AVIS DE PRATIQUE DE L'OMBUDSMAN DU MANITOBA

Les avis de pratique sont rédigés par l'Ombudsman du Manitoba pour aider ceux et celles qui utilisent la législation. Ils ne visent qu'à donner des conseils et ne remplacent pas les textes législatifs.

Ombudsman du Manitoba
500, avenue Portage, bureau 750
Winnipeg (Manitoba) R3C 3X1
Tél. : 204 982-9130 ou 1 800 665-0531
Téléc. : 204 942-7803
Site Web : www.ombudsman.mb.ca

PRINCIPALES ÉTAPES À SUIVRE EN CAS D'ATTEINTE À LA VIE PRIVÉE AU REGARD DE LA *LOI SUR L'ACCÈS L'INFORMATION ET LA PROTECTION DE LA VIE PRIVÉE* (LAIPVP) ET DE LA *LOI SUR LES RENSEIGNEMENTS MÉDICAUX PERSONNELS* (LRMP)

But

Le présent document a pour but d'orienter les organismes publics et les dépositaires en cas d'atteinte à la vie privée.[1]

Les organismes publics et les dépositaires qui établissent une politique ou une procédure pour les cas d'atteinte à la vie privée trouveront peut-être utile d'y incorporer certains des renseignements qui suivent.

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

Il y a atteinte à la vie privée en cas de collecte, d'utilisation, de communication ou de destruction non autorisée de renseignements personnels ou de renseignements médicaux personnels. Ces activités sont « non autorisées » lorsqu'elles contreviennent à la Loi sur l'accès à l'information et la protection de la vie privée (LAIPVP) ou à la Loi sur les renseignements médicaux personnels (LRMP). Les atteintes à la vie privée peuvent se produire de diverses manières, notamment lorsque les renseignements (médicaux) personnels de clients, de patients, d'élèves ou d'employés sont volés, perdus ou communiqués par erreur, par exemple en cas de perte ou de vol d'appareils mobiles (ex. ordinateurs portables, clés USB) ou en cas de communication mal adressée (ex. télécopie, courriel, courrier).

Elles peuvent aussi être intentionnelles, lorsqu'un employé consulte, utilise ou communique des renseignements (médicaux) personnels sans en avoir l'autorisation aux termes de la LAIPVP et de la LRMP.

[1] Le présent document est une adaptation autorisée des documents suivants : *Privacy Breaches: Tools and Resources*, élaboré en mars 2012 par le bureau du commissaire à l'information et à la protection de la vie privée (CIPVP) de la Colombie-Britannique; *Outil d'évaluation aux fins de la notification en cas d'atteinte à la vie privée*, produit conjointement en décembre 2006 par le CIPVP de la C.-B. et le CIPVP de l'Ontario; *Key Steps in Responding to Privacy Breaches* et *Privacy Breach Report Form,* élaborés en juillet 2012 par le CIPVP de l'Alberta; *Keys Steps to Responding to Privacy Breaches,* élaboré en mars 2015 par le CIPVP de la Nouvelle-Écosse.

Quatre étapes principales à suivre en cas d'atteinte à la vie privée

Il y a quatre étapes principales à considérer en cas d'atteinte à la vie privée, présumée ou non :

1. Contenir l'incident
2. Évaluer les risques liés à l'incident
3. Notifier les personnes concernées et d'autres personnes
4. Prévenir d'autres atteintes à la vie privée

La mesure la plus importante que vous puissiez prendre consiste à intervenir immédiatement. Vous devriez suivre les étapes 1, 2 et 3 décrites ci-dessous immédiatement après l'incident et de façon simultanée ou en succession rapide. La quatrième étape comprend des recommandations pour des solutions à plus long terme et des stratégies de prévention.

PREMIÈRE ÉTAPE : CONTENIR L'INCIDENT

Prenez sans tarder des mesures de bon sens pour contenir l'incident, notamment les suivantes :

- Contenez immédiatement l'incident, par exemple en mettant fin à la pratique non autorisée, en récupérant les documents, en mettant hors service le système en cause, en révoquant ou en changeant les codes d'accès ou en corrigeant les lacunes des systèmes de sécurité matériels.
- Communiquez immédiatement avec le fonctionnaire chargé de la protection des renseignements personnels, l'agent et le coordonnateur de l'accès à l'information et de la protection de la vie privée, la direction et(ou) la personne chargée de la sécurité dans votre organisation.
- Prévenez la police si l'infraction procède d'un vol présumé ou de toute autre activité criminelle.
- Prenez garde de ne pas détruire d'éléments d'information liés à l'infraction qui pourraient servir à déterminer la cause de l'incident ou vous permettre de prendre les mesures correctives qui s'imposent.

