisionnel. L'agent de la protection de la vie privée est consulté. Si l'agent de la protection de la vie privée ne peut pas participer à la prise de décision, les dirigeants concernés sont responsables

de l'aviser de la situation et des mesures prises le plus tôt possible après la décision.

Rétention et destruction :

Rétention de renseignements personnels
Agilec conserve des dossiers contenant des renseignements personnels seulement aussi longtemps qu'ils sont nécessaires pour la prestation de service ou des raisons contractuelles, ou comme requis en vertu de la loi. Cette pratique s'applique aux dossiers électroniques et papier.

Dans la pratique : La direction de chaque projet d'Agilec détermine la durée de rétention de renseignements personnels après la fin de la prestation de services (période de rétention). Les besoins du service des finances doivent entrer en considération dans la décision. La période de rétention du projet est communiquée à l'agent de la protection de la vie privée qui veille à l'alignement avec nos pratiques de confidentialité et la loi, et qui surveille la conformité.

Destruction de renseignements personnels
Tous les dossiers d'Agilec (papier et électroniques) contenant des renseignements personnels doivent être détruits dans l'année suivant la fin de la période de rétention.

Agilec a rédigé un guide pour assurer la destruction sécuritaire des renseignements papier et électroniques.

Dans la pratique : La direction de chaque projet d'Agilec doit s'assurer, au moins une fois par année, que tous les dossiers contenant des renseignements personnels qui ont dépassé la période de rétention sont détruits en utilisant des méthodes de destruction sécuritaires décrites dans le guide.

Principe 6 : Exactitude des renseignements personnels
Agilec prend des mesures afin de garantir que les renseignements personnels des clients sont exacts, complets et aussi actualisés que nécessaire aux fins pour lesquelles ils seront utilisés. Notre intention est d'éliminer l'utilisation de renseignements inexacts lorsque nous faisons des recommandations ou des décisions en matière de service.

Dans la pratique : Lors de réunions avec des clients, les employés demanderont si des renseignements personnels ont changé et feront les mises à jour correspondantes.

Principe 7 : Mesures de protection des renseignements personnels
Agilec prendra des mesures adéquates pour protéger les renseignements personnels de l'accès, de la divulgation, de l'utilisation ou de la modification non autorisés. Les mesures de protection devront être adéquates pour la sensibilité des renseignements à protéger.

Nous avons établi un ensemble de méthodes organisationnelles, physiques et technologiques de protection des renseignements personnels. Il incombe à chaque employé d'Agilec de se familiariser avec ces méthodes et de garantir que les renseignements personnels des clients sont protégés en tout temps, qu'ils soient enregistrés sur papier ou électroniquement.

Mesures de protection organisationnelles

- Les employés d'Agilec, les étudiants et les fournisseurs de service de tierce partie doivent signer des ententes de confidentialité les liant à protéger les renseignements personnels auxquels ils ont accès.
- Les nouveaux employés reçoivent une formation sur les pratiques de confidentialité d'Agilec dans le cadre du processus d'intégration.
- Chaque année, tous les employés suivent une formation de recyclage sur la confidentialité.
- Des inspections ou des vérifications de la confidentialité sont effectuées tous les trimestres sous la direction de l'agent de la protection de la vie privée.
- L'agent de la protection de la vie privée effectue une révision annuelle du programme de confidentialité d'Agilec. Cette approche peut inclure :
    - l'évaluation et la mise à jour de la politique et des pratiques de confidentialité;
    - la revue de notre expérience de l'année précédente (incluant les plaintes et les infractions en matière de confidentialité);
    - la comparaison avec les pratiques exemplaires à l'intérieur et à l'extérieur d'Agilec;
    - l'évaluation par rapport aux changements de la loi ou des exigences des clients;
    - la rétroaction des équipes de prestation de services; et/ou
    - l'évaluation de la confirmation interne et/ou des connaissances des employés.

Mesures de protection physiques

- Les documents envoyés à une imprimante partagée ne doivent pas être laissés à la vue de personnes non autorisées.

Dans la pratique : Les choix comprennent :
  - la cueillette des documents dès l'impression;
  - l'envoi de documents à imprimer à une boîte de réception sécurisée afin de les imprimer lorsque l'employé autorisé entre son code personnel dans l'imprimante;
  - demander à une personne autorisée d'attendre l'impression du document à l'imprimante afin de les récupérer immédiatement.

