

Considérations liées à la protection de la vie privée concernant l'outil GRIG-PE



Remarque : cette présentation est destinée aux fournisseurs de service qui signalent des incidents graves auprès du ministère des Services à l'enfance et des Services sociaux et communautaires (MSESSC). Elle ne remplace pas un avis juridique. Si vous avez des questions à propos de vos obligations en matière de protection de la vie privée, veuillez communiquer avec un conseiller juridique.

Bienvenue à la formation sur l'outil GRIG-PE

Module 2



- Cette présentation fait partie de la formation globale qui vise à faciliter la mise en œuvre et la gestion continue des exigences relatives aux signalements d'incidents graves au moyen de l'outil GRIG-PE.
- Cette formation est divisée en quatre modules :
 - Module 1** Lignes directrices du SIG du MSESC
 - Module 2** Considérations liées à la protection de la vie privée
 - Module 3** Marche à suivre pour le RIG manuel
 - Module 4** Comment se servir de l'outil GRIG-PE
- Nous vous invitons à suivre chaque module de formation dans l'ordre indiqué ci-dessus, et ces modules sont accessibles en tout temps.

Produits de formation pour les fournisseurs de services

Module 1 : Lignes directrices du



Les Lignes directrices abordent le but des RIG, les processus de gestion qui déterminent qui doit faire le signalement et quand ainsi que les catégories et sous-catégories de RIG. Le tableau des principales améliorations et la vidéo mettent en évidence les modifications apportées aux Lignes directrices.



Module 2 : Considérations liées à la protection de la vie privée



La présentation et la vidéo mettent en lumière les rôles et responsabilités des utilisateurs de l'outil GRIG-PE pour protéger les renseignements personnels.



Vous êtes ici!



Module 3 : Marche à suivre pour le RIG manuel



Le processus de gestion et la vidéo expliquent la façon de signaler des incidents graves lorsque l'outil en ligne GRIG-PE est temporairement hors d'usage.



Module 4 : Comment se servir de l'outil GRIG-PE



Le processus de gestion et la vidéo décrivent comment les RIG seront transmis au Ministère si l'outil GRIG-PE en ligne est temporairement inaccessible. Le guide d'enregistrement des utilisateurs explique comment s'inscrire et se connecter à l'outil GRIG-PE. Le guide d'utilisation et la vidéo décrivent comment se servir du module sur les RIG en mettant



Voici l'ordre recommandé pour suivre les modules. On peut revisiter des parties des modules en tout temps.

Sujets de la formation

- Renseignements personnels
- Lois et règlements pertinents
- Principes de protection de la vie privée
- Droits individuels de protection de la vie privée
- Votre rôle dans la protection de la vie privée
- Assurer l'exactitude et respecter la vie privée
- Atteintes à la vie privée et protection des renseignements personnels
- Demandes d'accès et de correction

Section un : Concepts généraux entourant la protection de la vie privée

Qu'est-ce que la vie privée et comment la respectez-vous?

1) Protection de la vie privée

2) Renseignements personnels

3) Paysage des lois sur la protection

de la vie privée

4) Droit à la vie privée

5) Principes de protection de la vie privée

Section deux :

Tenir compte de la protection de la vie privée dans votre travail

1) Votre rôle dans la protection de la vie privée

2) Assurer l'exactitude et respecter la vie privée

3) Atteintes à la vie privée et protection des renseignements personnels

4) Demande d'accès et de correction

Section un : Concepts généraux entourant la protection de la vie privée

Qu'est-ce que la vie privée et comment la respecte-t-on?

Objectifs d'apprentissage

- Définir la vie privée
- Comprendre pourquoi il est important de protéger la confidentialité des renseignements personnels
- Définir l'environnement actuel de la législation encadrant la protection de la vie privée en Ontario
- Définir et reconnaître les renseignements personnels

Qu'est-ce que la vie privée?

- La vie privée a des aspects différents
 - *L'aspect territorial de la vie privée* – Un espace ou un lieu à l'abri de l'intrusion qui est historiquement lié à votre demeure
 - *L'aspect personnel de la vie privée* – La liberté de mouvement et d'expression, le droit à un espace personnel
 - *L'aspect informationnel de la vie privée* – Les personnes maîtrisent et s'approprient leurs renseignements (p. ex. les antécédents médicaux, les dates de naissance, les renseignements bancaires)
- Cette formation porte sur l'aspect **informationnel de la vie privée**
- Les personnes déterminent quand, comment et dans quelle mesure les renseignements qui les concernent sont communiqués et utilisés.

La protection de la vie privée : une responsabilité et un droit!