DEUXIÈME ÉTAPE : ÉVALUER LES RISQUES LIÉS À L'INCIDENT

Pour déterminer toute autre mesure devant être prise immédiatement, vous devriez évaluer les risques liés à l'incident en tenant compte des facteurs suivants :

Les renseignements personnels ou les renseignements médicaux personnels en cause

- Quels sont les renseignements en cause? En général, plus les renseignements sont de nature délicate, plus les risques sont élevés. Les renseignements sur la santé, les numéros d'assurance sociale (NAS) et les renseignements financiers sont des exemples de données sensibles pouvant servir au vol d'identité.

Personnes concernées par l'incident

- Combien de personnes sont concernées par l'incident?
- Qui sont ces personnes : clients, patients, élèves, employés, entrepreneurs, fournisseurs de services, autres organisations?

Cause et étendue de l'incident

- Quelle est la cause de l'incident?
- Y a-t-il un risque que l'incident se reproduise ou que les renseignements soient encore plus compromis?
- Quelle a été l'étendue de la collecte, de l'utilisation ou de la communication non autorisée des renseignements, y compris le nombre des destinataires probables et la mesure dans laquelle l'accès

à ces renseignements, leur utilisation ou leur communication risque de se poursuivre, notamment par l'entremise des médias ou en ligne?
- Les renseignements ont-ils été retrouvés?
- Sont-ils chiffrés ou autrement difficiles d'accès?
- Quelles mesures ont déjà été prises pour atténuer les préjudices?

Préjudices prévisibles découlant de l'incident
- Y a-t-il un lien entre les personnes concernées et les destinataires non autorisés?
- Les personnes concernées peuvent-elles être considérées comme étant vulnérables, par exemple des jeunes ou des aînés.
- Comment les renseignements peuvent-ils être utilisés? L'information peut-elle servir à des fins frauduleuses ou autrement préjudiciables?
- Quel préjudice l'infraction pourrait-elle causer aux personnes concernées? Exemples :
    - risque pour la sécurité (ex. sécurité physique)
    - vol ou fraude d'identité
    - pertes commerciales ou perte de possibilités d'emploi
    - tort, humiliation, atteinte à la réputation ou détérioration des relations
    - risque de mesure discriminatoire prise à l'encontre d'une personne

Lorsque vous aurez évalué tous les risques mentionnés ci-dessus, vous serez capable de déterminer s'il y a lieu de notifier la(les) personne(s) concernée(s).

Le tableau suivante résume les facteurs de risque et établit un niveau de risque pour chacun. Il donne des exemples de facteurs de risque et de la façon dont ils peuvent être évalués; cependant, il appartient à chaque organisme public et dépositaire d'évaluer lui-même les risques étant donné les circonstances uniques de ce genre de situation. Le tableau vise à donner un aperçu général des niveaux de risque à attribuer et il n'a rien d'exhaustif.

Aperçu des niveaux de risque

Facteur de risque	Niveau faible	Niveau moyen	Niveau élevé
Nature des renseignements personnels ou des renseignements médicaux personnels	▪ Renseignements personnels accessibles au public et non associés à d'autres renseignements	▪ Renseignements personnels propres à l'organisation qui ne sont pas de nature médicale ou financière	▪ Renseignements médicaux, psychologiques, financiers ou de counselling, ou numéros d'identification uniques attribués par le gouvernement ▪ Renseignements concernant une personne vulnérable (p. ex. jeune ou aîné
Facteur de risque	**Niveau faible**	**Niveau moyen**	**Niveau élevé**
Relations	▪ Communication accidentelle à un autre professionnel qui a signalé l'infraction et confirmé la	▪ Communication accidentelle à une personne étrangère qui a signalé l'infraction et confirmé la destruction ou la restitution des renseignements	▪ Communication à une personne ayant un certain lien avec la(les) personne(s) touchée(s), ou qui les connaît, en

