Santé Canada Health Canada

**Rapport de vérification définitif**

# Vérification des pratiques de protection des renseignements personnels

**7 décembre 2012**

# Table des matières



*Version traduite. La version anglaise doit prévaloir en cas d'incohérence.*

# Sommaire

La présente vérification porte sur les pratiques de Santé Canada en matière de protection des renseignements personnels conformément à la *Loi sur la protection des renseignements personnels*, laquelle constitue le cadre juridique régissant la collecte, l'utilisation et la divulgation de renseignements personnels du gouvernement fédéral. Santé Canada recueille, utilise et conserve plus de renseignements personnels que la plupart des autres ministères. De plus, il se distingue quant à la sorte et à la sensibilité des renseignements personnels qui relèvent de lui. La protection des renseignements personnels est une responsabilité partagée entre la Division de l'accès à l'information et de la protection des renseignements personnels (AIPRP) et les directions générales des programmes. La Division de l'AIPRP joue un rôle de premier plan dans l'élaboration et le soutien de pratiques de protection des renseignements personnels dans l'ensemble du Ministère, tandis que les directions générales ont la responsabilité au jour le jour de la protection et du traitement de renseignements personnels.

La vérification a été effectuée conformément à la *Politique sur la vérification interne* du Conseil du Trésor et aux *Normes internationales pour la pratique professionnelle de vérification interne*. Des procédures suffisantes et appropriées ont été suivies et des preuves ont été recueillies pour appuyer la conclusion de la vérification.

Dans l'ensemble, Santé Canada gère avec soin et attention les renseignements personnels qui relèvent de lui. En effet, le Ministère possède une solide culture de sécurité et de confidentialité dans l'exécution des activités essentielles des programmes. Toutefois, l'assurance de la sécurité et de la confidentialité des renseignements personnels n'est pas, en soi, synonyme de protection de la vie privée d'une personne.

Bien que Santé Canada se soit beaucoup amélioré en ce qui concerne le respect de ses exigences législatives en vertu de la Loi, il lui sera avantageux de finaliser, d'approuver et de mettre en œuvre son cadre de gestion de la protection des renseignements personnels, lequel servira à orienter et à mettre en application, dans l'ensemble du Ministère, de bonnes pratiques de protection des renseignements personnels. Le Ministère tirera également avantage d'une meilleure intégration des questions touchant la protection des renseignements personnels au processus décisionnel stratégique et à d'autres processus de gestion des risques au sein des directions générales.

Basé sur un examen d'un échantillon de formulaires utilisés pour recueillir des renseignements personnels au sein de certaines directions générales, le Ministère tirera avantage de réexaminer ses formulaires sous l'orientation du directeur de l'AIPRP afin d'obtenir la conformité aux dispositions relatives aux avis en vertu de la Loi et les directives qui l'appuient.

De plus, les domaines des programmes dépendent sur des procédures opérationnelles normalisées tel qu'il en découle des lois habilitantes et des règlements afin de gouverner le recueil et l'utilisation des renseignements personnels. Dans certains cas, ces procédures opérationnelles normalisées comprennent des dispositions relatives à la vie privée et pour la saine manipulation de renseignements personnels. Dans d'autres cas, les procédures

opérationnelles normalisées et les lignes directrices concernant la manipulation des renseignements personnels ne comprennent pas suffisamment d'information destinée au personnel de première ligne concernant les exigences en matière de manipulation des renseignements personnels en vertu de la Loi. Les directions générales tireront avantage en collaborant avec la Division de l'AIPRP en vue d'examiner et de mettre à jour les procédures opérationnelles normalisées, les lignes directrices et les protocoles du Programme afin de renforcer les contrôles pour le recueil, l'utilisation, la divulgation et la conservation des renseignements personnels.

Bien que la formation et la sensibilisation à l'égard de la protection des renseignements personnels s'améliorent constamment, la vaste majorité des employés de Santé Canada, dont un grand nombre participent activement à la gestion et au traitement de données de nature délicate, n'ont toujours pas reçu de formation officielle sur ce sujet.

Nonobstant les constatations précédentes, la vérification a révélé la présence de plusieurs cas de bonnes pratiques de protection des renseignements personnels au sein de Santé Canada et ces derniers sont signalés tout au long du présent rapport. En fonction des données disponibles, lorsque les programmes individuels ont pris l'initiative de financer les ressources affectées à la protection des renseignements personnels, le secteur de programme a été en mesure de faire progresser ses pratiques à cet égard.

La direction souscrit aux six recommandations et a fourni un plan d'action pour renforcer les pratiques de protection des renseignements personnels au sein du Ministère.

# A- Introduction

## 1. Contexte

La *Loi sur la protection des renseignements personnels* constitue le cadre juridique régissant la collecte, l'utilisation et la divulgation de renseignements personnels du gouvernement fédéral. Entrée en vigueur le 1er juillet 1983, elle s'appuie sur le principe selon lequel les personnes ont le droit de savoir quels sont les renseignements recueillis à leur sujet et comment ils seront utilisés dans l'administration des services et programmes gouvernementaux.

Selon la loi, les institutions fédérales doivent limiter la collecte de renseignements personnels à ceux qui ont un lien direct avec leurs programmes ou leurs activités. Une fois les renseignements recueillis, ils doivent les gérer avec soin et attention. Afin de se conformer à la Loi, ainsi qu'aux politiques et directives connexes, les ministères fédéraux doivent disposer de politiques et de pratiques suffisantes pour protéger les renseignements personnels qui leur sont confiés.

Le Secrétariat du Conseil du Trésor du Canada est chargé de s'assurer que le Ministère respecte la Loi. Il exerce ses responsabilités en matière de surveillance en grande partie en analysant et en examinant des rapports institutionnels, y compris les présentations au Conseil du Trésor, les rapports ministériels sur le rendement et les résultats des vérifications, des évaluations et des études indépendantes.

En plus des activités de surveillance du Secrétariat du Conseil du Trésor (SCT) du Canada, le gouvernement a confié au Commissariat à la protection de la vie privée du Canada (CPVP) la responsabilité de faire enquête sur les plaintes portées par des particuliers à l'égard du traitement de renseignements personnels par les institutions fédérales. Le Commissaire à la protection de la vie privée, a également le pouvoir de mener des examens de conformité à l'égard des pratiques de protection des renseignements personnels des institutions fédérales en ce qui concerne la collecte, la conservation, l'exactitude, l'utilisation, la divulgation ou le retrait des renseignements personnels.

Lorsqu'il a été déterminé qu'un ministère ne s'est pas acquitté de ses obligations juridiques ou politiques, le président du Conseil du Trésor peut, si on lui signale un problème systématique de conformité, examiner et annuler des tâches et fonctions choisies du ministre, tel qu'il est prévu à l'article 71 de la Loi. Le SCT peut également imposer à une institution des exigences additionnelles en ce qui concerne les rapports annuels au Parlement et/ou en vertu de son Cadre de responsabilisation de gestion.

**Exemples de renseignements personnels à Santé Canada**

- Nom, adresse, sexe, religion, numéro d'assurance sociale.
- Dossiers médicaux, psychiatriques, psychologiques et de laboratoire.
- Dossiers d'exposition aux rayonnements au travail.
- Dossiers relatifs aux maladies transmissibles.
- Information générique.

Santé Canada recueille, utilise et conserve plus de renseignements personnels que la plupart des autres ministères fédéraux. De plus, il se distingue quant à la sorte et à la sensibilité des

renseignements personnels qui relèvent de lui. Les renseignements personnels sont définis comme étant des renseignements au sujet d'un individu identifiable qui sont consignés sous n'importe quelle forme.

En vertu de la Loi, les responsables des institutions fédérales sont tenus d'identifier, de décrire et de rendre publics leurs renseignements personnels et leurs catégories de renseignements personnels dans les publications annuelles du Secrétariat du Conseil du Trésor intitulées *Info Source*. Les descriptions de fichier de renseignements personnel (FRP) sont les instruments qu'utilise une institution fédérale pour informer le public sur les renseignements personnels qu'elle recueille. Ces descriptions permettent aux individus d'apprendre comment leurs renseignements personnels sont utilisés et la durée pendant laquelle ils sont conservés.