La Déclaration universelle des droits de l'homme des Nations Unies reconnaît la protection de la vie privée qu'elle considère globalement comme :



Comprendre comment nos renseignements sont recueillis, utilisés et partagés nous aide à être autonomes et à nous sentir en sécurité

Droit à la vie privée

En Ontario, les lois confèrent généralement aux particuliers le droit :

- 1.de consentir** à la collecte, à l'utilisation et à la divulgation de leurs renseignements personnels*
- 2.de savoir pourquoi et comment** leurs renseignements personnels seront recueillis, consultés, stockés et divulgués
- 3.d'avoir un accès raisonnable** aux renseignements conservés qui les concernent
- 4.d'être informés des atteintes à la vie privée** et des mesures prises pour les corriger ou les atténuer
- 5.de demander des corrections** ou des annotations dans leurs dossiers
- 6.de faire une plainte** à un organisme pertinent*

*Plus d'information aux annexes A et B

Vous avez un rôle clé à jouer pour faire respecter le droit à la vie privée des particuliers

Paysage des lois sur la protection de la vie privée

Principes de protection

Équité La protection de la vie privée

Aider à faire respecter le droit à la vie privée afin de protéger les personnes contre les préjudices :

Responsabilisation
Exactitude

Transparence et consentement

Accès individuel
Limiter la collecte, l'utilisation, la divulgation et la conservation

Ouverture

Mesures de protection

Contester la conformité

Les politiques et procédures des fournisseurs de service
harmonisent la pratique quotidienne avec les lois et règlements.

Les autorités et obligations liées à la protection de la vie privée
dans les lois ou les règlements dictent comment les renseignements sont recueillis, utilisés, divulgués, stockés et protégés.
L'application de la loi dépendra de votre organisme, de votre personnel, des personnes que vous servez et du type de renseignements personnels recueillis et utilisés.

La loi
autorise la collecte de renseignements personnels pour l'outil GRIG-PE ou devrait être prise en considération au moment de faire des RIG.*

LSEJF

Loi sur les services à l'enfance, à la jeunesse et à la famille

LSJPA

Loi sur le système de justice pénale pour les adolescents

LMSSC

Loi sur le ministère des Services sociaux et communautaires

LPRPS

Loi de 2004 sur la protection des renseignements personnels sur la santé

LISPD

Loi de 2008 sur les services et soutiens favorisant l'inclusion sociale des personnes ayant une déficience intellectuelle

LAIPVP

Loi sur l'accès à l'information et la protection de la vie privée

*Voir l'annexe A pour plus de contexte et de détails

En quoi consistent les renseignements personnels ?

Tout renseignement consigné qui pourrait mener à **l'identification d'une personne.**

Il est important de reconnaître les renseignements personnels quand vous les voyez afin de pouvoir les protéger en les recueillant, les utilisant et les divulguant adéquatement et en employant les mesures de sécurité ainsi que les pratiques de gestion de l'information adéquates.

Posez-vous la question : *peut-on raisonnablement s'attendre à ce que cette information conduise à l'identification d'une personne?*



N'oubliez pas! Le contexte est important.

Reconnaître des renseignements personnels ne se limite pas seulement à déterminer si vous pourriez personnellement identifier la personne à l'aide de l'information que vous avez en main, mais à déterminer aussi si d'autres personnes pourraient le faire compte tenu de leurs connaissances et de leurs antécédents.

Par exemple, si la personne provient d'une petite communauté, un autre membre de sa communauté pourrait l'identifier plus facilement que vous à l'aide des mêmes éléments d'information.

Mettez votre compréhension à l'épreuve!

(Renseignements personnels)

Parmi ces cas, quel est celui qui comporterait des renseignements personnels?



Une liste d'âges?

Dans beaucoup cas, l'âge ne mènerait pas, à lui seul, à l'identification d'une personne, mais il pourrait être combiné à une autre information, comme une adresse et des renseignements scolaires.



Un nom retiré?

Si, au lieu de contenir des noms, une base de données renfermait l'adresse et la date de naissance, on pourrait quand même combiner ces renseignements pour identifier une personne.



Des renseignements regroupés?

Si les renseignements personnels étaient regroupés à un niveau régional ou provincial, ils pourraient ne plus mener à l'identification d'une personne.

Mettez votre compréhension à l'épreuve!

(Renseignements personnels)

Lisez les scénarios suivants. Selon ce contexte, choisissez l'option qui serait LA MOINS considérée comme étant un renseignement personnel.