- Chaque employé doit s'assurer qu'aucun document n'est laissé à la vue de personnes non autorisées.
- Les classeurs contenant des renseignements personnels doivent être dans des endroits inaccessibles au public ou gardés sous clé. Tous les classeurs doivent être verrouillés lorsque l'occupant quitte le bureau.
- Agilec fournit des télécopieurs distincts pour l'usage par le public et les clients et par le personnel. Les télécopieurs utilisés par les employés doivent être à des endroits non accessibles au public. Les télécopies entrantes doivent être récupérées et remises aux destinataires sur une base régulière.
- Chaque établissement d'Agilec est doté de portes verrouillables et d'équipement de sécurité électronique installés à toutes les entrées. Seuls des employés d'Agilec et des tiers autorisés ont des clés et des codes d'accès. Les clés sont suivies et reprises des employés ou tiers qui n'en ont plus besoin et les codes de sécurité sont changés au même moment.
- Chaque zone où des renseignements personnels sont stockés est sécurisée par une porte et/ou des armoires verrouillées. Une clé est remise à une personne désignée responsable de la sécurité de cette zone. Un double de la clé existe et elle est sécurisée par le chef d'équipe local ou son substitut.

Dans la pratique : Nous rappelons aux candidats de protéger leurs renseignements lorsqu'ils utilisent nos ressources (par exemple, en publiant des instructions pour l'enregistrement de fichiers dans nos ordinateurs et en leur demandant de récupérer leurs documents à l'imprimante sans tarder).

Mesures de protection technologiques

Ordinateurs :

- Agilec maintient un réseau privé virtuel sécurisé.
- D'autres mesures de sécurité informatique, incluant :
  - mots de passe,
  - verrouillage d'écran,
  - enregistrement et accès à l'information,
  - sécurité des portables et autres appareils informatiques,

- téléphones intelligents,

sont expliquées dans la section *Sécurité de la technologie et de l'information* des Pratiques technologiques d'Agilec.

Mesures de protection de la transmission

Les employés d'Agilec ont à leur disposition plusieurs options pour le transfert de renseignements personnels à d'autres. Chaque méthode comporte ses propres considérations en matière de confidentialité.

Portail des clients :

- Dans certains cas, Agilec fournit un portail Web pour l'échange bidirectionnel sécurisé d'information protégée par SSL entre Agilec et les secondes ou tierces parties.

Courriel interne :

- À l'interne, le RPV d'Agilec et son serveur sécurisé garantissent que tous les courriels et leurs pièces jointes envoyés entre des adresses de courriel d'Agilec sont sécurisés.

Courriel externe :

- Tout courriel envoyé à une adresse hors d'Agilec doit être considéré comme étant **non sécurisé**, parce que le contenu du courriel et toute pièce jointe peuvent être vus en cours de route par les réseaux parcourus.
- Chez Agilec, nous reconnaissons :
  - que les renseignements personnels ne présentent pas tous le même niveau de sensibilité;
  - que la plupart des membres du public sont à l'aise avec l'utilisation du courriel pour l'envoi de renseignements personnels non sensibles;
  - que le courriel est souvent la méthode la plus efficace d'échanger de l'information en temps opportun entre des parties.

  Par conséquent, les pratiques de confidentialité d'Agilec permettent l'envoi par courriel de *renseignements personnels non sensibles* à l'externe, sous réserve des conditions suivantes :

  Exigences :

  1. Chaque candidat lit ou se fait expliquer les pratiques d'Agilec en matière de courriel établies dans le document Protection de votre vie privée.
  2. L'accord ou le désaccord du candidat concernant nos pratiques de courriel relativement à ses renseignements personnels est obtenu et consigné dans le CTS.
  3. La sensibilité des renseignements personnels envoyés par courriel est faible, conformément au tableau ci-dessous :

Envoi par courriel permis [1]	**Envoi par courriel interdit** [2]