Pour l'année 2011, Santé Canada avait approximativement 45 FRP enregistrés. Le tableau ci-dessous résume l'inventaire enregistré de renseignements personnels par direction générale de programme et architecture des activités de programmes :

| DIRECTION GÉNÉRALE RESPONSABLE | PRINCIPALES ACTIVITÉS DE PROGRAMMES (ARCHITECTURE DES ACTIVITÉS DE PROGRAMMES) | FRP | % DE FRP* |
|---|---|---|---|
| Direction générale de la santé environnementale et de la sécurité des consommateurs (DGSESC) | ▪ Risques environnementaux pour la santé<br>▪ Sécurité des produits de consommation<br>▪ Consommation et abus de substances<br>▪ Protection contre les radiations | 21 | 46 % |
| Direction générale des produits de santé et des aliments (DGPSA) | ▪ Produits de santé<br>▪ Salubrité des aliments et nutrition | 8 | 18 % |
| Direction générale de la santé des Premières nations et des Inuits (DGSPNI) | ▪ Soins de santé primaires des Premières nations et des Inuits<br>▪ Prestations supplémentaires en santé à l'intention des membres des Premières nations et des Inuits | 8 | 18 % |
| Bureau des régions et des programmes (BRP) | ▪ Système de santé canadien<br>▪ Services de santé spécialisés | 7 | 16 % |
| Agence de réglementation de la lutte antiparasitaire (ARLA) | ▪ Sécurité des pesticides | 1 | 2 % |
| **Nombre total de fichiers de renseignements personnels enregistrés** | | 45 | 100 % |

*** Remarque :** Le nombre total de FRP indiqué ci-dessus ne reflète pas le nombre d'ensembles de données que détient une direction générale ou un secteur de programme donné. Toutefois, les FRP fournissent un aperçu assez juste des secteurs où le Ministère est le plus actif en ce qui a trait à la collecte et à l'utilisation de renseignements personnels. En fonction de ce qui précède, la gestion des renseignements personnels par Santé Canada semble être centralisée au sein de la DGSESC, de la DGPSA et de la DGSPNI, avec les régions qui jouent un rôle essentiel dans la collecte et l'utilisation de données personnelles au sein de chaque direction générale de programme.

**Pratiques de Santé Canada en matière de protection des renseignements privés**

Comme le Ministère recueille, utilise et divulgue des renseignements personnels, il est assujetti aux exigences de la *Loi sur la protection des renseignements personnels*. Il est également assujetti aux politiques et directives établies par le Conseil du Trésor qui appuient l'administration de la Loi, principalement la *Politique sur la protection de la vie privée*, la *Directive sur les pratiques relatives à la protection de la vie privée* et la *Directive sur l'évaluation des facteurs relatifs à la vie privée*.

La Division de l'accès à l'information et de la protection des renseignements personnels (AIPRP) assume les responsabilités générales relatives à l'administration de la Loi. La Division de l'AIPRP relève du sous-ministre adjoint, Direction générale des services de gestion, par l'entremise du directeur général, Direction de la planification, de l'intégration et des services de gestion. Elle est actuellement composée de six unités : Réception rapide et pratiques professionnelles, Conseils en matière de politique (protection des renseignements personnels), Portefeuille des médicaments, Intérêt public et autre, Arriéré/opérations de protection des renseignements personnels et soutien à l'Agence de la santé publique du Canada (ASPC). Pour l'exercice 2011-2012, la Division avait un budget de base destiné aux activités de protection des renseignements privés ainsi qu'à celles de l'accès à l'information d'environ 4,2 millions de dollars. De plus, elle compte actuellement 42 équivalents temps plein, dont neuf sont consacrés à la protection des renseignements personnels.

La Division de l'AIPRP est responsable d'un large éventail de services de gestion. Sous la direction du directeur et du coordonnateur de l'AIPRP, elle est chargée de répondre aux demandes d'information et de renseignements personnels de la part du public, de promouvoir la sensibilisation du personnel et la formation en matière de protection des renseignements personnels et d'élaborer des politiques et pratiques en matière d'accès à l'information et de protection des renseignements personnels à l'échelle ministérielle. Elle est également responsable d'examiner les lois et politiques proposées qui ont une incidence sur la protection des renseignements personnels et de conseiller les gestionnaires de programme quant à leurs obligations à l'égard de la collecte, de l'utilisation et de la divulgation de renseignements personnels en vertu de la Loi, ce qui comprend la coordination et la supervision du Processus ministériel d'évaluation des facteurs relatifs à la vie privée (ÉFVP).

Alors que la Division de l'AIPRP joue un rôle de premier plan dans l'élaboration et le soutien de pratiques de protection des renseignements personnels dans l'ensemble du Ministère, la responsabilité concernant la protection et le traitement des renseignements personnels est une responsabilité que se partagent la Division de l'AIPRP et les directions générales des programmes. Bien que la *Loi sur la protection des renseignements personnels confère* les pouvoirs au directeur de la l'AIPRP, les directions générales des programmes doivent appuyer le responsable fonctionnel en gérant les renseignements personnels sous le contrôle des directions générales d'une manière cohérente et légale. Cela comprend notamment les activités suivantes : protéger les renseignements personnels d'une manière correspondant à leur sensibilité, porter à l'attention de la Division de l'AIPRP les questions et préoccupations de protection des renseignements personnels à mesure où elles surviennent lors du traitement de ces derniers, procéder à une évaluation des facteurs relatifs à la vie privée, au besoin, et informer immédiatement la Division de l'AIPRP de toute atteinte. De plus, les directions

générales sont tenues d'informer la Division de l'AIPRP de toute mise à jour ou modification à leurs fonds de renseignements personnels.

## 2. Objectif de la vérification

La vérification visait à évaluer la pertinence et l'efficacité des politiques, des pratiques et des mesures de contrôle de Santé Canada qui appuient la conformité du Ministère à la *Loi sur la protection des renseignements personnels* et à ses politiques et directives connexes.

## 3. Portée et méthode

La vérification était axée sur les responsabilités de la Direction générale des services de gestion en matière de gestion des renseignements personnels et sur les pratiques des directions générales des programmes participant le plus activement dans le traitement des renseignements personnels. Au moment du lancement de la vérification, trois directions générales représentaient environ 82 pourcent des fonds de renseignements personnels enregistrés du Ministère. Ensemble, elles étaient responsables d'activités de programme dans le cadre desquelles on recueillait, utilisait et divulguait les ensembles de données les plus volumineux et sensibles.

D'après une évaluation préliminaire des risques, il a été déterminé qu'un examen des pratiques de protection des renseignements personnels de ces trois directions générales des programmes (DGSESC, DGPSA, DGSPNI), ainsi qu'un examen des initiatives stratégiques et politiques sous la responsabilité de la Direction générale des services de gestion (particulièrement la Division de l'AIPRP), fourniraient la meilleure évaluation possible des pratiques globales du Ministère en matière de protection des renseignements personnels. Les renseignements personnels appartenant aux employés de Santé Canada, lesquels seront inclus à la *Vérification de PeopleSoft* prévue en 2013-2014, ainsi que les renseignements appartenant aux Services de santé spécialisés – Programme de la santé des fonctionnaires fédéraux qui ont été examinés lors de la Vérification du Programme de la santé des fonctionnaires fédéraux de 2012, ont été exclus de la présente vérification.

Dans le cadre de la vérification, on a examiné la conception et le fonctionnement des pratiques de Santé Canada en matière de protection des renseignements personnels, tels qu'ils ont été mesurés par rapport aux exigences de la Loi et de ses politiques et directives connexes. Des activités de vérification ont été menées au sein des directions conformément à la *Politique sur la vérification interne*. Les méthodes employées comprenaient des entrevues et des observations, l'examen des documents, des politiques, des normes, des lignes directrices et des cadres, ainsi que des enquêtes, des mises à l'essai et des analyses.

## 4. Énoncé d'assurance

Selon le jugement professionnel du dirigeant principal de la vérification, des procédures suffisantes et appropriées ont été suivies, et des preuves ont été recueillies pour confirmer l'exactitude de la conclusion de la vérification. Les constatations et la conclusion de la vérification se fondent sur une comparaison des conditions qui existaient au moment de la vérification et des critères convenus avec la direction. De plus, les preuves ont été

rassemblées conformément aux *Normes relatives à la vérification interne au sein du gouvernement du Canada* et aux *Normes internationales pour les méthodes professionnelles de la vérification interne.*

# B- Constatations, recommandations et réponses de la direction

## 1. Gouvernance

### *1.1 Cadre de gestion de la protection des renseignements personnels*

***Critère de vérification :*** *Le Ministère a élaboré et mis en œuvre un cadre de gestion de la protection des renseignements personnels pour appuyer la gestion et la surveillance des pratiques de gestion des renseignements personnels à l'échelle ministérielle.*

En vertu de la *Politique sur la protection de la vie privée du gouvernement*, les responsables des institutions doivent établir des pratiques de gestion des renseignements personnels pour appliquer de façon juste et uniforme la Loi sur la protection des renseignements personnels. La conformité à la Loi suppose l'existence d'une infrastructure administrative pour orienter et appuyer le traitement et la protection des renseignements personnels. La plupart du temps, les pratiques de gestion sont régies au moyen d'un cadre ministériel de gestion de la protection des renseignements personnels.

