LIGNES DIRECTRICES SUR LA MISE EN OEUVRE D'UN PROGRAMME DE GESTION DE LA PROTECTION DE LA VIE PRIVÉE

Pour favoriser la responsabilité du secteur public du Manitoba à l'égard de la protection de la vie privée

TABLE DES MATIÈRES

Ombudsman du Manitoba

www.ombudsman.mb.ca | ombudsman@ombudsman.mb.ca | 1 800 665-0531 | 204 982-9130

INTRODUCTION

Gestion responsable de la protection de la vie privée

Le présent document explique en détail aux organismes publics et aux dépositaires comment mettre en œuvre un programme efficace et responsable de gestion de la protection de la vie privée. Dans le domaine de la protection de la vie privée, on entend par responsabilité le fait d'accepter et de démontrer le devoir de protéger les renseignements (médicaux) personnels. Cela signifie qu'il faut se doter de politiques, de procédures et de pratiques qui respectent la Loi sur l'accès à l'information et la protection de la vie privée (LAIPVP) et la Loi sur les renseignements médicaux personnels (LRMP). De même, certains organismes publics et dépositaires sont parfois assujettis à d'autres lois comportant des dispositions sur la protection des renseignements (médicaux) personnels. Un programme de gestion de la protection de la vie privée fait en sorte que la confidentialité des renseignements fasse partie intégrante de toutes les initiatives et de tous les programmes ou services.

Les Manitobains et Manitobaines confient leurs renseignements, notamment des renseignements de nature très délicate, à des organismes publics et à des dépositaires pour pouvoir bénéficier de services, de programmes et d'avantages. Il est donc essentiel d'assurer la gestion responsable de ces renseignements pour obtenir et maintenir la confiance des citoyens. Il est important également que les mesures d'une organisation visant à protéger ces renseignements soient transparentes et que le public puisse s'informer clairement sur le programme de gestion de la protection de la vie privée de l'organisation en question.

Le fait de disposer d'un programme de gestion de la protection de la vie privée aide les organismes à respecter leurs obligations législatives dans ce domaine. Notre bureau se servira de ces lignes directrices dans ses enquêtes pour trouver des signes de gestion responsable en matière de protection de la vie privée.

Pour rester pratiques et efficaces, les programmes de gestion de la protection de la vie privée doivent s'adapter aux changements qui s'opèrent dans les services, dans les structures administratives et dans les textes législatifs applicables. Les organisations doivent donc constamment examiner et réviser leurs programmes et faire en sorte que la gestion de la protection de la vie privée fasse partie intégrante de leurs activités régulières.

Les organisations varient de par leur taille, leur mandat et leurs fonctions. Le volume, le type et la nature délicate des renseignements (médicaux) personnels qu'elles recueillent et ce qu'elles en font varient grandement aussi. Par conséquent, les programmes de gestion de la protection de la vie privée doivent être conçus et adaptés en fonction des besoins de chaque organisation.

Le présent document fournit un cadre évolutif que toutes les organisations peuvent utiliser pour mettre en œuvre un programme de gestion de la protection de la vie privée composé des éléments suivants :

- **A. Engagement de l'organisation**
- **B. Mesures de contrôle du programme**
- **C. Évaluation continue et révision**

Pour commencer : Étapes à suivre pour la mise en place d'un programme de gestion de la protection de la vie privée

Avant de concevoir un programme de gestion de la protection de la vie privée, l'organisation doit d'abord évaluer les pratiques qu'elle a déjà en place pour respecter ses obligations en matière de confidentialité des renseignements. Cela lui permet de déterminer les lacunes et d'élaborer un plan d'action pour appliquer tout élément manquant d'un programme de gestion. L'annexe, intitulée Programme de gestion de la protection de la vie privée en bref, décrit les composantes du programme et vise à faciliter le processus d'évaluation.

Voici les étapes dont il faut tenir compte pour évaluer et mettre en œuvre un programme :

1. Nommer une personne responsable suffisamment au courant des questions de protection de la vie privée et ayant l'autorité nécessaire pour évaluer la conformité de l'organisation par rapport à ses obligations dans le cadre de la LAIPVP et de la LRMP, et pour examiner et documenter les pratiques existantes de gestion de la protection de la vie privée (cela pourrait être le fonctionnaire chargé de la protection des renseignements médicaux personnels ou bien l'agent ou le coordonnateur de l'accès à l'information et de la protection de la vie privée).

2. Veiller à ce que la haute direction surveille l'évaluation du programme de gestion, par l'intermédiaire de la personne responsable.

3. En fonction de la taille de l'organisation et de la complexité des systèmes d'information, la personne responsable peut aussi former un groupe de travail ou un comité chargé de procéder à l'évaluation.

4. Dans la mesure du possible, faire participer le personnel chargé de la gestion de l'information ou des dossiers, de la technologie de l'information (TI), de la sécurité des renseignements, de la gestion des risques, de la vérification interne et des ressources humaines.

5. Au besoin, faire appel aux services de professionnels externes spécialisés en protection de la vie privée.

6. Obtenir et consigner les renseignements nécessaires pour évaluer la conformité, notamment en procédant à des entrevues avec le personnel, en examinant les dossiers, les systèmes de TI et les politiques.