	destruction ou la restitution des renseignements		particulier les cas de communication avec d'ex-conjoints, des membres de la famille, des voisins ou des collègues ▪ Vol par une personne étrangère
Cause de l'infraction	▪ Erreur technique ayant été réglée	▪ Perte ou communication accidentelle	▪ Infraction délibérée ▪ Cause inconnue ▪ Erreur technique (si elle n'est pas réglée)
Étendue de l'infraction	▪ Très peu de personnes concernées	▪ Groupe connu et limité de personnes concernées	▪ Grand groupe ou tout un groupe non identifié
Efforts de limitation	▪ Données convenablement chiffrées ▪ Le dispositif de stockage portable a été effacé à distance et des preuves montrent que personne n'y a eu accès avant l'effacement ▪ Les copies papier des fichiers ou le dispositif ont été récupérés presque immédiatement et tous les fichiers semblent intacts ou non déchiffrés	▪ Le dispositif de stockage portable a été effacé à distance dans les heures qui ont suivi la perte mais il n'existe pas de preuves pour confirmer que personne n'y a eu accès avant l'effacement ▪ Les copies papier des fichiers ou le dispositif ont été récupérés mais il s'est écoulé suffisamment de temps entre la perte et la récupération pour que quelqu'un ait pu accéder aux données	▪ Données non chiffrées ▪ Les fichiers de données ou le dispositif n'ont pas été retrouvés ▪ La communication des données risque de se poursuivre notamment par l'entremise des médias ou en ligne
Préjudice prévisible découlant de l'infraction	▪ Aucun préjudice prévisible découlant de l'infraction	▪ Pertes commerciales ou perte de possibilités d'emploi ▪ Tort, humiliation, atteinte à la réputation ou détérioration des relations ▪ Préjudice social ou relationnel ▪ Perte de confiance dans l'organisme public ou dans le dépositaire ▪ Perte de biens pour l'organisme public ou le dépositare ▪ Perte de contrats ou pertes commerciales pour l'organisme public ou le dépositaire ▪ Risques financiers ou risque d'actions en justice pour l'organisme public ou le dépositaire	▪ Risque pour la sécurité (ex. sécurité physique) ▪ Risque de vol ou de fraude d'identité ▪ Risque élevé de tort, d'humiliation ou d'atteinte à la réputation selon les circonstances ▪ Risque pour la santé ou la sécurité publique

Résumé de l'évaluation des risques

Le préjudice prévisible découlant de l'infraction est souvent le facteur principal que l'on utilise pour décider s'il y a lieu de notifier les personnes concernées. En général, un risque de niveau moyen ou élevé devrait entraîner la notification de ces personnes. Un risque de niveau faible peut aussi entraîner une notification selon les circonstances uniques de chaque cas. Pour chacun des facteurs énoncés ci-dessus, veuillez déterminer le niveau de risque.

Facteur de risque	Niveau faible	Niveau moyen	Niveau élevé
Nature des renseignements personnels ou des renseignements médicaux personnels			
Relations			
Cause de l'infraction			
Étendue de l'infraction			
Efforts de limitation			
Préjudice prévisible découlant de l'infraction			
Autres facteurs			
Niveau de risque global			

TROISIÈME ÉTAPE : NOTIFIER LES PERSONNES CONCERNÉES ET D'AUTRES PERSONNES

Dans certaines circonstances, la notification peut constituer une importante stratégie d'atténuation des risques. Pour décider s'il convient de notifier, il est essentiel de se demander si la notification est nécessaire pour éviter ou atténuer le préjudice causé à une personne dont les renseignements personnels ou les renseignements médicaux personnels ont été recueillis, utilisés ou communiqués de façon inappropriée. Servez-vous de l'évaluation des risques que vous avez effectuée à la deuxième étape pour déterminer s'il y a lieu de procéder à la notification.

Si le cas d'atteinte à la vie privée se produit avec une tierce partie chargée, en vertu d'un contrat, de maintenir ou de traiter des renseignements personnels ou des renseignements médicaux personnels, il faut signaler l'incident à l'organisme public ou au dépositaire d'où ces renseignements proviennent. Pour ce qui est de la notification, il appartient à l'organisme public ou au dépositaire de notifier les personnes concernées lorsqu'il se produit une brèche dans la protection des renseignements.