**Éléments essentiels d'un cadre de gestion de la protection des renseignements personnels**

- Engagement organisationnel (participation des dirigeants)
- Rôles et responsabilités en matière de conformité à la protection des renseignements personnels clairement définis
- Exigences sur les plans de la formation et de l'éducation
- Protocoles de réponse de la direction en cas d'atteinte et d'incident
- Référence à la politique en matière de protection sur la vie privée et aux outils d'évaluation des risques
- Mécanismes de surveillance et d'examen

Un cadre de gestion de la protection des renseignements personnels expose les règles et les pratiques sur lesquelles la haute direction s'appuie pour définir les attentes à l'égard de la protection des renseignements personnels, attribuer ou déléguer des pouvoirs et des responsabilités, ainsi que la responsabilisation relativement à la conformité à la Loi et à ses politiques connexes. En plus de démontrer une capacité à se conformer à la Loi et à ses politiques et directives connexes, un cadre de gestion de la protection des renseignements personnels aide à préciser les rôles et responsabilités ministériels sur le plan de la protection des renseignements personnels, fournissant une base pour déterminer les structures, les ressources et les compétences nécessaires pour qu'il y ait des pratiques de gestion saines en matière de protection des renseignements personnels dans toutes les directions générales, à promouvoir la responsabilisation et l'amélioration continues des pratiques relatives au traitement des renseignements personnels au moyen de rapports, de vérifications et d'évaluations de programmes ainsi que de la prestation de formation continue en matière de protection des renseignements personnels destinée aux employés, à établir des normes claires pour la collecte, l'utilisation, la divulgation et la conservation des renseignements personnels, ainsi que des pratiques exemplaires ou des contrôles efficaces pour la promotion et l'application de la protection des renseignements personnels.

Bien que le résultat le plus évident d'un cadre de gestion de la protection des renseignements personnels soit la capacité démontrable à se conformer aux exigences de la *Loi sur la protection des renseignements personnels*, s'il est efficace, l'existence d'un tel cadre

appuierait également les ministères et organismes pour qu'ils gèrent efficacement les risques liés à la protection des renseignements personnels, préservant ainsi la réputation d'un ministère aux yeux de la population canadienne à titre de gardien de confiance des renseignements de nature délicate.

Santé Canada reconnaît depuis longtemps qu'un cadre de gestion de la protection des renseignements personnels pour orienter le traitement des renseignements personnels est une priorité. Dès 2001, la haute direction a soulevé le besoin qu'il y ait, dans l'ensemble des directions générales, une approche centralisée, coordonnée et cohérente à la gestion des renseignements personnels qui inclurait des outils et des politiques de soutien. En 2010, sous la direction de la Division de l'AIPRP, Santé Canada a élaboré et entrepris la mise en œuvre de la Stratégie en matière de protection des renseignements personnels pour sensibiliser davantage les employés à cet égard. Cette stratégie n'a toutefois par permis d'établir des structures de gouvernance et de responsabilisation pour qu'on puisse déterminer et surveiller à l'échelle ministérielle des responsabilités liées à la protection des renseignements personnels. De plus, à elle seule, la stratégie ne satisfait pas aux exigences relatives à la gestion de la protection des renseignements personnels énoncées dans la *Politique sur la protection de la vie privée* du Conseil du Trésor.

Récemment, la Division de l'AIPRP a entrepris l'élaboration d'un cadre de gestion de la protection des renseignements personnels, qui demeure à l'état d'ébauche. Il importera que le Ministère fasse progresser ses politiques de protection des renseignements personnels en approuvant et en mettant en œuvre le cadre provisoire.

***Recommandation 1***

*Il est recommandé que le sous-ministre adjoint, Direction générale des services de gestion, mette en œuvre un cadre de gestion de la protection des renseignements personnels pour appuyer la gestion et la surveillance de la pratique ministérielle liée à la protection des renseignements personnels.*

***Réponse de la direction***

La direction souscrit à cette recommandation.

Un cadre de gestion de la protection des renseignements personnels sera finalisé afin d'exposer les règles et les pratiques sur lesquelles la haute direction s'appuie pour définir les attentes à l'égard de la protection des renseignements personnels, attribuer ou déléguer des pouvoirs et des responsabilités, ainsi que la responsabilisation relativement à la conformité à la Loi et à ses politiques connexes.

Il convient de noter que Santé Canada fournit des services de gestion à l'Agence de la santé publique du Canada depuis juin 2012, et que lorsqu'il sera finalisé, le Cadre de gestion du rendement sera utilisé par les deux organisations.

## *1.2 Rôles et responsabilités*

***Critère de vérification :*** *Le Ministère a désigné une ou des personnes qui doivent s'assurer que l'institution respecte la Loi sur la protection des renseignements personnels, les politiques et directives. Les rôles et les responsabilités liés à la protection des renseignements personnels sont compris et attribués de façon appropriée.*

Selon la *Loi sur la protection des renseignements personnels*, les responsables des institutions fédérales peuvent déléguer, à un ou à plusieurs cadres ou employés, des pouvoirs, des attributions ou des fonctions choisis prévus à la Loi. Une fois qu'un arrêté de délégation est signé, les pouvoirs, attributions ou fonctions qui ont été délégués ne peuvent être exercés que par l'administrateur général, ou bien les cadres ou employés nommés. Bien que les délégués soient responsables des décisions prises en vertu de l'arrêté, la responsabilité finale quant au respect de la Loi incombe à l'administrateur général.

Voici certaines des responsabilités assignées aux administrateurs généraux ou aux délégués : la sensibilisation à l'égard de la protection des renseignements personnels (faire connaître aux employés les politiques, les procédures et leurs responsabilités légales aux termes de la Loi), les évaluations de facteurs relatifs à la vie privée (ÉFVP) (assurer la réalisation, la mise à jour et la publication des ÉFVP) et surveiller le respect de la *Politique sur la protection de la vie privée* dans le cadre de l'administration de la Loi.

En plus des responsabilités susmentionnées confiées aux responsables ou aux délégués ministériels, le Conseil du Trésor a confié des responsabilités complémentaires aux cadres et aux agents principaux des ministères qui gèrent des programmes ou des activités comportant la création, la collecte et le traitement de renseignements personnels. Ces responsabilités vont dans le même sens que les dispositions prévues à la Loi en matière d'avis, de collecte, d'utilisation, de divulgation et d'exactitude. Ensemble, la *Politique sur la protection de la vie privée* et la *Directive sur les pratiques relatives à la protection de la vie privée* du gouvernement visent à définir des responsabilités claires quant à la prise de décisions relatives à des affaires discrétionnaires en vertu de la Loi, ainsi que la responsabilisation relativement à la gestion des renseignements personnels au sein des institutions.

À Santé Canada, les responsabilités en matière de protection des renseignements personnels sont décrites dans plusieurs documents disponibles à l'interne, plus particulièrement : le wiki du Ministère sur la protection des renseignements personnels, sa politique proposée sur la protection de la vie privée et son Cadre de gestion de la protection de la vie privée provisoire. Bien que l'attribution des responsabilités relatives à la protection des renseignements personnels soit généralement conforme aux responsabilités définies par le Secrétariat du Conseil du Trésor du Canada, les rôles et responsabilités devraient être plus normatifs quant aux responsabilités relatives à la protection des renseignements personnels propres à la nature des directions générales régionales et opérationnelles de Santé Canada. On pourrait également les améliorer en définissant les responsabilités générales en matière de protection des renseignements personnels des employés de première ligne et des gestionnaires divisionnaires qui participent le plus activement au traitement des renseignements personnels.

**Personnes-ressources en matière de protection des renseignements personnels**

- Agent de programme, protection des renseignements personnels/Gestion de l'information
- Analyste divisionnaire de la conformité
- Analyste de la protection des renseignements personnels des directions générales
- Champion de la protection des renseignements personnels des directions générales
- Coordonnateur de la protection des renseignements personnels des directions générales
- Conseiller en gestion de l'information des directions générales (CGIDG)
- Conseiller en gestion de l'information des régions (CGIR)
- Membres du Comité sur la protection des renseignements personnels du Ministère
- Groupe consultatif en matière de politiques, AIPRP
- Services juridiques, groupe de gestion de l'information

Bien que l'on accepte généralement qu'à Santé Canada, la responsabilité à l'égard de la gestion des renseignements personnels est une responsabilité partagée entre les responsables des directions générales et la Division de l'accès à l'information et de la protection des renseignements personnels (AIPRP), peu des répondants de programme interrogés étaient en mesure d'indiquer clairement où commencent et se terminent leurs responsabilités.

Dans les affaires liées à la politique relative à la protection de la vie privée, la Division de l'AIPRP se considère principalement comme un expert en la matière, fournissant des conseils et une orientation lorsqu'elle participe. Par défaut, le contrôle de la collecte, de l'utilisation et de la divulgation de renseignements personnels incombe aux gestionnaires de programme. Toutefois, en vertu de nombreuses exigences prévues à la Loi, les opérations et la Division de l'AIPRP doivent participer. Dans de tels cas, les responsabilités partagées sont souvent mal comprises. En effet, on croit souvent que la responsabilité de l'un est celle de l'autre, ce qui peut donner lieu à une responsabilisation insuffisante. Cela est peut-être également le fruit de la prolifération des « personnes-ressources en matière de protection des renseignements personnels » au sein du Ministère et à la confusion croissante au sein des directions générales quant aux responsabilités de fond de chaque poste. Au cours de la vérification, les vérificateurs ont identifié pas moins de dix personnes-ressources principales pour les questions liées à la protection des renseignements personnels émanant du fonctionnement des directions générales. Non seulement les rôles et responsabilités de chaque poste n'étaient pas clairs, mais ces postes n'étaient pas dotés en personnel de façon régulière.