7. Remettre des rapports de situation à la haute direction en y incluant les problèmes éventuels de conformité.

8. Remettre un rapport définitif à la haute direction incluant une évaluation de la conformité à la LAIPVP et(ou) à la LRMP ainsi qu'une description des éléments manquants ou inadéquats du programme de gestion de la protection de la vie privée.

9. Prendre toute autre mesure susceptible d'aider l'organisation à documenter sa situation courante en matière de conformité, à déterminer les lacunes et à décider des mesures à prendre.

10. Élaborer un plan d'action pour remédier aux lacunes éventuelles du programme de gestion de la protection de la vie privée.

A. ENGAGEMENT DE L'ORGANISATION

L'engagement de l'organisation à l'égard de la protection de la vie privée est à la base de tout programme de gestion de la protection de la vie privée. Il est visible lorsque l'organisation accorde la priorité au respect de la LAIPVP et(ou) de la LRMP et qu'elle favorise une culture respectueuse de la vie privée. Il consiste aussi à assumer la responsabilité de protéger et de gérer convenablement les renseignements (médicaux) personnels.

L'engagement de l'organisation sous-entend :

1. **L'appui et le soutien réels de la haute direction**
2. **La désignation d'un agent habilité qui est responsable de la protection de la vie privée**
3. **La mise en place de mécanismes pour la production de rapports de conformité**

1. Engagement et appui confirmés de la haute direction

L'appui et le soutien de la haute direction sont essentiels à la réussite d'un programme de gestion de la protection de la vie privée. La haute direction doit entériner les mesures de contrôle du programme, appuyer le rôle de l'agent responsable de la protection de la vie privée et fournir les ressources nécessaires au bon fonctionnement du programme. Il est important d'avoir des processus en place pour qu'elle reste informée de la conformité de l'organisation en matière de protection de la vie privée.

2. Désignation et responsabilisation d'un agent chargé de la protection de la vie privée

Il est essentiel de nommer au sein de l'organisation une personne responsable de la conformité et des pratiques liées à la protection de la vie privée, et notamment que cette personne soit chargée de la gestion et de l'orientation du programme de gestion de la protection de la vie privée.

Il est important d'affecter des ressources suffisantes. Dans certaines organisations, l'agent responsable de la protection de la vie privée est également chargé de l'accès à l'information et d'autres tâches. Dans les grandes organisations, il a parfois besoin du soutien d'autres employés et cela peut mener à la création d'un bureau de la protection de la vie privée ou d'un bureau de l'accès à l'information et de la protection de la vie privée.

Chaque organisation doit évaluer les ressources qui lui sont nécessaires pour être conforme à la législation et avoir en place de bonnes pratiques. Cela peut se faire dans le cadre de l'évaluation initiale et de la conception du programme de gestion de la protection de la vie privée, en affectant les ressources et le personnel nécessaires à la mise en place du programme lorsque celui-ci est approuvé.

La personne à qui le « responsable », au sens de la LAIPVP, a délégué la responsabilité serait chargée de veiller à l'observation de la LAIPVP. Elle pourrait également être chargée de l'observation de la LRMP pour ce qui est des renseignements médicaux personnels. En vertu de la LRMP, les établissements de soins de santé et les organismes de services de santé sont tenus de nommer un fonctionnaire chargé de la protection des renseignements médicaux personnels.

Le rôle de l'agent chargé de la protection de la vie privée (ou de l'agent ou coordonnateur de l'accès à l'information et de la protection de la vie privée) inclut généralement ce qui suit :

- établir et appliquer les mesures de contrôle du programme, notamment élaborer les procédures et les politiques relatives à la protection de la vie privée, et concevoir et mettre en œuvre un programme de formation pour les employés
- évaluer les mesures du contrôle du programme de façon continue et les réviser
- représenter l'organisation en cas d'enquête par l'Ombudsman du Manitoba
- faire preuve de leadership au sein de l'organisation en créant et en faisant la promotion d'une culture respectueuse de la vie privée

Le rôle de cet agent doit être clairement communiqué dans toute l'organisation et être appuyé par la haute direction.

3. Adoption de mécanismes de production de rapports de conformité

Un programme de gestion de la protection de la vie privée doit intégrer divers types de mécanismes de production de rapports qui se reflètent dans ses mesures de contrôle. Cela permet de veiller à ce que l'agent et la haute direction soient régulièrement informés et sachent si le programme fonctionne comme prévu et, dans le cas contraire, quels sont les remèdes proposés.

Un examen interne ou un processus de vérification est un mécanisme essentiel pour la production de rapports de conformité. Il faut donc prévoir une forme quelconque d'examen ou de vérification pour surveiller la conformité des politiques et des procédures de l'organisation en matière de protection de la vie privée et en faire rapport. L'examen ou la vérification peut aussi se produire à la suite d'une atteinte à la vie privée. Les résultats de ces examens ou vérifications doivent être communiqués à la haute direction.