1. Zack, un homme, a une déficience X rare et habite dans un établissement de soins dans une petite ville. Seulement trois autres personnes ont la déficience X dans la petite ville.
 - a) Un homme adulte qui a une déficience X dans une petite ville
 - b) Une personne qui a une déficience X dans une petite ville
 - c) Un homme adulte dans une petite ville

2. Carole, une femme, s'identifie comme une noire et habite au foyer de groupe ABC à Toronto. Elle est la seule femme dans le foyer.
 - a) Une femme adulte dans le foyer de groupe ABC
 - b) Carole, de Toronto, femme noire
 - c) Une femme adulte dans le foyer de groupe à Toronto

Mettez votre compréhension à l'épreuve!

(Scénarios sur les renseignements personnels : RÉPONSES)

Lisez les scénarios suivants. Selon ce contexte, choisissez l'option qui serait LA MOINS considérée comme étant un renseignement personnel.

1. Zack, un homme, a une déficience X rare et habite dans un établissement de soins dans une petite ville. Seulement trois autres personnes ont la déficience X dans la petite ville.
 - a) Un homme adulte qui a une déficience X dans une petite ville
 - b) Une personne qui a une déficience X dans une petite ville
 - c) **Un homme adulte dans une petite ville**

2. Carole, une femme, s'identifie comme une noire et habite au foyer de groupe ABC à Toronto. Elle est la seule femme dans le foyer.
 - a) Une femme adulte dans le foyer de groupe ABC
 - b) Carole, de Toronto, femme noire
 - c) **Une femme adulte dans le foyer de groupe**

Section deux :

Tenir compte de la protection de la vie privée dans votre travail

Objectifs d'apprentissage

- Connaître et comprendre les mécanismes de sécurité de l'outil GRIG-PE
- Comprendre votre rôle dans la protection des renseignements personnels
- Comprendre les principes qui régissent l'exactitude, la réduction au minimum des données ainsi que leur rôle dans la protection de la vie privée
- Utiliser les principaux conseils et outils pour protéger les renseignements personnels dans le milieu de travail
- Comprendre comment déceler une atteinte à la vie privée et déterminer les meilleures pratiques pour y réagir
- Répondre aux demandes d'accès et de correction aux dossiers

Mécanismes de sécurité de l'outil GRIG-PE SOR-RL

Le ministère des Services à l'enfance et des Services sociaux et communautaires (MSESSC) améliore les processus pour les rapports d'IG et pour les permis des foyers pour enfants afin de favoriser de meilleurs résultats pour les enfants, les jeunes et les adultes qui sont parmi les plus vulnérables de l'Ontario. Cette démarche comprend la création de l'outil GRIG-PE afin de remplacer les processus manuels pour les signalements d'IG dans le but de faciliter les rapports et de les rendre plus sécuritaires.

Le MSESSC comprend l'importance de garder les renseignements sensibles qui seront entrés dans l'outil GRIG-PE en sécurité. C'est la raison pour laquelle l'outil GRIG-PE comporte les mécanismes de sécurité intégrés suivants pour sécuriser les renseignements :

Dispositifs techniques

- Les renseignements seront stockés sur une plateforme de données sécurisée de la FPO utilisée pour les renseignements de nature très délicate.
- Tous les renseignements transmis seront cryptés pendant leur transit et leur stockage dans l'outil GRIG-PE.
- Les copies exportées ou imprimées des RIG de l'outil GRIG-PE caviarderont le nom et la date de naissance des personnes concernées.
- Plusieurs coupe-feu contribueront à prévenir les accès non autorisés.
- L'outil GRIG-PE a été soumis à des essais de vulnérabilité et de pénétration.

Dispositifs d'accès

- Avant de confier un compte pour l'outil GRIG-PE aux utilisateurs externes, on vérifie leur identité dans le cadre d'une rencontre en personne.
- L'accès utilisateur est authentifié à l'aide d'une vérification en deux étapes.
 - L'attribution d'un nom d'utilisateur et d'un mot de passe
 - L'envoi de mots de passe ponctuels et aléatoires à l'adresse courriel des utilisateurs pour chaque ouverture de session
- L'accès aux renseignements contenus dans l'outil GRIG-PE est en fonction des rôles attribués aux utilisateurs.
- L'accès des membres du personnel aux RIG se limite à l'emplacement de leur site.
- À l'ouverture de session, on rappelle aux usagers que l'utilisation du compte d'une autre personne est un acte frauduleux.
- Les registres des activités des utilisateurs suivront le stockage et la consultation des renseignements pour les besoins de vérification.

Votre rôle dans la protection de la vie privée

En plus de respecter la législation applicable, les mécanismes de sécurité TI et les politiques de protection de la vie privée de votre organisme, **les mesures que vous prenez dans vos tâches quotidiennes** jouent un rôle clé pour la protection de la vie privée des particuliers.



Réduction au minimum des données

La réduction au minimum des données signifie que seule la **quantité minimum de renseignements personnels nécessaires dans un but précis et légitime** est recueillie, utilisée, divulguée ou conservée. La réduction au minimum des données était un aspect important dans la création de l'outil GRIG-PE.