La mise en œuvre d'un cadre de gestion de la protection des renseignements personnels approuvé qui définit les rôles et les responsabilités des personnes qui s'occupent de la gestion de la protection des renseignements personnels dans l'ensemble du Ministère et qui la supervisent servira à renforcer les pratiques relatives à la protection des renseignements personnels (voir la recommandation 1).

## Arrêté de délégation

Les délégations en vertu de la *Loi sur la protection des renseignements personnels* varient au sein des institutions fédérales, car elles dépendent de la taille, du mandat et de la culture de l'institution. La délégation se fait entièrement à la discrétion de l'administrateur général et n'a lieu que si elle est considérée comme étant appropriée. Elles précisent que, lorsque le responsable d'une institution décide de déléguer, un arrêté de délégation doit être signé, et les

cadres ou employés à qui sont déléguées les attributions doivent être d'un niveau approprié pour pouvoir assurer la délégation.

Santé Canada dispose d'un arrêté de délégation signé en 2007, en vertu duquel les pouvoirs concernant toutes les responsabilités en matière de protection des renseignements personnels attribuables en vertu de la Loi sont délégués au directeur de l'AIPRP. Le Ministère administre plusieurs lois et programmes comprenant la divulgation de renseignements personnels. Dans chaque cas, les responsables des programmes restent bien informés des considérations contextuelles liées à la collecte, à l'utilisation et à la divulgation de renseignements personnels au sein des secteurs de programme respectifs. De même, tandis que le directeur de l'AIPRP est responsable des divulgations effectuées en vertu du paragraphe 8(2) de la Loi, il n'exerce pas le contrôle sur les renseignements personnels à divulguer. Il existe donc le risque que le Ministère prenne une décision en vertu de la *Loi sur la protection des renseignements personnels* sans bien comprendre et évaluer les risques découlant des exigences juridiques particulières applicables au programme en question. Compte tenu de la quantité de renseignements personnels sous le contrôle de Santé Canada combinée avec le besoin de recueillir et de divulguer couramment de tels renseignements, les nécessités opérationnelles ne permettent pas, du point de vue pratique, la participation directe du directeur de l'AIPRP à toute divulgation. Même si les Services juridiques et la Division de l'AIPRP devraient continuer à jouer un rôle consultatif dans l'application des fonctions déléguées, la responsabilité à l'égard de la protection des renseignements personnels devrait incomber au responsable du programme qui a le contrôle des renseignements personnels en question.

Le Ministère aurait avantage à examiner l'arrêté de délégation à la lumière de l'application des pratiques en matière de protection des renseignements personnels par le personnel des directions générales et étant donné qu'il a été examiné et signé cinq ans plus tôt.

***Recommandation 2***

> *Il est recommandé que le sous-ministre adjoint, Direction générale des services de gestion, examine et mette à jour son arrêté de délégation en vertu de la Loi sur la protection des renseignements personnels de manière à indiquer clairement à qui incombe les responsabilités en matière des responsabilités protection des renseignements personnels*

***Réponse de la direction***

La direction souscrit à la recommandation.

L'arrêté de délégation sera examiné afin de déterminer s'il est nécessaire ou approprié de réaffecter les pouvoirs, les tâches et les fonctions en vertu de la *Loi sur la protection des renseignements personnels.* Si nécessaire, un arrêté de délégation sera mis en place à la suite de l'examen.

# 2. Gestion des risques

## *2.1 Évaluation des facteurs relatifs à la vie privée*

***Critère de vérification :*** *Le Ministère dispose d'un processus efficace d'évaluation des facteurs relatifs à la vie privée pour déterminer, évaluer et atténuer les risques liés à la vie privée dans le contexte des activités nouvelles ou modifiées nécessitant l'utilisation de renseignements personnels.*

Depuis 2002, tous les ministères et organismes sont responsables de déterminer, d'évaluer et d'atténuer les risques relatifs à la vie privée et les répercussions associées aux programmes ou aux activités, nouveaux ou ayant subi des modifications importantes, comportant des renseignements personnels. Les évaluation des facteurs relatifs à la vie privée (ÉFVP) sont le processus de gestion des risques qui permet aux organismes de prévoir et d'analyser les risques liés à la protection de la vie privée inhérents à un programme, à un service ou à une politique proposé. Selon le Commissariat à la protection de la vie privée du Canada, les ÉFVP sont le modèle le plus complet en place pour évaluer les effets d'une initiative particulière de prestation de services sur la protection de la vie privée d'une personne et une composante essentielle du Cadre de gestion de la protection des renseignements personnels du gouvernement fédéral. Le produit final d'une ÉFVP est l'assurance que les questions potentielles relatives à la protection de la vie privée ont été cernées et que des stratégies d'atténuation ont été élaborées.

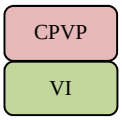
Les ministères doivent avoir en place l'infrastructure nécessaire pour appuyer la réalisation d'ÉFVP proportionnée au niveau de risque d'entrave à la vie privée lié au programme ou à l'activité faisant l'objet d'un examen. Un processus efficace d'ÉFVP devrait inclure ce qui suit : une politique qui éclaire le personnel et d'autres parties prenantes à l'égard de la *Directive sur l'évaluation des facteurs relatifs à la vie privée* et de ses exigences et qui définit officiellement les responsabilités ministérielles en ce qui a trait aux ÉFVP, un système pour signaler efficacement toutes les nouvelles initiatives nécessitant une ÉFVP, un système pour suivre et surveiller la conformité des ÉFVP visées par la *Directive sur l'évaluation des facteurs relatifs à la vie privée* aux exigences en matière de rapports, ainsi que l'engagement des ressources et de l'expertise appropriées pour appuyer les obligations ministérielles relatives aux ÉFVP.

En 2006, Santé Canada a mis en place un processus administratif officiel pour gérer et diriger la réalisation ÉFVP. La Division de l'AIPRP du Ministère a publié une « Boîte à outils des évaluations des facteurs relatifs à la vie privée » qui, entre autres, souligne l'importance des considérations à prendre concernant la protection des renseignements personnels dans le cadre de projets ministériels ainsi que les rôles et les responsabilités liés à la protection des renseignements personnels, décrit le processus des ÉFVP du Ministère et fournit des outils à l'intention du personnel des programmes qui est responsable d'exécuter les ÉFVP. La boîte à outils des évaluations des facteurs relatifs à la vie privée a été mise à jour régulièrement depuis 2006 et plus récemment pour faire refléter les exigences en vertu de la nouvelle Directive du Conseil du secrétariat du Trésor du Canada. Avant cela, le processus en place était arbitraire et informel; il reposait presque exclusivement sur la participation du personnel de l'AIPRP aux activités de sensibilisation en ce qui a trait à la notification de nouvelles initiatives comportant des renseignements personnels. Même si de telles mesures

permettaient, jusqu'à un certain point, à sensibiliser aux répercussions relatives à la protection de la vie privée associées à l'élaboration de systèmes d'envergure, cette activité ne parvenait pas à appuyer pleinement la réalisation d'ÉFVP pour les projets non liés à la technologie de l'information.

En 2007 le Commissariat à la protection de la vie privée a produit le Modèle de maturité des évaluations des facteurs relatifs à la vie privée afin d'établir un repère raisonnable pour l'évaluation des cadres de contrôle de la gestion. À ce moment, Santé Canada était reconnu comme ayant un niveau de maturité 1. Les résultats de la vérification interne indiquent que depuis, le Ministère est passé au niveau 3 – voir la grille ci-dessous.