Il faut prévoir un autre mécanisme redditionnel dans les situations où il est nécessaire de transmettre certaines questions à un échelon supérieur, par exemple en cas d'atteinte à la vie privée ou de plainte d'un particulier. Le processus nécessite la participation de personnes compétentes au sein de l'organisation et l'assurance que tout le personnel nécessaire participe à la résolution de la situation. En établissant des procédures de signalement pour les employés, ce genre de situation peut être communiqué à l'agent chargé de la protection de la vie privée, qui, au besoin, peut lui-même demander l'aide de la haute direction. Dans les organisations plus grandes, cela peut inclure les spécialistes des TI, les gestionnaires de l'information, les experts en sécurité, les conseillers juridiques et les conseillers en communication.

B. MESURES DE CONTRÔLE DU PROGRAMME

Les mesures de contrôle du programme permettent de veiller à ce que les exigences de la LAIPVP et(ou) de la LRMP soient respectées dans toute l'organisation.

Elles doivent inclure les éléments suivants :

1. **Inventaire des renseignements (médicaux) personnels**
2. **Politiques**
3. **Procédures d'intervention en cas d'atteinte à la vie privée**
4. **Formation**
5. **Outils d'évaluation des risques pour la vie privée et la sécurité**
6. **Gestion des fournisseurs de services, gestionnaire de l'information et ententes de recherche**
7. **Communication transparente avec les particuliers**

1. Inventaire des renseignements (médicaux) personnels

Chacun des aspects d'un programme efficace de gestion de la protection de la vie privée commence par l'examen des types de renseignements (médicaux) personnels que l'organisation détient et de la façon dont elle les gère. Il est essentiel de déterminer la nature des renseignements que l'organisation collecte, utilise, communique et conserve, ainsi que les raisons de telles activités, pour s'assurer de la conformité à la LAIPVP et(ou) à la LRMP. Par exemple, si l'organisation ne sait pas qu'elle détient des renseignements médicaux personnels, il est peu probable qu'elle respecte certaines des exigences de la LRMP, lesquelles diffèrent de celles de la LAIPVP.

En dressant un inventaire, l'organisation peut examiner les calendriers de conservation des documents ou autre documentation décrivant les types de renseignements (médicaux) personnels qu'elle détient (qu'elle a en sa possession ou sous sa garde). L'établissement et la tenue d'un inventaire des renseignements (médicaux) personnels lui permettent d'évaluer ses pratiques de gestion de l'information au regard de la LAIPVP ou de la LRMP. Ils lui permettent aussi de déterminer les risques associés aux renseignements et de prendre les mesures administratives, techniques et physiques appropriées pour protéger l'information.

L'inventaire doit notamment décrire ce qui suit :

- les types de renseignements (médicaux) personnels que l'organisation détient (ex. : noms, adresses domiciliaires et coordonnées des clients)
- la nature délicate des renseignements
- où les renseignements (médicaux) personnels sont détenus, aussi bien à l'intérieur de l'organisation (ex. : dossiers papier dans les bureaux des membres du personnel et renseignements électroniques dans une base de données) que chez des tierces parties (y compris les fournisseurs de services)
- les raisons pour lesquelles l'information est recueillie, utilisée et communiquée

2. Politiques

Les politiques constituent une partie essentielle du programme de gestion de la protection de la vie privée. En l'absence de politiques et de procédures consignées par écrit, la conformité d'une organisation aux dispositions de la LAIPVP et de la LRMP n'est que ponctuelle et risque d'être désordonnée. Les politiques aident les employés à comprendre leurs obligations en matière de protection de la vie privée et à savoir comment faire pour les respecter.

Exemples de points clés que les politiques doivent traiter :

2.1 Exigences en matière d'avis et de consentement quant à la collecte des renseignements
2.2 Communication et correction des renseignements (médicaux) personnels
2.3 Conservation et élimination sécurisée des renseignements (médicaux) personnels
2.4 Mesures de protection administratives, techniques et physiques
2.5 Processus de traitement des plaintes

Au besoin, les organisations devraient aussi intégrer des exigences liées à la conformité en matière de protection de la vie privée dans d'autres politiques, par exemple dans les politiques de gestion des contrats et dans les politiques relatives aux ressources humaines.

La section suivante décrit chacune des politiques mentionnées ci-dessus de façon plus détaillée.

2.1 Exigences en matière d'avis et de consentement quant à la collecte des renseignements

Il est important que les employés sachent quels types et quelles quantités de renseignements (médicaux) personnels ils peuvent recueillir à des fins autorisées. Non seulement cela garantit que la collecte est conforme aux dispositions de la LAIPVP et(ou) de la LRMP mais cela permet aux employés d'expliquer aux particuliers les raisons pour lesquelles la collecte de renseignements est nécessaire et d'obtenir leur consentement le cas échéant.

Une politique à cet effet permet aux employés de comprendre leur obligation d'aviser les personnes des raisons pour lesquelles ils recueillent des renseignements et aussi de savoir quand et comment obtenir leur consentement. Elle peut par exemple préciser les informations que les employés sont tenus de fournir quand ils recueillent des renseignements directement auprès des personnes, de façon à respecter les obligations prévues par la LAIPVP et(ou) la LRMP. Elle peut aussi décrire les formes possibles de l'avis, p. ex. sous forme verbale ou sur des formulaires que les personnes doivent remplir. La politique peut également expliquer les circonstances dans lesquelles les employés doivent obtenir le consentement des personnes pour recueillir les renseignements auprès d'une autre source, où quand le consentement est nécessaire pour l'utilisation ou la communication des renseignements dans le cadre de la LAIPVP ou de la LRMP, cette dernière prévoyant d'autres obligations en matière de consentement.