Pourquoi la réduction au minimum de données est-elle importante?

- Elle protège la vie privée en diminuant le risque d'utilisation malveillante et inappropriée de l'information ou de divulgations non autorisées (atteintes à la vie privée).
- Elle réduit les coûts liés à la collecte, au stockage et à l'archivage de l'information.
- Elle facilite le repérage des renseignements pertinents.
- Elle porte au maximum la clarté de l'information.

Dans l'outil GRIG-PE, il est important d'envisager la réduction au minimum de données au moment de remplir des sections ouvertes aux commentaires.

Comment puis-je mettre la réduction au minimum des données en pratique dans l'outil GRIG-PE?

Pour protéger la vie privée d'une personne et diminuer les risques d'atteintes à la vie privée, il est important de garder la réduction au minimum des données à l'esprit au moment de consigner, de partager et de stocker les RIG. Veuillez inclure des renseignements personnels seulement quand on le précise ou on l'exige pour remplir le mandat du RIG (gérer les incidents et surveiller les réactions afin de prévenir ou d'atténuer les incidents).

Par exemple

Une altercation physique se produit entre deux résidents d'un établissement de soins lors d'une sortie à un événement sportif local. Le résident A n'a pas été blessé, mais le résident B a reçu des soins médicaux pour des contusions graves.

Qu'est-ce que la préposée ou le préposé devrait inclure?

- Des renseignements personnels sur les deux résidents liés à l'incident (p. ex. les noms, une partie des renseignements médicaux du résident B)

Qu'est-ce que la préposée ou le préposé devrait omettre?

- Des renseignements personnels sur les deux résidents qui ne sont pas liés à l'incident (p. ex. les antécédents médicaux complets du résident A)
- Des renseignements personnels sur les individus qui étaient présents à l'événement, mais qui ne sont pas concernés par l'incident

* Pour compléter les RIG, voir les lignes directrices 2019 de l'outil GRIG-PE du MSESSC.

Prise de notes exactes et professionnelles

Il est important de garder à l'esprit le but de votre signalement d'incident grave (IG) et de ne pas oublier que les personnes ont le droit d'avoir accès à leurs renseignements.

Vous devriez donc vous efforcer de faire en sorte que les renseignements personnels inclus dans les rapports soient **exacts** et **professionnels**.

Les pratiques exemplaires consistent notamment à :

- veiller à ce que les dossiers soient factuels, à jour et centrés sur le sujet ou l'incident
- donner des détails sur les décisions et en expliquer le raisonnement
- employer un langage professionnel (p. ex. un ton objectif, des termes adéquats)
- exclure les opinions, sauf si elles sont des opinions professionnelles ou des opinions qui sont indiquées comme étant le point de vue ou la perspective d'un particulier dans le RIG

Prise de notes exactes et professionnelles pour les RIG

Il est important de ne pas oublier les objectifs du RIG. Il s'agit d'un processus qui :

- permet aux fournisseurs de service de gérer les incidents à mesure qu'ils surviennent, de créer des dossiers concernant les incidents, et de faire le suivi des mesures prises pour éviter qu'ils se répètent ou du moins atténuer les conséquences.
- assiste le MESSC dans le suivi et la supervision de la prestation des services par les fournisseurs.

Les RIG doivent comporter suffisamment de renseignements pour atteindre leurs objectifs moyennant un juste équilibre entre le droit à la vie privée des particuliers et la nature délicate des renseignements personnels.

Qu'est-ce qu'une atteinte à la vie privée?

- Il y a atteinte à la vie privée quand des renseignements personnels sont :
 - perdus ou volés
 - recueillis, utilisés ou divulgués sans autorisation

L'atteinte à la vie privée peut être volontaire ou involontaire ainsi que d'une portée et d'une gravité variable.

- Exemples d'atteintes à la vie privée :
 - « **Fouiner** » ou consulter des dossiers contenant des renseignements personnels quand ce n'est pas nécessaire ou sans en avoir l'autorisation
 - **Perdre ou voler** une clé USB qui contient des renseignements personnels
 - **Envoyer des renseignements personnels à la mauvaise personne** : transmettre par courriel des fichiers qui contiennent des renseignements personnels à quelqu'un qui n'est pas autorisé à connaître ces renseignements, ou il peut aussi s'agir de discuter de renseignements personnels à un endroit où d'autres personnes pourraient entendre.
 - **Pirater** une base de données électronique qui contient des renseignements personnels (p. ex. une attaque à l'aide d'un logiciel rançonneur)