Statut de l'environnement des ÉFPV de Santé Canada (d'après le modèle de maturité des ÉFPV de 2007 du Commissariat à la protection de la vie privée)




Évaluation de 2007 de la maturité des ÉFVP de Santé Canada (CPVP)
Évaluation de 2012 de la maturité des ÉFVP de Santé Canada (vérification interne)

| NIVEAU DE MATURITÉ | | STATUT DE L'ENVIRONNEMENT DES ÉFVP DE SANTÉ CANADA |
|---|---|---|
| **0** | Inexistant | L'organisme ne reconnaît pas la nécessité de procéder à des évaluations des facteurs relatifs à la vie privée (ÉFVP). La vie privée (y compris le traitement adéquat des renseignements personnels en général) ne fait pas partie de la culture de l'organisme. Le risque de non-conformité à la Politique et de manquements ou d'incidents à l'égard de la protection des renseignements personnels est très grand. Dans un tel environnement, peu d'ÉFVP, s'il en est, sont réalisées en temps opportun. |
| **1** | Initial/aléatoire (CPVP) | L'organisme reconnaît l'existence de la *Directive sur l'ÉFVP* et de la nécessité d'une infrastructure administrative pour gérer le processus d'ÉFVP au sein de l'organisme. L'approche de l'organisation à l'égard du respect des exigences de la Directive est aléatoire et manque de direction officielle, d'orientation ou de supervision de la part de la haute direction. Les irrégularités dans la manière dont les ÉFVP sont réalisées n'ont pas encore été étudiées ni cernées. Les employés ne sont pas sensibilisés à leurs responsabilités tant au sein de leur organisme que par rapport à la mise en œuvre de la Directive dans l'ensemble du gouvernement. Dans un tel environnement, certaines ÉFVP peuvent être réalisées, mais bon nombre ne le sont pas, et la qualité de l'évaluation des facteurs relatifs à la vie privée laisse probablement à désirer. |
| **2** | Reconnu, mais intuitif | L'organisme a mis en place un cadre d'ÉFVP mais il manque parfois des éléments essentiels pour appuyer les objectifs et les exigences de la Politique. Le contrôle du processus d'ÉFVP affiche certaines faiblesses et celles-ci n'ont pas été cernées adéquatement ni soulevées par la direction; les répercussions de telles faiblesses peuvent être importantes. La direction peut ou non être consciente de ses obligations en vertu de la Directive. Les employés peuvent ne pas connaître leurs responsabilités à l'égard du processus d'ÉFVP. La qualité des ÉFVP et la manière dont elles sont réalisées (y compris leur absence) dépendent des connaissances et de la motivation des employés. |

| | | |
|---|---|---|
| **3** | **Processus défini d'ÉFVP (VI)** | L'organisme a mis en place et documenté un processus d'ÉFVP officiel. La direction connaît pleinement ses responsabilités en matière d'ÉFVP et a commencé à appliquer des lignes directrices sur l'ÉFVP à l'ensemble de ses activités. Cependant, le processus n'est pas encore normalisé et le contrôle présente encore des faiblesses. Bien que la direction compose de manière attendue avec la plupart des problèmes de protection de la vie privée qui découlent de ses activités, il reste encore certaines faiblesses dans le processus d'ÉFVP qui pourraient avoir de graves répercussions. Les employés connaissent leurs responsabilités, mais l'organisme manque de ressources nécessaires pour s'acquitter des obligations du Ministère en vertu de la Directive. |
| **4** | Géré et mesurable | L'organisme a mis en place et documenté un processus d'ÉFVP officiel. La direction connaît très bien ses responsabilités en la matière et satisfait aux exigences et aux obligations prévues par la Directive. Les responsabilités et la responsabilisation en vertu de la Directive ont été officiellement définies et la direction et les employés participent de manière proactive à tous les aspects du processus d'ÉFVP. Des programmes sont en place en vue d'informer le personnel et les autres intervenants des objectifs et des exigences de la Directive, et des ressources adéquates ont été affectées pour respecter les obligations du Ministère en vertu de la Directive. Un système efficace d'établissement de rapports concernant tous les nouveaux projets exigeant une ÉFVP a été mis en place. La plupart des ÉFVP sont de grande qualité et réalisées, s'il y a lieu et en temps opportun. |
| **5** | Optimal | L'organisme a intégré l'évaluation des facteurs opérationnels relatifs à la vie privée dans le cadre général de gestion des risques de l'organisme (au centre duquel se trouve un processus officiel d'ÉFVP). Des contrôles effectués à l'échelle de l'organisme assurent une surveillance continue et efficace de la conformité au processus d'ÉFVP de l'organisme et à la Directive du Conseil du Trésor. Une personne ou un organisme est chargé de surveiller le respect de la Politique, et un organisme composé d'employés expérimentés doit examiner les candidats aux ÉFVP et les approuver une fois les évaluations réalisées. L'organisme effectue un suivi du rendement touchant les principaux aspects financiers, opérationnels et des ressources humaines liés aux activités d'ÉFVP et les résultats des ÉFVP sont intégrés à la gestion continue des projets. |

Reconnaissant ces progrès, de nouveaux efforts sont nécessaires pour que le Ministère s'acquitte pleinement de ses obligations en vertu de la nouvelle Directive Les processus d'évaluation des facteurs relatifs à la vie privée varient toujours d'une direction générale à l'autre. Par exemple, des évaluations ne sont pas toujours réalisées et si elles le sont, ce n'est pas suffisamment en temps opportun pour intégrer des considérations relatives à la protection de la vie privée aux programmes nouveaux ou ayant subi des modifications importantes comportant des renseignements personnels. De plus, malgré l'exigence selon laquelle les directions générales obtiennent l'approbation officielle, l'aval ou la signature du directeur de l'AIPRP pour toutes les ÉFVP, la Division de l'AIPRP n'est souvent pas au courant des ÉFVP entreprises par les directions générales ou de la décision de ces dernières de ne pas effectuer une évaluation. La vérification a révélé une bonne pratique de programme au sein de la Direction générale des produits de santé et des aliments qui comprend l'utilisation systématique des ÉFVP pour informer son programme.

**Évaluations des facteurs relatifs à la vie privée • Direction des produits de santé commercialisés – Direction générale des produits de santé et des aliments.**

Au cours des dernières années, la Direction des produits de santé commercialisés de Santé Canada a procédé à plus de huit ÉFVP ou examens relatifs à la protection de la vie privée pour évaluer les répercussions des nouveaux programmes (ou de modifications aux programmes existants) sur la protection de la vie privée comportant des renseignements personnels. Chaque évaluation comprenait une analyse des plans du programme réalisée par des experts par rapport aux exigences relatives à la protection de la vie privée prévues à la *Loi sur la protection des renseignements personnels* et au *Code type sur la protection des renseignements personnels* de CSA. Au moment de la vérification, la Direction tenait un dépôt des ÉFVP et faisait le suivi de l'état des recommandations émises pour atténuer convenablement les questions soulevées relativement à la protection de la vie privée.

Santé Canada pourrait tirer profit de la présence de contrôles internes additionnels tel qu'un processus de dépistage obligatoire et officiel pour déterminer les projets potentiels comportant des renseignements personnels. Les personnes-ressources des directions générales interrogées ont mentionné qu'il n'y avait pas de politiques ou de processus en place pour déterminer toutes les activités nécessitant une ÉFVP. Un processus de dépistage sert de déclencheur pour toute analyse des répercussions sur la protection de la vie privée – il empêche les gestionnaires de programme de bien évaluer la mesure dans laquelle une nouvelle initiative peut présenter des risques relatifs à la protection de la vie privée. Un tel contrôle limiterait les cas d'omissions d'ÉFVP mentionnés dans le cadre de la présente vérification.

***Recommandation 3***

*Il est recommandé que le sous-ministre adjoint, Direction générale des services de gestion, améliore le processus d'Évaluation des facteurs relatifs à la vie privée du Ministère pour qu'il soit mieux harmonisé avec la Directive du Conseil du Trésor.*

***Réponse de la direction***

La direction souscrit à cette recommandation.

La Boîte à outils des évaluations des facteurs relatifs à la vie privée actuelle est en place depuis 2006. Toutefois, elle sera examinée, améliorée et mise à jour pour l'utilisation de Santé Canada et de l'Agence de la santé publique du Canada.

La Direction générale élaborera une stratégie des communications interne pour promouvoir la compréhension de la part des employés du besoin et du processus impliqué quant à la mise au point d'une Évaluation des facteurs relatifs à la vie privée. Dans le cadre de cette stratégie à plusieurs volets, la boîte à outils sera affichée sur le site intranet de Santé Canada.

## *2.2 Sensibilisation et formation*

***Critère de vérification :*** *Le Ministère a un programme de formation et de sensibilisation efficace sur la protection de la vie privée.*

Le gouvernement du Canada (*Politique sur la protection de la vie privée*) attend des administrateurs généraux ou des délégués qu'ils soient responsables de faire connaître aux employés les politiques, les procédures et les obligations légales en vertu de la Loi. À Santé Canada, cette responsabilité incombe au directeur de l'AIPRP.

En octobre 2010, la Division de l'AIPRP a lancé sa Stratégie de sensibilisation à la protection des renseignements personnels. Cette dernière vise à accroître la sensibilisation générale des employés à l'égard de la protection des renseignements personnels et à mieux faire comprendre les pratiques exemplaires en matière de traitement des renseignements personnels dans les secteurs de programme relevés comme étant à risque élevé. La première étape de la stratégie a été mise en œuvre au cours de la période de rapport 2011-2012. La deuxième étape doit être mise en œuvre en 2012-2013.

Le pivot de la formation de Santé Canada en matière de protection des renseignements personnels est son cours « Protection des renseignements personnels 101 ». Le cours, dont la durée varie entre 90 minutes et 2 heures, aborde un large éventail de sujets, surtout les obligations ministérielles aux termes de la Loi et de ses politiques et directives connexes. Le cours vise à fournir aux employés une introduction sur les responsabilités en matière de protection des renseignements personnels aux termes de la Loi. Bien qu'il soit parvenu à sensibiliser les participants à la protection des renseignements personnels, il n'aborde pas en détail les exigences ministérielles liées à l'évaluation des facteurs relatifs à la vie privée, aux protocoles dans le cadre d'une atteinte à la vie privée ou à l'enregistrement et à la mise à jour des fichiers de renseignements personnels à Santé Canada. Depuis l'automne 2010, le cours a été offert régulièrement de septembre à mai. Dorénavant, la Division de l'AIPRP a l'intention de l'offrir tout au long de l'année.