Curriculum vitæ abrégé	Renseignements médicaux
Lettres de présentation	Rapports (progrès, évaluation, etc.)
Calendriers	Demandes pour des programmes (p. ex., SC, OSEB)
Rendez-vous	Noms combinés à d'autres numéros d'identification
Relevés de paie/revenus (si aucun NAS inclus)	NAS
Recommandations (si la sensibilité de l'information n'est pas supérieure à celle d'un CV)	Recommandations (si elles contiennent de l'information plus sensible que celle d'un CV, p. ex., invalidité)
Renseignements scolaires (avec nom ou numéro d'identification seulement, pas les deux)	TIPA
Plans d'action de SRP	Dossier de conduite
Offres d'emploi/coordonnées d'employeur	Vérification des antécédents criminels
Questionnaires de satisfaction et réponses	

[1]Protection par mot de passe non requise [2]Voir la protection par mot de passe ci-dessous

[3]Ces listes ne sont pas exhaustives. Utilisez ce contenu comme guide pour évaluer d'autres types de renseignements personnels avant de les envoyer par courriel.

Dans la pratique : En tant que protection contre les infractions qui se produisent lorsqu'un message est accidentellement envoyé à au moins une mauvaise adresse, il est préférable d'éviter, dans la mesure du possible, d'inclure des renseignements personnellement identifiables dans un courriel (y compris les courriels internes). Par exemple, des personnes peuvent être référencées en utilisant un numéro ou un code interne d'Agilec qui n'aurait aucune signification pour quiconque de l'extérieur.

- Protection par mot de passe : Cette approche offre une protection limitée et peu fiable contre l'accès malveillant à des renseignements personnels. Par conséquent, elle ne fait plus partie des pratiques de courriel normalisées d'Agilec. Cependant, dans des cas exceptionnels où le courriel est la seule méthode disponible pour transmettre des renseignements personnels (voir la liste des *envois par courriel interdits* ci-dessus), l'information peut être envoyée sous forme d'une pièce jointe protégée par mot de passe dans un courriel non sécurisé. Aucun renseignement personnel identifiable ne doit figurer dans le titre ou le corps du courriel lui-même. Il ne faut jamais faire d'exceptions pour des renseignements hautement sensibles. Protection par mot de passe d'un Document ou d'un PDF.

Dans la pratique : La protection par mot de passe est une barrière pour les renifleurs humains et automatisés qui peuvent balayer les courriels et les pièces jointes pour des types de contenu particuliers. Les mots de passe créent une enveloppe qui doit être ouverte afin d'exposer et de renifler le

document. Toutefois, des logiciels de cassage de mot de passe sont capables de pénétrer la plupart des mots de passe.

Si la protection par mot de passe n'est pas disponible, l'impression et le scannage d'un document au format PDF transforme le contenu textuel en une image qui ne peut pas être reniflée (bien qu'elle puisse encore être lue par un humain).

- Lorsque les exigences du client en matière de confidentialité divergent de ces pratiques, les plus restrictives des deux doivent être observées.

Livraison en personne par le client :

- Un client d'Agilec peut livrer, obtenir ou retourner en personne des documents contenant ses propres renseignements personnels. Bien que cela puisse protéger Agilec de la responsabilité entière si l'information est égarée, Agilec pourrait quand même être jugée comme participante à l'infraction. La fiabilité du client, la sensibilité au temps et la nature des renseignements personnels doivent toutes être considérées avant de choisir cette option.

Dans la pratique : Cette approche peut être efficace lorsque l'on tente d'obtenir de l'information de médecins.

Messagerie :

- Généralement sécurisé (l'envoi est scellé et peut être suivi).
- La livraison est offerte dans des délais garantis.
- Cela peut ne pas être pratique et comporter des frais excessifs.
- Utilisez des étiquettes d'adresse et de retour préimprimées afin de réduire le risque de livraison à la mauvaise adresse.

Poste expresse

- Similaire à la messagerie.
- La signature à la réception peut être demandée contre des frais supplémentaires afin d'améliorer le suivi, mais cela peut causer des retards dans la livraison et des inconvénients pour le destinataire.

Poste ordinaire :

- Peut être utilisée pour livrer des renseignements non sensibles au client.
- N'utilisez pas la poste ordinaire pour livrer des documents contenant des renseignements médicaux, d'invalidité, financiers ou personnels confidentiels comme le numéro d'assurance sociale (NAS).
- Utilisez des étiquettes d'adresse et de retour préimprimées afin de réduire le risque de livraison à la mauvaise adresse.