2.2 Communication et correction des renseignements (médicaux) personnels

En vertu de la LAIPVP et de la LRMP, les particuliers, y compris les membres du personnel de l'organisation, ont le droit de demander à ce qu'on leur communique leurs renseignements personnels ou à ce qu'on y apporte des corrections. Les employés peuvent aider les particuliers à exercer leur droit en sachant quels processus ils doivent suivre. Le mieux est d'avoir une politique en place sur la façon de traiter les demandes de communication et de correction des renseignements. Cela favorise l'uniformité, la qualité et la rapidité des décisions, en plus de la conformité aux dispositions de la LAIPVP et de la LRMP.

Les organisations doivent savoir que la LRMP les oblige à informer les personnes de leur droit d'avoir accès à leurs renseignements médicaux personnels et de la façon dont elles peuvent exercer ce droit, ainsi que de leur droit d'autoriser une autre personne à exercer ce droit d'accès. Une politique à cet effet peut préciser la façon dont l'organisation se soumettra aux obligations de la LRMP à cet égard.

2.3 Conservation et élimination sécurisée des renseignements (médicaux) personnels

Des politiques de conservation et d'élimination sont nécessaires pour les employés de façon que les renseignements (médicaux) personnels ne soient pas éliminés prématurément ni gardés indéfiniment, et de façon qu'ils soient éliminés de manière sécurisée quand on n'en a plus besoin.

La LAIPVP et la LRMP énoncent les obligations en matière de politique écrite sur la conservation des renseignements (médicaux) personnels. Comme les lois ne précisent pas pendant combien de temps les renseignements devraient être conservés, les organisations devraient tenir compte de leurs circonstances opérationnelles, juridiques et financières, mais aussi en matière de vérification et d'archives, pour déterminer des périodes de conservation appropriées. Une politique doit également traiter la façon sécuritaire d'éliminer les renseignements (médicaux) personnels tant sur papier que sur support électronique.

Une politique doit préciser les procédures spéciales qui sont nécessaires pour retirer les renseignements (médicaux) personnels d'appareils électroniques dont on veut se séparer. Par exemple, une organisation peut avoir en place une politique particulière sur la destruction des renseignements stockés dans des photocopieurs ou des télécopieurs avant de se débarrasser de ces appareils.

2.4 Mesures de protection administratives, techniques et physiques

Les organisations doivent protéger les renseignements (médicaux) personnels qu'elles détiennent en adoptant des mesures de sécurité raisonnables, comme l'exigent la LAIPVP et la LRMP. Une politique à cet effet doit énoncer ce que doivent faire les employés pour protéger ces renseignements quand ils les recueillent, les utilisent, les communiquent et les stockent. De même, elle peut expliquer de quelle façon ils doivent protéger les renseignements quand ils les sortent de lieux sécurisés, par exemple quand ils les emportent dans d'autres lieux de travail ou quand ils travaillent à domicile.

Le choix des mesures de protection à inclure dans la politique dépend de divers facteurs, notamment de la nature délicate des renseignements et s'ils existent sur papier ou sur support électronique. Par exemple, une politique sur les renseignements figurant dans un système électronique doit informer les employés au sujet des conditions de connexion et de déconnexion, des mots de passe et aussi de l'obligation de ne pas communiquer les mots de passe. Les mesures de sécurité peuvent inclure des classeurs et des bureaux verrouillés, préciser quels renseignements peuvent être stockés dans des dispositifs de stockage portables et prévoir l'obligation d'utiliser des périphériques chiffrés.

2.5 Processus de traitement des plaintes

Toute personne a le droit de remettre en question la conformité d'une organisation à la LAIPVP et à la LRMP. Par conséquent, les organisations doivent se doter d'une politique énonçant les processus que les employés doivent suivre si quelqu'un veut se plaindre au sujet de leurs pratiques de gestion des renseignements (médicaux) personnels, notamment en matière de communication et de correction, mais aussi de collecte, d'utilisation et de sécurité de ces renseignements. En plus d'avoir un processus interne de plainte en matière de protection de la vie privée, les organisations devraient également informer les individus de leur droit de déposer une plainte auprès de l'ombudsman et fournir les coordonnées du bureau de l'ombudsman.

3. Procédures d'intervention en cas d'atteinte à la vie privée

En cas d'atteinte à la vie privée portant sur des renseignements (médicaux) personnels, il est important que les organisations soient prêtes à intervenir immédiatement. Cela ne peut se faire de façon efficace que si elles disposent d'une politique qui énonce les procédures à suivre dans de pareils cas.

L'organisation doit clairement assigner les responsabilités pour la gestion des incidents. Ces responsabilités sont notamment les suivantes : confinement et limitation de l'impact de l'incident, enquête sur les causes de l'incident et intégration, par la suite, des leçons tirées de l'expérience dans les procédures, les pratiques ou la formation des employés. Cela nécessite parfois la collaboration des employés de divers secteurs de l'organisation. La politique doit expliquer les responsabilités en matière de production de rapports internes et externes à la suite d'incidents.