En plus du cours « Protection des renseignements personnels 101 », la Division de l'AIPRP offre également aux secteurs de programme qui en font la demande une formation personnalisée sur la protection des renseignements personnels. Dans un tel cas, le cours « Protection des renseignements personnels 101 » est adapté au secteur de programme visé. Ce dernier est également offert annuellement à des groupes ciblés déterminés par le Comité exécutif des services internes du Ministère. Bien que l'on dise que l'orientation des employés comprend une formation de quinze minutes sur la protection des renseignements personnels par le biais du « Programme de responsabilisation à l'égard de la gestion de l'information », lorsque cette formation est offerte, elle ne porte que sur le traitement confidentiel des renseignements personnels et non sur les responsabilités plus générales des employés fédéraux à cet égard aux termes de la Loi. Bien que Santé Canada dispose également d'un outil d'apprentissage en ligne relatif à la protection des renseignements personnels, la Division de l'AIPRP ignore le taux de participation au programme ou sa popularité.

Pour l'exercice se terminant en 2012, la Division de l'AIPRP déclare avoir donné à 3 122 employés de Santé Canada (ou environ 29 pourcent des équivalents temps plein du

Ministère) une formation de sensibilisation à la protection des renseignements personnels soulignant l'importance de protéger ces derniers. Ce nombre inclut les 896 employés de Santé Canada à l'échelle du pays qui ont suivi le cours « Protection des renseignements personnels 101 ». Ce résultat est louable compte tenu des ressources limitées consacrées à la prestation de formation sur la protection des renseignements personnels. En dépit de l'élan que la Stratégie de sensibilisation à la protection des renseignements personnels du Ministère a généré à l'égard de la formation, la formation actuelle sur la protection des renseignements personnels dispensée au sein de Santé Canada est parfois sporadique. Par exemple, dans le but de fournir une telle formation dans les régions éloignées du pays considérées comme étant à « risque élevé », la Division de l'AIPRP a mis son programme de formation sur des disques compacts qui sont expédiés à diverses collectivités. Pourtant, les entrevues ont révélé que la participation à la formation n'est pas claire. La Division de l'AIPRP aurait eu avantage à faire un suivi après l'envoi des trousses de formation pour déterminer si la formation a été dispensée.

Lorsque les employés possèdent des connaissances à l'égard de la protection des renseignements personnels, il semble qu'elles aient été acquises auprès d'autres employés, à partir de sources anecdotiques ou par l'expérience avec d'autres questions ministérielles liées à la protection des renseignements personnels. Il a été démontré que lorsque des programmes individuels ont pris l'initiative de financer des ressources particulières affectées à la formation sur ce sujet, le secteur de programme a été en mesure de promouvoir les pratiques en matière de protection des renseignements personnels.

**Formation sur la protection des renseignements personnels • Division de l'accès à la marihuana (Direction générale de la santé environnementale et de la sécurité des consommateurs)**

En octobre 2010, le Programme d'accès à la marihuana à des fins médicales de Santé Canada a été identifiée comme étant un secteur de programme pouvant poser un risque élevé relativement à la protection des renseignements personnels. Reconnaissant le besoin que les employés de première ligne et les gestionnaires soient davantage sensibilisés à la protection des renseignements personnels, le Programme a depuis dispensé une formation spéciale à cet égard à tout son personnel sans exception. Non seulement la formation (donnée par la Division de l'AIPRP) a-t-elle accru la sensibilisation des parties prenantes à l'égard de ce sujet, elle a également donné lieu à l'amélioration des pratiques concernant la collecte, l'utilisation et la divulgation des renseignements personnels.

En conclusion, bien qu'il existe, au sein du Ministère et dans l'ensemble des directions générales, une solide culture de confidentialité et une sensibilisation générale au besoin de protéger les renseignements personnels, les exigences particulières relatives au traitement des renseignements personnels (en particulier chez le personnel de première ligne) sont moins bien comprises. Les données empiriques recueillies dans le cadre de la vérification semblent indiquer que les employés ont une compréhension limitée de ce qui constitue des renseignements personnels aux termes de la Loi et une compréhension très superficielle de leurs responsabilités à l'égard de la collecte, de l'utilisation et de la divulgation des renseignements personnels.

***Recommandation 4***

*Il est recommandé que le sous-ministre adjoint, Direction générale des services de gestion, améliore la stratégie de sensibilisation et de formation à l'égard de la protection des renseignements personnels en établissant des exigences de formation particulières à l'intention des employés de Santé Canada qui participent le plus activement au traitement de renseignements personnels.*

***Réponse de la direction***

La direction souscrit à cette recommandation.

Une stratégie complète sur la sensibilisation à la protection des renseignements personnels sera élaborée et celle-ci identifiera des exigences de formation pour les employés de Santé Canada et de l'Agence de la santé publique du Canada qui participent le plus activement au traitement des renseignements personnels.

# 3. Contrôle interne

## *3.1 Avis*

***Critère de vérification :*** *Le Ministère a établi des contrôles pour informer les personnes dont les renseignements personnels sont recueillis des fins de la collecte, sauf pour les exceptions prévues par la loi.*

En vertu du paragraphe 5(2) de la *Loi sur la protection des renseignements personnels*, une institution fédérale est tenue d'informer l'individu auprès de qui elle recueille des renseignements personnels des fins auxquelles ils sont destinés. L'institution peut ne pas être tenue d'informer l'individu dans des circonstances particulières, c'est-à-dire lorsque le fait d'indiquer le but de la collecte risquerait d'avoir pour résultat la collecte de renseignements inexacts ou de compromettre l'usage auxquels les renseignements sont destinés. L'exigence selon laquelle une institution informe un individu du but de la collecte s'applique également à la collecte indirecte effectuée par un tiers.

En veillant à ce que les ministères avisent dûment les personnes des fins auxquelles les renseignements personnels sont recueillis, le Secrétariat du Conseil du Trésor du Canada a émis des lignes directrices concernant la notification. En vertu de la section 6.2.9 de la *Directive sur les pratiques relatives à la protection de la vie privée*, les ministères doivent aviser l'individu, dont les renseignements personnels font l'objet d'une collecte directe, des éléments suivants :

1) La raison d'être de la collecte et l'autorisation obtenue pour la collecte
2) Toute utilisation ou divulgation conforme à la raison d'être originale
3) Toute utilisation ou divulgation non conforme à la raison d'être originale
4) Toute conséquence administrative ou légale découlant d'un refus de fournir les renseignements personnels

5) Le droit d'accéder et de demander des corrections à ses renseignements personnels et le droit de leur protection en vertu de la Loi

En vertu de son large mandat concernant les soins de santé, la recherche, la politique et l'application de la loi, Santé Canada utilise des centaines de formulaires différents pour recueillir des renseignements personnels. Dans bien des cas, les formulaires utilisés à cette fin sont désuets, certains remontant avant l'entrée en vigueur de la Loi. D'autres, bien qu'ils soient plus à jour, n'ont pas fait l'objet d'une révision depuis un certain temps et ce, malgré les changements importants aux programmes auxquels ils se rapportent et aux exigences de ces derniers en matière de renseignements personnels. En se fondant sur l'examen d'un échantillon de formulaires de certaines directions générales servant à la collecte de renseignements personnels, le Ministère aura avantage à examiner ses formulaires, sous l'orientation du directeur de l'AIPRP, afin de respecter les dispositions prévues à la Loi et à sa directive connexe.

***Recommandation 5***

*Il est recommandé que le sous-ministre adjoint, Direction générale des services de gestion, collabore avec les autres directions générales pour coordonner l'examen des formulaires qu'utilisent les directions opérationnelles pour recueillir des renseignements personnels afin de respecter la disposition relative à l'avis prévue à la Loi et à la Directive sur les pratiques relatives à la protection de la vie privée.*

***Réponse de la direction***

La direction souscrit à cette recommandation.

La Division de l'accès à l'information et de la protection des renseignements personnels examinera, conjointement avec la direction générale convenable, les formulaires identifiés dans le cadre de cette vérification comme étant non conformes aux dispositions de la Loi relatives à l'avis afin d'identifier si des modifications doivent être effectuées.