Protection de l'information : prévenir les atteintes à la vie privée

- **Secure information starts with you!** As a person delivering services, you should consider taking reasonable steps to protect personal information. The following tips will help you ensure information isn't disclosed or used without permission, lost or stolen:



Verrouillez

- Ne laissez jamais de documents papier sans surveillance et ne laissez pas les clés dans les classeurs ou les tiroirs.
- Verrouillez ou déconnectez votre poste de travail ou vos appareils avant de laisser votre bureau sans surveillance.
- Observez une politique en matière de rangement du bureau – tous les bureaux doivent être désencombrés à la fin de chaque journée de travail.
- Gardez les disques, les clés USB et les autres appareils portables avec vous ou dans un lieu sûr.
- Cryptez et choisissez des mots de passe forts et uniques.
- N'écrivez jamais les mots de passe et ne les partagez pas.
- Ne mettez jamais de renseignements personnels sur des appareils personnels ou non sécurisés.



Vérifiez votre entourage

- Utilisez des espaces privés pour les conversations dans le cadre desquelles des renseignements personnels seront divulgués.
- Limitez la quantité de renseignements personnels que vous divulguez quand vous êtes au téléphone, à des comptoirs de services ou en discussion avec des collègues.
- N'examinez pas de documents contenant des renseignements personnels dans des lieux publics où quelqu'un d'autre pourrait en voir le contenu.



Faites preuve d'un bon jugement

- Suivez les politiques et procédures liées à la protection de la vie privée de votre organisme.
- Considérez les risques d'atteintes à la vie privée au moment de consulter, de divulguer, d'éliminer ou de transférer des renseignements personnels.
- Servez-vous de la méthode la plus sécuritaire si vous avez le choix (p. ex., déchiquetez les documents avant de les recycler).
- Utilisez et divulguez seulement les renseignements personnels pertinents.

Outils proactifs que les organismes peuvent utiliser pour protéger les renseignements personnels

Votre organisme possède-t-il les bons outils pour protéger les renseignements personnels?

Électroniques



- Coupe-feu
- Cryptage (p. ex. courriel, clé USB)
- Antivirus, antipourriel, logiciel anti-espion
- Mises à jour régulières pour les logiciels de sécurité
- Évaluations des menaces pour la sécurité



Physiques

- Accès contrôlé aux dossiers et aux salles de réunion
- Classeurs verrouillés
- Identification, vérification et supervision des visiteurs



Administration

- Politiques et procédures de protection de la vie privée
- Formation du personnel
- Ententes de confidentialité
- Tenue d'un registre des membres du personnel qui ont accès à l'outil GRIG-PE
- Processus d'enregistrement à l'outil GRIG-PE du Ministère

Mettez votre compréhension à l'épreuve! (prévenir les atteintes à la vie privée)

Karen, qui rédigeait un RIG, était sur le point de prendre une pause pour aller aux toilettes. Comme elle voulait reprendre la rédaction là où elle était rendue à son retour, au lieu de verrouiller son ordinateur, elle a simplement éteint son écran et recouvert les documents qui étaient sur son bureau. Après tout, elle allait revenir dans cinq minutes à peine!



Dans le courant de la journée, Karen est tombée sur sa collègue, qui travaillait elle aussi à un RIG séparé dans un café local. En voulant laisser libre cours à ses frustrations, Karen lui a fait un résumé de l'incident et des détails sur l'historique familial de l'enfant tout en buvant son café à petites gorgées dans le restaurant.

- **Quelles erreurs Karen a-t-elle commises?**
- **Qu'est-ce qui aurait pu se passer?**
- **Comment Karen peut-elle améliorer ses pratiques à l'avenir?**
- **Comment l'organisme de Karen pourrait-il l'aider à s'améliorer?**

Mettez votre compréhension à l'épreuve!

(Prévenir les atteintes à la vie privée : réponses)

Quelles erreurs Karen a-t-elle commises?

- Elle a laissé des dossiers contenant des renseignements personnels sans surveillance – elle n'a pas sécurisé l'accès à son ordinateur ni verrouillé les dossiers avant de quitter son bureau. Karen a discuté de renseignements personnels dans un endroit public avec une personne non autorisée à connaître ces renseignements.

Qu'est-ce qui s'est passé ou aurait pu se passer?

- Les autres personnes au bureau de Karen auraient pu prendre connaissance des renseignements personnels qu'elle a laissés sur son bureau, les voler ou en faire des copies (p. ex., prendre les renseignements en photo avec leur téléphone), ce qui correspond à atteinte à la vie privée. Il pourrait s'agir des collègues de Karen qui ne sont pas autorisés à prendre connaissance de ces renseignements, des employés d'entretien et des visiteurs.