Livraison en personne par des employés d'Agilec :

- Déconseillée.
- Exige un soin et une diligence accrus de la part de l'employé.
- Limitez les étapes en cours de route.
- Les employés doivent garder les renseignements dans une mallette verrouillée qui les accompagne ou qui est rangée dans le coffre de la voiture en tout temps.

Dans la pratique : Les employés d'Agilec sur le terrain doivent apporter le minimum d'information ou de dossiers requis pour la journée afin de réduire le risque d'accès ou d'exposition non autorisés.

Télécopie :

- Cette méthode comporte des risques inhérents : l'envoi au mauvais destinataire; la réception de télécopies n'est pas sécurisée.
- Utilisez des numéros de télécopie préprogrammés dans le télécopieur afin de réduire le risque de composer le mauvais numéro.
- Appelez avant l'envoi afin de confirmer qu'un destinataire autorisé est avisé de l'arrivée de la télécopie.
- Arranger la confirmation de la réception de la télécopie par le destinataire autorisé.

Téléphone :

- Prenez des mesures pour vous satisfaire que la personne à qui vous vous adressez est couverte par le consentement de divulgation du client.

Recommandations externes :

- Utilisez les formulaires de recommandation normalisés d'Agilec afin de limiter les renseignements personnels du client que nous partageons à ce qui est considéré comme nécessaire pour les services recommandés.

Principe 8 : Ouverture en matière de confidentialité

Agilec rend l'information concernant ses pratiques de confidentialité facilement accessible à ses clients de diverses manières, dont :

- la publication d'un résumé de notre politique et de nos pratiques et des coordonnées des agents de la protection de la vie privée à tous ses établissements;
- l'utilisation de formulaires de consentement du client qui expliquent les raisons pour lesquelles Agilec recueille, utilise et divulgue des renseignements personnels;
- la publication de la Politique et des pratiques de confidentialité d'Agilec sur son site Web et sur demande.

Principe 9 : Accès par le client à ses renseignements personnels
Sur demande par écrit dans un délai raisonnable, Agilec avisera un client de l'existence de tout renseignement personnel le concernant en notre possession et lui donnera accès à ces renseignements.

Sur demande, Agilec fournira aussi un compte-rendu de la manière dont les renseignements personnels du client ont été utilisés, y compris la divulgation à des tiers. En fournissant cette information, nous tenterons d'être aussi spécifiques que possible.

Nous répondrons aux demandes d'accès dans un délai raisonnable contre des frais modiques au client, le cas échéant. Les renseignements demandés seront rendus disponibles dans un format généralement jugé compréhensible.

Le client est libre de contester l'exactitude et l'exhaustivité de ses renseignements et de les faire modifier, amender ou changer.

> **Dans la pratique :** D'autres détails sur la manière de répondre aux demandes de renseignements personnels sont contenus dans nos Directives d'accès au dossier.

Principe 10 : Contestation de la conformité
Un client ou un employé peut contester notre conformité à ces principes en utilisant le Processus de plainte formelle d'Agilec. L'information concernant le processus de plainte est disponible sur le site d'Agilec et à tout établissement d'Agilec. Les employés d'Agilec aideront ceux qui souhaitent soulever des questions de confidentialité à accéder au processus de plainte.

Toutes les plaintes formelles liées à la confidentialité doivent être adressées à l'agent de la protection de la vie privée d'Agilec qui informera également le plaignant des autres recours qui s'offrent à lui, comme contacter les commissaires à la protection de la vie privée de l'Ontario ou du Canada. S'il est établi qu'une plainte est justifiée, l'agent de la protection de la vie privée prendra les mesures adéquates, y compris, si nécessaire, la modification des pratiques d'Agilec.

Approche d'AQ en matière de confidentialité

Des inspections ou des vérifications internes trimestrielles de notre conformité à la politique et aux pratiques de confidentialité d'Agilec sont effectuées sous la direction du vice-président, assurance qualité.

Outre l'évaluation continue de la conformité, l'agent de la protection de la vie privée mène une révision annuelle du système et produit un rapport afin d'assurer l'efficacité et l'amélioration continues du système de confidentialité.

D'autres détails se trouvent dans notre Cadre de conformité à la confidentialité.