Un examen sera effectué pour tous les formulaires du Ministère utilisés pour la collecte des renseignements personnels pour assurer que les directions générales correspondantes sont au courant des exigences et qu'elle effectuent des modifications, le cas échéant

## *3.2 Collecte, utilisation, divulgation et conservation*

***Critère de vérification :*** *Le Ministère a établi des contrôles pour limiter la collecte, l'utilisation, la divulgation et la conservation de renseignements personnels à ceux prévus par la loi.*

Conformément à l'article 4 de la *Loi sur la protection des renseignements personnels*, un ministère/organisme ne peut recueillir des renseignements personnels que s'ils ont un lien direct avec ses programmes ou ses activités. Les institutions fédérales doivent limiter leur collecte de renseignements personnels seulement à ceux qui sont manifestement nécessaires. Des restrictions similaires s'appliquent à *l'utilisation* et à la *divulgation* de renseignements

personnels par les institutions fédérales lorsque ces derniers ne peuvent être utilisés ou divulgués qu'aux fins auxquelles ils sont destinés, sauf si l'individu a donné son consentement (ou dans des cas exceptionnels sans le consentement de ce dernier). Bien que les périodes de conservation des renseignements personnels varient d'un programme à l'autre ainsi qu'au niveau des règlements applicables qui se rapportent à ces programmes, le paragraphe 6(1) de la Loi exige que les renseignements personnels utilisés à des fins administratives soient conservés après usage pendant une période suffisamment longue pour permettre à l'individu d'exercer son droit d'accès à ces renseignements.

Pour limiter sa collecte, l'utilisation, la divulgation et la conservation de renseignements personnels, le Ministère est tenu de disposer de contrôles administratifs appropriés pour gérer et surveiller ses fonds de renseignements personnels. La vérification a toutefois révélé l'absence de contrôles officiels et documentés relatifs à la collecte, à l'utilisation, à la divulgation et à la conservation des renseignements personnels, ce qui n'est pas conforme à la Loi. Dans la plupart des cas, les secteurs de programme reposent sur des procédures opératoires normalisées, en fonction des lois et règlements d'application, pour régir la collecte et l'utilisation de renseignements personnels. Parfois, ces procédures opératoires normalisées comprennent des dispositions concernant la protection de la vie privée ou le bon traitement des renseignements personnels. D'autres fois, les procédures opératoires normalisées et les lignes directrices relatives au traitement des renseignements personnels ne fournissent pas assez d'information au personnel de première ligne quant aux exigences de la Loi concernant le traitement des renseignements personnels. Malgré ces conclusions, la vérification a permis d'observer deux bonnes pratiques chez la Direction générale de la santé des Premières nations et des Inuits qui démontrent que la direction générale participe grandement à la protection des renseignements personnels.

**Un Code de protection des renseignements personnels disponible publiquement • Services de santé non assurés (DGSPNI)**

Dans le but d'encourager le traitement équitable, transparent et uniforme des renseignements personnels, le Programme des services de santé non assurés (SSNA) a rendu public son engagement à assurer la confidentialité des données qu'il recueille et utilise dans le cadre de son exécution en créant un « Code de protection des renseignements personnels » officiel. Ce Code s'applique à tous les employés du Programme des SSNA, ainsi qu'à tous les individus, groupes ou organismes qui recueillent, utilisent ou divulguent des renseignements personnels, ou qui y ont accès, pour gérer les services de santé non assurés. En plus d'aider à s'assurer que le Programme demeure conforme à la *Loi sur la protection des renseignements personnels*, le Code de protection des renseignements personnels témoigne d'un engagement résolu envers la protection des renseignements personnels des collectivités des Premières nations et de ceux des personnes pour lesquels le Programme a le contrôle.

**Guides sur le partage des renseignements personnels à l'intention du personnel infirmier • Services internes à la clientèle (DGSPNI)**

Dans le cadre de la prestation de soins de santé primaires, il est souvent indispensable de partager des renseignements personnels. Souvent, la prestation de soins appropriés et opportuns nécessite que des renseignements personnels sur la santé soient divulgués à des spécialistes du « cercle de soins » d'un patient ou à d'autres personnes ayant un besoin légitime d'accéder à de tels renseignements personnels dans des cas limités et très particuliers. Pour divulguer des renseignements personnels, le cas échéant, sans oublier le besoin de concilier le droit au respect des renseignements personnels d'une personne et les besoins légitimes des autres pour ce qui est de recueillir, d'utiliser et de divulguer des renseignements personnels sur la santé dans le cadre de la prestation de soins de santé primaires, la DGSPNI a élaboré des procédures opératoires normalisées relatives à la divulgation des renseignements personnels. Ces procédures, élaborées en consultation avec les Services juridiques et la Division de l'AIPRP, fournissent aux employés de première ligne une référence rapide quant à la façon et au moment où des renseignements personnels peuvent être partagés et aux mesures à prendre pour protéger la vie privée des patients.

En plus de procédures opératoires normalisées et de protocoles documentés relativement au traitement des renseignements personnels, on dit que Santé Canada se réfère à la réglementation provinciale régissant la conduite des professionnels de la santé provinciaux pour obtenir une assurance à l'égard des pratiques des dispensateurs de soins médicaux en matière de traitement des renseignements personnels (particulièrement lors de la prestation de soins de santé aux populations des Inuits et des Premières nations).

Toutefois, l'analyse d'échantillon de tels instruments indique qu'ils ne sont pas équivalents à ce qui est prévu à la *Loi sur la protection des renseignements personnels*. Dans certains cas, les obligations professionnelles et éthiques d'un professionnel de la santé peuvent entrer en conflit avec des lois fédérales relatives à la protection des renseignements personnels. Ainsi, le fait que le programme repose sur des lignes directrices concernant les pratiques professionnelles (ou les politiques provinciales régissant les professionnels de la santé) peut ne pas suffire pour que Santé Canada respecte ses obligations prévues à la Loi relativement au traitement des renseignements personnels.

***Recommandation 6***

*Il est recommandé que le sous-ministre adjoint, Direction générale des services de gestion, collabore avec les autres directions générales pour coordonner l'examen et la mise à jour des procédures opératoires normalisées, des lignes directrices et des protocoles du Programme afin de renforcer les contrôles relatifs à la collecte, à l'utilisation, à la divulgation et à la conservation des renseignements personnels.*

***Réponse de la direction***

La direction souscrit à cette recommandation.

Des lignes directrices pour la collecte de renseignements personnels seront émises par la Division de l'accès à l'information et de la protection des renseignements personnels.

Un échantillon de procédures et protocoles du programme sera examiné par la Division de l'accès à l'information et de la protection des renseignements personnels à l'intérieur de l'année suivant la publication des lignes directrices susmentionnées pour assurer que la collecte des renseignements personnels est menée en conformité à celles-ci.

## *3.3 Exactitude*

***Critère de vérification :*** *Le Ministère a établi des contrôles pour appuyer la collecte de renseignements exacts, complets et à jour utilisés pour prendre des décisions administratives à l'égard d'un individu.*

Conformément au paragraphe 5(2) de la Loi sur la protection des renseignements personnels, les institutions fédérales sont tenues de prendre toutes les mesures raisonnables pour que les renseignements personnels qu'elles utilisent à des fins administratives soient à jour, exacts et complets. Ces mesures raisonnables doivent comprendre l'une ou plusieurs des mesures administratives suivantes :

- Collecte ou validation directe auprès de l'individu;
- collecte ou validation indirecte pouvant comporter la vérification des renseignements personnels auprès d'une source fiable (publique ou privée), lorsque cette action est autorisée ou que le consentement approprié a été obtenu;
- mesures technologiques permettant de détecter les erreurs et les divergences.

En plus de ce qui est susmentionné, les institutions fédérales doivent donner aux individus, dans le mesure du possible, l'occasion de corriger tout renseignement inexact les concernant avant la prise de toute décision à leur endroit qui pourrait avoir une incidence sur leur réputation ou leur admissibilité à des programmes ou à des services gouvernementaux.

Dans le cadre de l'exécution de ses programmes et de la prestation de ses services, Santé Canada repose à la fois sur la collecte directe et indirecte de renseignements personnels. Lorsque les renseignements personnels font l'objet d'une collecte directe, le Ministère repose sur des formulaires types qui sont conservés pendant une période suffisante permettant la mise à jour ou la correction de renseignements inexacts. Lorsque les renseignements personnels font l'objet d'une collecte indirecte, le Ministère repose sur des dispositions contractuelles et des mécanismes de consentement pour confirmer l'exactitude des renseignements recueillis et utilisés à des fins administratives. Dans certains cas, les procédures opératoires normalisées de programmes encouragent la vérification des renseignements personnels avant de les utiliser (voir la recommandation 6). La Division de

l'AIPRP offre aux individus l'accès aux renseignements personnels, ainsi que la capacité de les mettre à jour et de les corriger.

La vérification n'a révélé aucun cas où les renseignements personnels qu'utilise le Ministère étaient jugés inexacts ou incomplets. Pour les deux années se terminant en 2012, Santé Canada n'a reçu aucune plainte ou n'a fait aucune enquête concernant des renseignements inexacts.