- Karen n'a pas respecté la vie privée de l'individu, car elle a divulgué des renseignements sur les antécédents de l'enfant et de la famille avec un collègue qui n'est pas autorisé à accéder à ces renseignements.

- Même si le collègue de Karen travaillait sur le dossier, en parler au café, un endroit public, était inapproprié. Les clients du café ont peut-être entendu les renseignements personnels divulgués par Karen. La divulgation de renseignements personnels et le commentaire émotif de Karen auraient aggravé la situation si l'un des

Mettez votre compréhension à l'épreuve!

(Prévenir les atteintes à la vie privée : réponses, 2^e partie)

Comment Karen peut-elle améliorer ses pratiques à l'avenir?

- Fermer sa session dans l'outil GRIG-PE sur son ordinateur, verrouiller son écran, ou prendre d'autres mesures pour s'assurer que seules les personnes qui connaissent le mot de passe peuvent accéder aux renseignements personnels.
- Ranger les dossiers imprimés sous verrou avant de partir, ou les laisser sous la supervision d'une personne autorisée.
- Discuter des renseignements personnels et des cas avec des collègues qui travaillent sur le cas en privé.

Comment l'organisme de Karen pourrait-il l'aider à s'améliorer?

- Former son personnel sur ses politiques, pratiques et outils de protection des renseignements personnels.
- Installer des classeurs à verrou.
- Sécuriser les ouvertures de session sur les appareils électroniques, y compris les ordinateurs.

Réagir aux atteintes à la vie privée SOR→RL

Des atteintes à la vie privée peuvent quand même survenir, malgré les meilleurs efforts. Il convient, en tant que pratique d'excellence, d'établir des protocoles pour y réagir. Voici quelques étapes et considérations clés qui devraient éclairer les réactions à une atteinte à la vie privée.

1)Intervenir et contenir

a. Signalez les atteintes soupçonnées à un supérieur ou gestionnaire ainsi qu'à d'autres autorités si nécessaire.

- a. **Déclarez l'atteinte ou l'atteinte possible comme un IG dans l'outil GRIG-PE**, selon les exigences relatives aux signalements et aux délais énoncés dans les Lignes directrices du SIG 2019 du MDESC. (voir la diapositive 29).

b. Évaluez et déterminez :

- a. Si une violation a eu lieu
- b. Le caractère délicat de l'information concernée
- c. S'il s'agit d'un incident isolé, continu ou récurrent
- d. Le nombre de personnes touchées
- e. Les préjudices possibles pour la ou les personnes touchées, l'établissement et la population

c. Passez à l'action

- a. **Cessez ou limitez l'exposition** des renseignements personnels. Exemples de mesures correctives :
 - Récupérez les copies papier des renseignements personnels qui ont été postées ou télécopiées de manière inadéquate.
 - Rappelez le courriel envoyé par erreur et demandez à la personne qui l'a reçu d'effacer le message.
 - Révoquez l'accès non autorisé à une base de données électronique.

b. Atténuez l'impact sur les personnes touchées (p. ex. en rappelant les courriels contenant des renseignements

Réagir aux atteintes à la vie privée (2e partie)

2) Avisez les personnes

Avisez toutes les personnes dont la vie privée a été atteinte (à moins qu'une notification ne soit pas pertinente ou possible). Veuillez inclure les détails de l'incident, les mesures prises pour aborder l'atteinte et pour atténuer les incidences ainsi que les coordonnées pour obtenir plus de détails.



Remarque : il s'agit d'une obligation pour les fournisseurs de service assujettis à la **partie X de la LPRPS et la LSEJF** (dont l'entrée en vigueur est prévue le 1^{er} janvier 2020).

3) Menez une enquête

Analysez les événements qui ont mené à l'atteinte à la vie privée, évaluez les mesures prises pour contenir l'atteinte et déterminez les moyens à prendre pour prévenir les atteintes à la vie privée à l'avenir.

4) Introduisez un changement

Mettez en place des mesures pour prévenir les atteintes à la vie privée, notamment en modifiant les politiques de protection de la vie privée, en élaborant de nouveaux protocoles de sécurité et de

Signaler les atteintes à la vie privée dans l'outil GRIG-PE

En cas d'atteinte avérée ou présumée à la vie privée qui cause de graves dommages ou risques à l'individu en question ou à d'autres personnes, ou en violation avec la Loi sur le système de justice pénale pour les adolescents (LSJPA), la situation doit obligatoirement être signalée en tant que RIG.

Toutes les atteintes à la vie privée correspondant à ces critères sont considérées comme étant un RIG de niveau 1 : les fournisseurs de services doivent en aviser immédiatement le Ministère et soumettre un RIG dans les 60 minutes suivant la prise de connaissance de l'incident grave ou la détermination que l'incident est grave.