La politique énonçant les procédures à suivre en cas d'atteinte à la vie privée est un élément essentiel du programme de gestion de la protection de la vie privée. En ce qui concerne les renseignements médicaux personnels, la LRMP exige l'adoption d'une politique écrite prévoyant la consignation des atteintes à la sécurité des renseignements ainsi que des mesures correctrices visant à remédier à ces atteintes.

Pour d'autres conseils sur la gestion des cas d'atteinte à la vie privée, veuillez consulter notre Avis de pratique sur les *Principales étapes à suivre en cas d'atteinte à la vie privée au regard de la LAIPVP et de la LRMP.*

4. Formation

La formation est essentielle, car, pour qu'un programme de gestion de la protection de la vie privée soit efficace, il faut que les employés prennent activement part à la protection de la vie privée. Il se peut qu'une organisation ait pris de solides mesures de contrôle pour protéger les renseignements personnels mais, si les employés ne sont pas informés de ces mesures, celles-ci sont pratiquement inutiles. Les employés sont mieux en mesure de protéger les renseignements personnels quand ils sont capables de reconnaître les problèmes lorsqu'ils surviennent et d'intervenir.

Tous les employés susceptibles d'avoir indirectement accès à des renseignements (médicaux) personnels doivent recevoir une formation générale en protection de la vie privée. Ceux et celles qui s'occupent directement de tels renseignements doivent suivre une formation complémentaire spécialement adaptée à leurs rôles. Le contenu du programme de formation doit être régulièrement réexaminé et mis à jour pour qu'il reflète les changements au sein de l'organisation.

Pour que le programme de formation d'une organisation soit efficace, il doit :

- être obligatoire pour tous les nouveaux employés avant que ceux-ci aient accès aux renseignements (médicaux) personnels ou s'en occupent, et régulièrement par la suite
- être adapté aux rôles des employés qui s'occupent des renseignements (médicaux) personnels
- couvrir les politiques et les procédures établies par l'organisation
- être offert de la manière la plus efficace et la plus appropriée, selon les besoins de l'organisation

La formation peut prendre bien des formes différentes notamment les suivantes : modules de formation obligatoires sur l'intranet de l'organisation, séances en petits groupes ou individuelles, ou bulletins d'information mensuels. L'organisation doit documenter ses processus de formation ainsi que la participation de ses employés.

En ce qui concerne les renseignements médicaux personnels, la LRMP exige que le dépositaire donne des séances d'orientation et une formation continue à ses employés et à ses mandataires au sujet de ses directives et procédures. Le dépositaire doit également faire en sorte que ses employés signent une promesse de confidentialité dans laquelle ils reconnaissent être liés par les directives et déclarent être au courant des conséquences que comporte leur inobservation.

5. Outils d'évaluation des risques pour la vie privée et la sécurité

L'évaluation des risques est un élément important de n'importe quel programme de gestion de la protection de la vie privée. Les risques liés aux renseignements (médicaux) personnels changent au fil du temps en raison de l'évolution des pratiques, des services, des programmes, de la technologie ou des structures administratives. L'utilisation appropriée d'outils d'évaluation des risques, notamment les évaluations de l'impact sur la vie privée (EIVP) et les évaluations des risques et des menaces pour la sécurité, peut aider à déterminer les problèmes et à y remédier, ou bien empêcher qu'ils ne se produisent en premier lieu.

C'est pourquoi il faut réaliser de telles évaluations dans le cadre de tous les nouveaux projets, services, programmes ou systèmes liés à des renseignements (médicaux) personnels ou en cas de changements importants que l'organisation peut apporter à ceux qui sont déjà en place. Les organisations doivent élaborer des procédures pour les évaluations de risques et prévoir un processus d'examen et d'approbation faisant intervenir l'agent chargé de la protection de la vie privée dès les premières étapes de la planification. Ces procédures doivent également s'appliquer à tous les secteurs opérationnels pertinents, notamment aux gestionnaires ou au personnel des TI pour ce qui est des systèmes d'information électroniques.

Pour en savoir davantage sur les EIVP, veuillez consulter notre Outil d'évaluation de l'impact sur la vie privée.

6. Gestion des fournisseurs de services, gestionnaire de l'information et ententes de recherche

Toutes sortes de relations liées aux renseignements (médicaux personnels) peuvent s'établir avec les fournisseurs de services, notamment dans le cadre de la sous-traitance de programmes ou de la passation de contrats pour des services particuliers. Un programme de gestion de la protection de la vie privée doit donc prévoir des procédures de conformité à la LAIPVP et à la LRMP pour les fournisseurs de services, y compris ceux qui sont « gestionnaires de l'information ».

Un tel programme doit comprendre des procédures faisant appel à l'agent chargé de la protection de la vie privée dans les processus d'approvisionnement et de passation de contrats de l'organisation pour des services touchant à des renseignements (médicaux) personnels.

Les organisations doivent également adopter des procédures pour traiter les demandes de renseignements (médicaux) personnels présentées par des chercheurs. Pour communiquer ce genre de renseignements, il faut remplir certaines conditions prévues par la LAIPVP et la LRMP, notamment établir une entente écrite avec le chercheur.