## *3.4 Mesures de protection*

***Critère de vérification :*** *Le Ministère a établi des contrôles pour protéger les renseignements personnels sous son contrôle contre leur utilisation ou divulgation non autorisée.*

La *Politique sur la sécurité du gouvernement* du gouvernement du Canada prévoit des mesures de protection relativement à l'utilisation et à la divulgation de renseignements personnels. Elle contient une exigence selon laquelle les renseignements personnels doivent être protégés par des mesures de sécurité adaptées à leur degré de sensibilité. D'autres dispositions régissant la protection des renseignements personnels sont stipulées dans la *Directive sur les pratiques relatives à la protection de la vie privée* du Secrétariat du Conseil du Trésor du Canada.

Bien que les protocoles de sécurité concernant les renseignements personnels varient selon la sensibilité des renseignements à risque, Santé Canada utilise généralement les moyens suivants pour protéger les données personnelles : des mesures physiques (par exemple, des classeurs verrouillés et un accès restreint aux bureaux), des mesures organisationnelles (par exemple, des enquêtes de sécurité et le partage limité des renseignements personnels, le principe du « besoin d'en connaître ») et des mesures technologiques (au moyen de mots de passe et du cryptage pour les systèmes contenant des renseignements personnels).

Des représentants de la Division de la gestion de la sécurité et des mesures d'urgence du Ministère et des agents de sécurité régionaux choisis ont été interrogés et l'équipe de vérification a procédé à l'examen des résultats et des actions à ce jour de deux vérifications récentes clés portant sur les risques liés à la sécurité de l'information – la *Vérification de la sécurité des technologies de l'information* de 2010 et la *Vérification de la gestion de l'information* de 2009. Enfin, les vérificateurs ont visité des installations choisies où des renseignements personnels sont conservés afin de déterminer le degré de sécurité physique des données.

Dans l'ensemble, Santé Canada dispose de contrôles appropriés pour protéger les renseignements personnels sous son contrôle contre leur utilisation et divulgation non autorisée. Toutefois, des questions relatives aux contrôles d'accès et à la surveillance des contrôles soulevées lors de vérifications récentes nécessitent toujours l'attention de la direction. Cette position est appuyée par les travaux de la Division de la gestion de la sécurité et des mesures d'urgence qui, par le biais du Plan de sécurité de Santé Canada, comprend des plans visant à protéger davantage les renseignements personnels. Lors de la *Vérification de la sécurité des technologies de l'information,* il a été mentionné que le réseau de Santé Canada était séparé en deux zones alors que le nombre minimum de zones recommandé est de quatre

qui sont habituellement associées à un réseau classé au niveau « Protégé B ». Depuis lors, le Ministère, en collaboration avec Services partagés Canada, a pris des mesures pour accroître sa posture de sécurité (faire passer le réseau à un niveau « Protégé B ») afin de mieux servir ses clients opérationnels de Santé Canada.

# C - Conclusion

La mise en œuvre de politiques et de lignes directrices gouvernementales visant à appuyer l'administration de la *Loi sur la protection des renseignements personnels* remonte à plus de dix ans. Santé Canada a clairement réalisé des progrès quant à l'application de ces politiques et directives (passant d'un niveau de maturité 1 à un niveau 3 sur le modèle de maturité des évaluations des facteurs relatifs à la vie privée) toutefois, du travail supplémentaire serait avantageux pour certains domaines.

Plus particulièrement, le Ministère tirera avantage d'un cadre centralisé et uniforme relatif à la gestion des pratiques de protection des renseignements personnels dans l'ensemble des directions générales. De plus, les rôles et responsabilités à l'égard de la protection des renseignements personnels doivent être plus clairement définis; il doit y avoir une meilleure intégration des résultats des évaluations des facteurs relatifs à la vie privée au processus décisionnel stratégique et à d'autres processus de gestion des risques et finalement, on doit offrir de la formation aux employés travaillant avec des renseignements personnels.

Au cours des deux dernières années, l'AIPRP a déployé d'importants efforts pour promouvoir la sensibilisation à la protection des renseignements personnels dans l'ensemble du Ministère. Il faut toutefois déployer des efforts supplémentaires pour que cette sensibilisation se traduise par de bonnes pratiques de protection des renseignements personnels dans l'ensemble du Ministère.

# Annexe A – Champs d'enquête et critères particuliers

| Vérification des pratiques de Santé Canada en matière de renseignements personnels | | |
|---|---|---|
| **Titre du critère** | | **Critère de vérification** |
| **Champ d'enquête 1 : *Gouvernance*** | | |
| 1.1 | Cadre de gestion de la protection des renseignements personnels | Le Ministère a élaboré et mis en œuvre un cadre de gestion de la protection des renseignements personnels pour appuyer la gestion et la surveillance des pratiques de gestion des renseignements personnels à l'échelle ministérielle. |
| 1.2 | Rôles et responsabilités | Le Ministère a désigné une ou des personnes qui doivent s'assurer que l'institution respecte la *Loi sur la protection des renseignements personnels*, les politiques et directives. Les rôles et les responsabilités liés à la protection des renseignements personnels sont compris et attribués de façon appropriée. |
| **Champ d'enquête 2 : *Gestion des risques*** | | |
| 2.1 | Évaluation des facteurs relatifs à la vie privée | Le Ministère dispose d'un processus efficace d'évaluation des facteurs relatifs à la vie privée pour déterminer, évaluer et atténuer les risques liés à la vie privée dans le contexte des activités nouvelles ou modifiées nécessitant l'utilisation de renseignements personnels. |
| 2.2 | Sensibilisation et formation | Le Ministère a un programme de formation et de sensibilisation efficace sur la protection de la vie privée. |
| **Champ d'enquête 3 : *Contrôle interne*** | | |
| 3.1 | Avis | Le Ministère a établi des contrôles pour informer les personnes dont les renseignements personnels sont recueillis des fins de collecte, sauf pour les exceptions prévues par la loi. |
| 3.2 | Collecte, utilisation, divulgation et conservation | Le Ministère a établi des contrôles pour limiter la collecte, l'utilisation, la divulgation et la conservation de renseignements personnels à ceux prévus par la loi. |
| 3.3 | Exactitude | Le Ministère a établi des contrôles pour appuyer la collecte des renseignements exacts, complets et à jour utilisés pour prendre des décisions administratives à l'égard d'un individu. |
| 3.4 | Mesures de protection | Le Ministère a établi des contrôles pour protéger les renseignements personnels sous son contrôle contre leur utilisation ou divulgation non autorisée. |

# Annexe B – Grille d'évaluation

| Critère | Cote | Conclusion | Nº de la rec. |
|---|---|---|---|
| **Gouvernance** | | | |
| 1.1 Cadre de gestion de la protection des renseignements personnels | **AMO** | Le Ministère travaille afin d'avoir un cadre de gestion de la protection des renseignements personnels pour appuyer la gestion et la surveillance des pratiques de gestion des renseignements personnels dans l'ensemble des directions générales. | 1 |
| 1.2 Rôles et responsabilités | **AMO** | Les rôles et responsabilités concernant la gestion et le traitement des renseignements personnels ne sont pas clairs. Les responsabilités désignées pour s'assurer que l'institution respecte la *Loi sur la protection des renseignements personnels* ne sont peut-être pas attribuées de façon appropriée. | 2 |
| **Gestion des risques** | | | |
| 2.1 Évaluation des facteurs relatifs à la vie privée | **AMO** | Le Ministère a réalisé d'importants progrès pour ce qui est d'améliorer ses pratiques relatives aux évaluations des facteurs relatifs à la vie privée (ÉFVP), mais de nouveaux efforts sont nécessaires pour qu'il s'acquitte pleinement de ses obligations en vertu de la *Directive sur l'ÉVFP*. | 3 |
| 2.2 Sensibilisation et formation | **AMO** | Le Programme de formation et de sensibilisation du Ministère à l'égard de la protection des renseignements personnels s'est beaucoup amélioré au cours des deux dernières années, mais il pourrait tirer profit d'un examen stratégique. La formation n'est pas intégrée à l'orientation des employés et devrait être donnée à tout le personnel qui participe à la gestion et au traitement des renseignements personnels. | 4 |
| **Contrôle interne** | | | |
| 3.1 Avis | **AMO** | Les formulaires qu'utilise Santé Canada pour recueillir des renseignements personnels ne satisfont pas tous aux dispositions concernant l'avis prévues à la *Loi*. | 5 |
| 3.2 Collecte, utilisation, divulgation et conservation | **AMO** | Il faut examiner et mettre à jour les procédures opératoires normalisées, les lignes directrices et les protocoles utilisés pour contrôler et limiter la collecte, l'utilisation, la divulgation et la conservation de renseignements personnels. | 6 |
| 3.3 Exactitude | **S** | La vérification n'a révélé aucun cas où les renseignements personnels qu'utilise le Ministère étaient jugés inexacts ou incomplets. | |
| 3.4 Mesures de protection | **AMI** | Santé Canada dispose de contrôles adéquats pour protéger les renseignements personnels sous son contrôle contre leur utilisation et divulgation non autorisée. | |

| S | AMI | AMO | AR | I | IIM |
|---|---|---|---|---|---|
| Satisfaisant | Améliorations mineures requises | Améliorations modérées requises | Améliorations requises | Insatisfaisant | Inconnu ou impossible à mesurer |