La description de l'incident grave doit inclure :

- la nature de l'atteinte à la vie privée
- une description des renseignements personnels divulgués
- Les mesures prises par le fournisseur de service pour corriger la situation et empêcher qu'elle se reproduise (reprendre possession des renseignements personnels, mener une enquête à l'interne, améliorer les procédures, etc.)
- une note pour indiquer si la victime de l'atteinte avérée ou potentielle à la vie privée a été avisée de la divulgation, et si ce n'est pas le cas, expliquer pourquoi
- Le cas échéant, confirmer que la victime de l'atteinte à la vie privée a été avisée de ses droits de soumettre une plainte auprès du Commissaire à l'information et à la protection de la vie privée (CIPVP) et indiquer si le CIPVP a été contacté

Ne pas oublier : il faut signaler les atteintes à la vie privée en tant que RIG uniquement si elles entraînent de graves dommages ou risques, ou sont en violation de la LSJPA.

Demandes d'accès et de correction

En général, les personnes doivent avoir accès aux renseignements personnels qui les concernent. Les personnes doivent être informées de l'existence, de l'utilisation et de la divulgation de leurs renseignements personnels et y avoir accès sur demande, sauf si certaines exceptions s'appliquent (p. ex. si la communication des renseignements augmenterait le risque de préjudice pour une personne). Les personnes peuvent également contester l'exactitude de leurs renseignements personnels et demander des modifications ou des annotations, suivant le cas.

Pratiques d'excellence :

- Les fournisseurs de services qui ont la garde et le contrôle des renseignements personnels doivent fournir les documents complets qui contiennent les renseignements personnels lorsque les individus en demandent l'accès (sauf s'il y a un risque de préjudice ou si d'autres exceptions s'appliquent).
- S'il faut apporter une correction et les renseignements personnels ont été modifiés, les fournisseurs de service doivent transférer les renseignements modifiés aux parties qui ont reçu les anciens renseignements.

Demandes d'accès et de correction : d'intervention

Loi	Application	Délai d'intervention	Prolongation maximum	Coût
LPRPS	Dépositaires de renseignements sur la santé	30 jours	30 jours	Droits de recouvrement des coûts raisonnables
LSEJF Partie X*	Les fournisseurs de services qui sont financés et agréés en vertu de la LSEJF et qui ne sont pas visés par d'autres lois sur la protection de la vie privée	30 jours	90 jours	Sans frais
LAIPVP	Les ministères et les agences, les conseils, les commissions, les corporations et autres organismes désignés en tant qu'établissement (p. ex., universités, LCBO et CSPAAT)	30 jours	Prolongation raisonnable selon les circonstances	5,00\$ + frais administratifs
LAIMPVP	Municipalités, conseils locaux (scolaires, etc.) et commissions locales	30 jours	Prolongation raisonnable selon les circonstances	5,00\$ + frais administratifs

*Remarque : LSEJF, partie X, entrera en vigueur le 1^{er} janvier 2020

Ce que nous avons abordé

- **La protection de la vie privée est un droit** énoncé dans les lois qui se rattachent à la protection des renseignements personnels des particuliers.
- **Vous avez un rôle important à jouer pour préserver la vie privée en :**
 - prévenant les atteintes à la vie privée
 - signalant les atteintes soupçonnées
 - veillant à ce que seuls les renseignements personnels les plus pertinents soient consignés (réduction au minimum des données)
 - créant et tenant à jour des dossiers exacts et professionnels
 - aidant les gens à avoir accès à leurs dossiers ou à demander que des modifications y soient apportées
- **Vous êtes encadrés pour protéger la vie privée par :**
 - les politiques et procédures de protection de la vie privée de votre organisme
 - les mesures de protection des données et de la vie privée de votre organisme (p. ex. des classeurs verrouillés, des logiciels)
 - les mécanismes de sécurité intégrés de l'outil CBIC DE

Prochaines étapes

1. Prenez en considération les concepts et principes de protection de la vie privée que vous avez appris et examinez les politiques et procédures de votre organisme ainsi que les autres formations du personnel
2. Consultez votre propre conseillère ou conseiller juridique si vous vous demandez si vous êtes en conformité avec les lois et règlements sur la protection de la vie privée pertinents
3. Acheminez vos questions sur les sujets abordés au cours de cette formation à votre représentante ou représentant ministériel habituel
4. Trouvez des ressources supplémentaires
 - Par exemple, les Premières Nations peuvent avoir leurs propres politiques ou règles pour leurs communautés – vérifiez le site Web du conseil de bande ou communiquez avec votre personne-ressource pour confirmer.