La LAIPVP et la LRMP prévoient des dispositions précises lorsqu'une organisation partage des renseignements (médicaux) personnels avec un « gestionnaire de l'information » qui traite, stocke ou élimine les renseignements pour le compte d'une organisation, ou qui fournit des services de gestion de l'information ou de technologie de l'information à une organisation. Les deux lois exigent de l'organisation qu'elle conclue une entente écrite prévoyant la protection des renseignements (médicaux) personnels, notamment contre leur communication, utilisation, élimination ou modification non autorisée.

7. Communication transparente avec les particuliers

La responsabilité en matière de gestion de la protection de la vie privée consiste notamment à faire preuve de transparence en communiquant avec les particuliers au sujet de leurs renseignements (médicaux) personnels. Les exigences de la LAIPVP et de la LRMP portent sur la communication entre les organisations et les personnes dont les renseignements sont recueillis, utilisés ou communiqués, y compris les employés de l'organisation elle-même. Cette communication consiste notamment à aviser les personnes de la collecte des renseignements, à obtenir leur consentement et à répondre à leurs demandes en ce qui concerne l'accès à leurs renseignements (médicaux) personnels et les corrections à y apporter.

Une organisation doit avoir en place des procédures pour informer les particuliers de leurs droits en matière de vie privée et des mesures de contrôle qu'elle a adoptées pour son programme, y compris de ses politiques. Ainsi, elle peut décider de publier ses politiques de confidentialité en ligne. La LRMP oblige les dépositaires à informer les personnes de leur droit d'avoir accès à leurs renseignements médicaux personnels, et de la façon dont elles peuvent procéder à cet égard, et aussi de la possibilité d'autoriser une autre personne à exercer ce droit d'accès.

Les particuliers doivent également pouvoir s'informer au sujet des procédures internes de l'organisation relatives au traitement des plaintes liées à la protection de la vie privée. De plus, les personnes qui se plaignent au sujet de la protection de leur vie privée doivent aussi pouvoir s'informer de leur droit de porter plainte à l'ombudsman en vertu de la LAIPVP et de la LRMP.

Ce type de communication doit être clair et compréhensible et non pas une simple réitération de la loi. La transparence au sujet des politiques, des pratiques et des mesures de conformité de l'organisation relativement à la protection de la vie privée fait partie de sa responsabilité à titre d'organisation du secteur public et de sa responsabilité à l'égard de la LAIPVP et de la LRMP.

C. ÉVALUATION CONTINUE ET RÉVISION

Une organisation doit surveiller, évaluer et réviser son programme de gestion de la protection de la vie privée pour faire preuve de responsabilité dans ce domaine et pour veiller à ce que sa façon de traiter les renseignements (médicaux) personnels) respecte les dispositions de la LAIPVP ou de la LRMP. Cela lui permet de s'assurer que les mesures de contrôle de son programme restent pertinentes et efficaces. Des changements dans les services, la technologie et les structures administratives, ainsi que dans les textes législatifs applicables, peuvent nécessiter des modifications aux mesures de contrôle du programme.

Pour évaluer de façon continue et réviser le programme de gestion de la protection de la vie privée, l'agent chargé de la protection de la vie privée doit :

1. **élaborer un plan de surveillance et d'examen**
2. **évaluer et réviser les mesures de contrôle du programme**

1. Élaborer un plan de surveillance et d'examen

L'agent responsable doit élaborer un plan pour examiner périodiquement le programme de gestion de la protection de la vie privée. Ce plan peut inclure un calendrier pour l'examen des politiques et autres mesures de contrôle du programme. En ce qui concerne les renseignements médicaux personnels, la LRMP exige en particulier la vérification des mesures de protection au moins tous les deux ans.

Certaines circonstances peuvent mener à l'examen et à la révision de certaines mesures de contrôle du programme. Par exemple, en cas d'atteinte à la vie privée, il est parfois nécessaire de réviser une politique particulière ou de donner une formation au personnel pour empêcher que d'autres incidents semblables se produisent. Cependant, il est recommandé de passer en revue toutes les mesures de contrôle du programme chaque année.

Le plan doit également inclure une évaluation documentée de tout changement éventuel dans le fonctionnement de l'organisation. Cela consiste à examiner tous les changements pertinents au sein de l'organisation en ce qui concerne les pouvoirs, les tâches ou les fonctions, le cadre réglementaire ou les politiques, les structures d'organisation ou de gestion, ou encore les activités ou programmes opérationnels.

2. Évaluer et réviser les mesures de contrôle du programme

L'efficacité des mesures de contrôle du programme doit être surveillée, périodiquement examinée et, au besoin, révisée. En ce qui concerne les renseignements médicaux personnels conservés dans un système d'information électronique, la LRMP prévoit certaines obligations précises au sujet des vérifications de l'activité des utilisateurs pour détecter les atteintes à la sécurité des renseignements.

Le contrôle est un processus continu qui doit permettre de répondre au moins aux questions suivantes :

- Quelles sont les dernières menaces et quels sont les derniers risques en matière de confidentialité ou de sécurité des renseignements?
- Est-ce que les mesures de contrôle du programme permettent de gérer les nouvelles menaces et reflètent les leçons tirées d'atteintes éventuelles à la sécurité des renseignements ainsi que les conclusions récentes d'enquêtes ou les conseils du bureau de l'ombudsman?
- Offre-t-on de nouveaux services qui nécessitent la collecte, l'utilisation ou la communication nouvelle ou accrue de renseignements (médicaux) personnels?
- Offre-t-on de la formation et est-elle efficace? Respecte-t-on les politiques et les procédures?