Notifier les personnes concernées

Comme il est mentionné ci-dessus, si la notification est nécessaire pour éviter ou atténuer le préjudice causé aux personnes concernées, il faut notifier ces personnes. Pour déterminer cela, il faut tenir compte de certains éléments, notamment les suivants :

- Notification exigée par la loi : Est-ce que l'organisme public ou le dépositaire est visé par des dispositions législatives qui obligent à notifier les personnes concernées? Sachez que l'obligation de notifier n'est pas prévue par la LAIPVP ni par la LRMP.
- Obligations contractuelles : Est-ce que l'organisme public ou le dépositaire est tenu, en vertu d'un contrat, de notifier les personnes concernées en cas d'atteinte à la vie privée?
- Risque de vol ou de fraude d'identité : Le risque de vol ou de fraude d'identité est inquiétant si l'infraction porte sur des renseignements comme des noms associés à des numéros d'assurance

sociale, de carte de crédit, de permis de conduire, de carte santé, ou sur tout autre renseignement pouvant être utilisé frauduleusement par des tiers (p. ex. renseignements financiers).
- Risque de préjudice physique : Est-ce que la brèche dans la protection des renseignements personnels expose une personne à un risque de préjudice physique ou de harcèlement?
- Risque de tort, d'humiliation ou d'atteinte à la réputation : Est-ce que l'incident peut causer du tort à la personne concernée, l'humilier ou nuire à sa réputation? Ce type de préjudice peut se produire après la perte de renseignements, notamment des dossiers médicaux ou disciplinaires.
- Risque de pertes commerciales ou de perte de possibilités d'emploi : Est-ce que l'incident peut nuire à la réputation d'une personne, à ses possibilités d'emploi ou d'affaires?
- Infraction délibérée : Dans le cas d'une infraction délibérée, la personne concernée est peut-être la mieux placée pour évaluer les risques et prendre les mesures nécessaires pour les atténuer. L'auteur de l'infraction ne divulgue pas toujours entièrement ses motifs ni ses liens avec la personne (p. ex. ex-conjoint, membre de la famille, voisin).

Quand et comment notifier

Quand?
Les personnes concernées devraient être notifiées le plus tôt possible après l'incident. Cependant, si vous avez fait appel aux autorités chargées de l'application de la loi, vous devriez leur demander s'il serait préférable d'attendre pour éviter de nuire à une enquête criminelle éventuelle.

Comment?
La méthode utilisée pour notifier dépend des circonstances. Dans certains cas, l'emploi de plusieurs méthodes est ce qu'il y a de plus efficace.

Dans de très rares occasions, des preuves médicales peuvent montrer qu'il y a de bonnes raisons de penser qu'une notification pourrait entraîner des préjudices graves et immédiats pour la santé physique ou mentale d'une personne. Dans ces circonstances, essayez d'autres options, en demandant par exemple au médecin de notifier la personne ou en attendant que le danger immédiat passe.

Voici des facteurs à prendre en considération pour décider de la façon de notifier les personnes concernées.

Notification directe
Il vaut mieux notifier directement les personnes concernées – par téléphone, par lettre ou en personne. Cette méthode est préférable lorsque :
- l'identité des personnes concernées est connue
- les coordonnées actuelles des personnes concernées sont connues
- les personnes concernées ont besoin de renseignements détaillés pour se protéger adéquatement contre les préjudices découlant de l'incident
- les personnes concernées ont peut-être de la difficulté à comprendre une notification indirecte (en raison de leur capacités mentale, de leur âge, de leur langue, etc.)

Notification indirecte
La notification indirecte – avis publics, sites Web ou médias – peut être appropriée dans certaines circonstances. Il ne faut généralement y recourir que lorsque :
- la notification directe risque de causer davantage de préjudices, les coûts sont excessifs ou les coordonnées des personnes concernées sont inconnues
- le nombre de personnes concernées est tellement élevé qu'il serait trop difficile de les contacter toutes directement

L'ombudsman du Manitoba a créé un avis de pratique intitulé *Aide-mémoire pour rédiger une lettre de notification en cas d'atteinte à la vie privée*, qui énonce les renseignements à inclure dans ce genre de lettre adressée à une personne concernée.