ANNEXE A : Paysage des lois sur la protection de la vie privée

Loi	Les personnes visées	Ses incidences sur l'outil GRIG-PE / facteurs à considérer
Loi sur l'accès à l'information et la protection de la vie privée (LAIPVP))	Les exigences générales relatives à la protection de la vie privée pour les institutions gouvernementales provinciales •(p. ex. les ministères, organismes, universités)	Permet à toute personne de demander l'accès aux renseignements conservés par le gouvernement et les institutions, y compris les renseignements personnels.
Loi sur l'accès à l'information municipale et la protection de la vie privée (LAIMPVP)	Les organismes gouvernementaux locaux •(p. ex. les conseils scolaires)	Permet aux gens de demander l'accès aux renseignements conservés par les organismes gouvernementaux locaux, y compris aux renseignements personnels.
Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS)	Les dépositaires des renseignements sur la santé •(p. ex. les hôpitaux, les professionnels de la santé)	La LPRPS énonce les objectifs ainsi que l'orientation de la collecte, de l'utilisation et de la divulgation des renseignements personnels dans le secteur de la santé. Les renseignements sur la santé devraient être traités conformément à l'orientation précisée dans la LPRPS.
Loi sur le système de justice pénale pour les adolescents (LSJPA)	Les entités du système de justice pour la jeunesse •(p. ex. les établissements de garde ou de détention)	La LSJPA protège la vie privée des jeunes ayant des démêlés avec la loi en limitant la publication d'information pouvant les identifier, de même que les témoins ou victimes de moins de 18 ans de crimes commis par des jeunes. La LSJPA impose aussi des limites strictes sur l'accès à des dossiers sur des jeunes tenus aux termes de la Loi, et sur leur divulgation. La LSJPA est une loi fédérale. Elle prévaut donc en cas de conflit avec une loi provinciale. Votre organisme doit respecter la LSJPA à l'égard des renseignements et des dossiers sur les jeunes.
Loi de 2017 sur les services à l'enfance, à la jeunesse et à la famille (LSEJF)	Les fournisseurs de services financés, les sociétés d'aide à l'enfance, les titulaires d'un permis d'établissement et certains parents de famille d'accueil	La partie X énonce les objectifs ainsi que l'orientation de la collecte, de l'utilisation et de la divulgation des renseignements personnels dans le secteur des services à l'enfance, à la jeunesse et à la famille.
Loi sur le ministère des Services sociaux et communautaires (LMSSC)	Le Ministère et les fournisseurs de services financés •(p. ex. les maisons d'hébergement pour femmes, les fournisseurs de services de ressourcement et de mieux-être pour les Autochtones en	Les bénéficiaires de paiements de transfert qui reçoivent des fonds pour mettre sur pied des programmes qui sont assujettis à la LMSSC doivent respecter les exigences relatives à la protection de la vie privée énoncées dans la Loi et dans les contrats de service.

Des questions? Consultez une conseillère ou un conseiller juridique pour connaître les incidences des lois sur votre

Loi de 2008 sur les services Les fournisseurs de services financés *travail* autorise la collecte directe et indirecte de renseignements personnels par les

ANNEXE B : Principes de protection de la vie privée

(1^{re} partie)

Responsabilisation

- Tous les membres du personnel sont responsables de la sécurité et de la confidentialité des renseignements personnels dont ils ont le contrôle.
- Les organismes et les membres du personnel doivent renseigner les personnes et les aider à faire des demandes d'accès, des plaintes ou des contestations.
- L'organisme a la responsabilité de créer des politiques et procédures qui veillent à ce que les renseignements personnels soient recueillis, utilisés, divulgués et conservés d'une manière qui respecte le droit à la vie privée des particuliers.

Exactitude

- Tous les membres du personnel ont la responsabilité de fournir des renseignements exacts, complets et à jour.
- Les RIG devraient être consignés et transmis d'une manière professionnelle (c.-à-d. en évitant les commentaires non fondés sur des faits, sauf s'il est précisé qu'il s'agit du point de vue ou de la perspective d'une personne).

Transparence et consentement

- Les personnes et/ou leurs tuteurs devraient savoir que leurs renseignements personnels seront communiqués au Ministère dans le cadre du processus de signalement d'IG pour les besoins de planification et de surveillance du système.

Accès individuel

- Les personnes ont le droit d'avoir accès à leurs dossiers et aux renseignements qui les concernent, sauf s'il y a des préoccupations importantes en matière de sécurité ou si une loi et/ou une ordonnance de la cour les en empêche.
- Les membres du personnel devraient être prêts à répondre aux demandes d'accès dans les délais prescrits par la loi et à préparer les dossiers en gardant l'accès à l'esprit (c.-à-d. en prenant de notes professionnelles, en veillant à l'exactitude