Si on découvre des problèmes pendant le contrôle, il faut que le personnel approprié les documente et y donne suite, en collaboration avec l'agent chargé de la protection de la vie privée.

L'agent doit régulièrement examiner les mesures de contrôle du programme et au moins :

- veiller à ce que l'inventaire des renseignements (médicaux) personnels soit à jour et faire en sorte de déterminer et d'évaluer les nouveaux cas de collecte, d'utilisation ou de communication de renseignements pour s'assurer qu'ils respectent la LAIPVP et la LRMP
- réviser éventuellement les politiques à la suite d'examens ou de vérifications, en réponse à une atteinte ou à une plainte, en fonction de nouvelles orientations ou de nouvelles pratiques exemplaires, ou à la suite d'analyses environnementales
- examiner les évaluations des risques pour déterminer les risques liés à la confidentialité et à la sécurité des renseignements en raison de modifications ou de nouvelles initiatives au sein de l'organisation, et pour y donner suite
- examiner et modifier les cours de formation et communiquer les changements apportés aux mesures de contrôle du programme
- examiner et adapter les procédures d'intervention en cas d'atteinte pour mettre en oeuvre les pratiques exemplaires et les leçons tirées d'examens réalisés à la suite d'incidents
- examiner et, au besoin, peaufiner les exigences dans les contrats conclus avec les fournisseurs de services et les ententes convenues avec les gestionnaires de l'information
- mettre à jour les communications avec les particuliers au sujet des droits liés à la protection de la vie privée et des politiques de l'organisation en matière de confidentialité

CONCLUSION

Des organisations responsables sont capables de prouver qu'elles ont mis en place un programme complet de gestion de la protection de la vie privée. Comme il n'existe pas de programme universel, il faut adapter le cadre évolutif proposé dans le présent document à la taille et au mandat de l'organisation ainsi qu'à la quantité et à la nature des renseignements (médicaux) personnels qu'elle a en sa possession ou sous sa garde.

Nous espérons que les conseils présentés dans ce document vont aider les organisations à observer la LAIPVP et la LRMP, à adopter des pratiques exemplaires et à montrer aux Manitobains qu'elles font preuve de responsabilité à l'égard de la protection de la vie privée.

ANNEXE : PROGRAMME DE GESTION DE LA PROTECTION DE LA VIE PRIVÉE EN BREF

A. ENGAGEMENT DE L'ORGANISATION

1. Engagement et appui réels de la haute direction

L'appui de la haute direction est essentiel à la réussite d'un programme de gestion de la protection de la vie privée et favorise une culture respectueuse de la vie privée. Il consiste notamment à :

- fournir les ressources nécessaires au bon fonctionnement du programme
- entériner les mesures de contrôle du programme
- surveiller le programme et examiner les rapports de conformité
- appuyer le rôle de l'agent chargé de la protection de la vie privée et favoriser une culture respectueuse de la vie privée au sein de l'organisation

2. Désignation d'un agent habilité qui est responsable de la gestion de la protection de la vie privée

L'organisation veille à :

- déléguer à l'agent la responsabilité de la conformité de l'organisation en matière de protection de la vie privée
- déterminer et communiquer clairement le rôle et les responsabilités de l'agent dans toute l'organisation

L'agent chargé de la protection de la vie privée est habilité à :

- établir, mettre en oeuvre, surveiller et réviser les mesures de contrôle du programme
- faire en sorte que la protection de la vie privée soit intégrée dans toutes les fonctions principales de l'organisation se rapportant à la collecte, à l'utilisation et à la communication des renseignements (médicaux) personnels

3. Adoption de mécanismes de production de rapports de conformité

Il faut établir des mécanismes redditionnels qui se reflètent dans les mesures de contrôle du programme pour que :

- la haute direction soit informée de la conformité de l'organisation par rapport aux politiques et procédures établies, notamment par des rapports de vérification ou d'examen, et aussi qu'elle sache si le programme de gestion de la protection de la vie privée fonctionne comme prévu
- les employés sachent quand, comment et à qui transférer les cas d'atteintes à la vie privée et les plaintes pour qu'on y donne suite

B. MESURES DE CONTRÔLE DU PROGRAMME

1. Inventaire des renseignements (médicaux) personnels

L'inventaire des renseignements (médicaux) personnels de l'organisation précise :

- les types de renseignements (médicaux) personnels qui sont en sa possession ou sous sa garde
- la nature délicate des renseignements
- où les renseignements sont détenus
- les raisons pour lesquelles les renseignements sont recueillis, utilisés et communiqués

2. Politiques

Points clés que les politiques de confidentialité doivent traiter :

- exigences en matière d'avis et de consentement quant à la collecte des renseignements
- communication et correction des renseignements (médicaux) personnels
- conservation et élimination sécurisée des renseignements (médicaux) personnels
- mesures de protection administratives, techniques et physiques
- processus de traitement des plaintes liées à la protection de la vie privée