Autres personnes à notifier

Que vous décidiez ou non qu'il est de votre devoir de notifier les personnes concernées, vous devriez vous demander si les autorités ou organisations suivantes devraient également être informées de l'incident :

- La police : si vous soupçonnez qu'il y a eu vol ou un autre crime
- Les fournisseurs de technologie : si l'incident est dû à une défaillance technique qui nécessite une modification technique ou un rappel
- Les compagnies d'assurance ou autres : s'il faut les notifier en vertu d'obligations contractuelles
- Les organismes professionnels ou de réglementation : s'il faut les notifier en vertu de normes professionnelles ou d'une réglementation

Signalement à l'ombudsman du Manitoba d'un cas d'atteinte à la vie privée

La LAIPVP et la LRMP n'obligent pas à signaler les cas d'atteinte à la vie privée à l'ombudsman du Manitoba. Cependant, nous encourageons le signalement de ces incidents lorsqu'il y a peut-être un risque de préjudice pour les personnes concernées. Les facteurs suivants peuvent permettre de décider si ce genre d'incident doit être signalé à l'ombudsman :

- la nature délicate des renseignements (médicaux) personnels
- si les renseignements peuvent servir à commettre un vol ou une fraude d'identité
- s'il existe un risque raisonnable de préjudice pour les personnes concernées, notamment de tort à la réputation ou aux relations, de préjudice physique ou mental, d'embarrassement, de peine ou d'humiliation
- le nombre de personnes touchées par l'incident

Nous avons créé un Formulaire de signalement de cas d'atteinte à la vie privée qui permet aux organismes publics et aux dépositaires de faire une analyse de l'incident en quatre étapes principales. Même si vous n'avez pas l'intention de signaler l'incident, vous pouvez vous servir du formulaire comme outil d'évaluation interne et d'intervention, car il peut vous aider à comprendre les questions à poser et les mesures à prendre.

Le signalement à l'ombudsman du Manitoba d'un cas d'atteinte à la vie privée peut être vu comme un acte positif. Il montre que l'organisme public ou le dépositaire considère la protection des renseignements (médicaux) personnels comme une question grave et importante. Nous pouvons peut-être vous aider à établir un plan d'intervention et à faire en sorte que des mesures soient prises pour empêcher que d'autres incidents se produisent dans l'avenir. Votre signalement nous aide nous aussi à répondre aux demandes de renseignements du public, à gérer les plaintes éventuelles déposées à la suite de l'incident et à déterminer le type de réponse à apporter, notamment une discussion informelle ou le lancement d'une enquête.

Si vous décidez de nous signaler un cas d'atteinte à la vie privée, il est important de le faire aussitôt que possible pour que nous puissions rapidement vous conseiller. Même si vous ne disposez pas de tous les détails concernant l'incident, vous pouvez fournir d'autres renseignements après le signalement.

QUATRIÈME ÉTAPE : PRÉVENIR D'AUTRES ATTEINTES À LA VIE PRIVÉE

Une fois que les mesures immédiates sont prises pour limiter les risques associés au cas d'atteinte à la vie privée, il faut prendre le temps d'enquêter sur les causes de l'incident. Cela peut consister en une vérification de la sécurité physique (p. ex. classeurs ou portes verrouillés, alarmes, mesures de contrôle pour l'accès des visiteurs), technique (p. ex. chiffrement, mots de passe, accès des utilisateurs) et administrative (p. ex. examen des politiques), ainsi que des pratiques du personnel (ex. formation sur la protection des renseignements). À la suite de cette évaluation, il faut adopter des mesures de protection à long terme contre de futures atteintes à la vie privée, ou améliorer au besoin celles qui sont déjà en place.

Il faut passer en revue et mettre à jour les politiques de façon qu'elles reflètent les leçons tirées du travail d'enquête, et faire cela régulièrement par la suite. Le plan qui en résulte devrait aussi inclure une vérification obligatoire à la fin du processus pour veiller à ce que les mesures de prévention ont toutes été mises en œuvre. Il faut également que les membres du personnel reçoivent une formation pour être informés de leurs responsabilités dans le cadre de la LAIPVP et de la LRMP.

Révision – novembre 2018