3. Procédures d'intervention en cas d'atteinte à la vie privée

Les mesures de gestion des cas d'atteinte à la vie privée sont notamment les suivantes :

- disposer d'une politique énonçant les procédures à suivre pour gérer les incidents
- désigner une personne chargée de gérer les cas d'atteinte à la vie privée
- définir les responsabilités en matière de production de rapports internes et externes à la suite d'incidents

4. Formation

La formation doit :

- être obligatoire pour tous les nouveaux employés avant que ceux-ci aient accès aux renseignements (médicaux) personnels ou s'en occupent, et régulièrement par la suite
- être adaptée aux rôles des employés qui s'occupent des renseignements (médicaux) personnels
- couvrir les politiques et les procédures établies par l'organisation
- être offerte de la façon la plus appropriée et la plus efficace, selon les besoins de l'organisation

5. Outils d'évaluation des risques pour la vie privée et la sécurité

L'évaluation et la gestion responsables des risques consistent à :

- exiger une évaluation des risques pour la sécurité des renseignements (médicaux) personnels dans le cadre de tous les nouveaux projets, services, programmes ou systèmes, ou en cas de changements importants à ceux qui sont déjà en place
- mettre en place des processus destinés à évaluer les risques et les menaces pour la sécurité, p. ex. en effectuant des évaluations de l'impact sur la vie privée (EIVP)
- prévoir un processus d'examen et d'approbation faisant intervenir l'agent chargé de la protection de la vie privée

6. Gestion des fournisseurs de services, gestionnaire de l'information et accords en matière de recherche

Pour protéger les renseignements (médicaux) personnels en cas de contrats conclus avec des fournisseurs de services ou des gestionnaires de l'information, ou d'ententes convenues avec des chercheurs :

- prévoir des clauses standard dans les contrats ou accords conclus avec des fournisseurs de services pour s'assurer que les fournisseurs respectent leurs obligations en matière de protection de la vie privée
- veiller à ce que des ententes écrites avec les « gestionnaires de l'information » soient en place et respectent la LAIPVP et la LRMP
- prévoir des procédures pour traiter les demandes de chercheurs et veiller également à ce que des ententes écrites soient en place et respectent la LAIPVP et la LRMP

7. Communication transparente avec les particuliers

La communication de l'organisation avec les particuliers doit :

- permettre de les informer sur leurs droits à l'information et sur la façon dont ils peuvent s'en prévaloir
- permettre de les aviser sur les pratiques de l'organisation en matière de collecte de renseignements
- permettre d'obtenir leur consentement lorsque c'est approprié ou nécessaire
- permettre de les aviser informer au sujet des politiques de l'organisation en matière de protection de la vie privée
- permettre de les informer sur les procédures internes de l'organisation relatives au traitement des plaintes liées à la protection de la vie privée et sur leur droit de se plaindre auprès de l'ombudsman
- être claire, compréhensible et pas seulement une réitération de la loi

C. ÉVALUATION CONTINUE ET RÉVISION

1. Élaborer un plan de surveillance et d'examen

Chaque année, l'agent chargé de la protection de la vie privée doit élaborer un plan de surveillance et d'examen qui énonce la façon dont il surveillera et évaluera l'efficacité des mesures de contrôle du programme.

2. Évaluer et réviser les mesures de contrôle du programme au besoin

L'agent doit régulièrement examiner les mesures de contrôle du programme et au moins :

- veiller à ce que l'inventaire des renseignements (médicaux) personnels soit à jour et faire en sorte de déterminer et d'évaluer les nouveaux cas de collecte, d'utilisation ou de communication de renseignements pour s'assurer qu'ils respectent la LAIPVP et la LRMP
- réviser éventuellement les politiques à la suite d'examens ou de vérifications, en réponse à une atteinte ou à une plainte, en fonction de nouvelles orientations ou de nouvelles pratiques exemplaires, ou à la suite d'analyses environnementales
- examiner les évaluations des risques pour déterminer les risques liés à la confidentialité et à la sécurité des renseignements en raison de modifications ou de nouvelles initiatives au sein de l'organisation, et pour y donner suite
- examiner et modifier les cours de formation et communiquer les changements apportés aux mesures de contrôle du programme
- examiner et adapter les procédures d'intervention en cas d'atteinte pour mettre en oeuvre les pratiques exemplaires et les leçons tirées d'examens réalisés à la suite d'incidents
- examiner et, au besoin, peaufiner les exigences dans les contrats conclus avec les fournisseurs de services et les accords avec les gestionnaires de l'information
- mettre à jour les communications avec les particuliers au sujet des droits liés à la protection de la vie privée et des politiques de l'organisation en matière de confidentialité

Remerciements

Les présentes lignes directrices s'inspirent du document intitulé *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité* et publié conjointement par le Commissariat à la protection de la vie privée du Canada et les commissariats à l'information et à la protection de la vie privée (CIPVP) de l'Alberta et de la Colombie-Britannique. Elles s'inspirent également de la publication *Accountable Privacy Management in BC's Public Sector*, du CIPVP de la Colombie-Britannique, et du document *Privacy Management Program*, publié par le CIPVP de la Nouvelle-Écosse.