

AVIS DE PRATIQUE DE L'OMBUDSMAN DU MANITOBA

Les avis de pratique sont préparés par l'Ombudsman du Manitoba afin d'aider les personnes qui utilisent la législation. Leur objet en est un de conseil seulement et ils ne sont pas un substitut à la Loi.

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

ÉTAPES CLÉS DE LA RÉPONSE AUX VIOLATIONS DU RESPECT DE LA VIE PRIVÉE EN VERTU DE 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)*

Objet

L'objet de ce document est de fournir des lignes directrices aux organismes et dépositaires publics lorsqu'il y a violation du respect de la vie privée.¹

Qu'est-ce qu'une violation du respect de la vie privée ?

Une violation du respect de la vie privée se produit lorsqu'il y a collecte, utilisation, communication ou destruction non autorisée de renseignements personnels ou de renseignements médicaux personnels. Une telle activité est « non autorisée » si elle se produit en contravention de la LAIPVP ou de la LRMP. Les violations du respect de la vie privée les plus fréquentes se produisent lorsque des renseignements personnels de clients, de malades, d'étudiants ou d'employés sont volés, perdus ou communiqués par erreur. Des exemples comprennent lorsqu'un ordinateur qui contient des renseignements personnels ou des renseignements médicaux personnels est volé ou que les renseignements sont transmis par erreur soit par télécopieur ou courrier électronique à la mauvaise personne.

Rapport des violations du respect de la vie privée

L'Ombudsman du Manitoba a créé un Formulaire de rapport des violations du respect de la vie privée qui permet aux organismes publics et aux dépositaires de faire une analyse de la violation en utilisant quatre étapes clés décrites plus bas. Ce formulaire fait partie de notre Note de pratique *Rapport d'une violation du respect de la vie privée à l'Ombudsman du Manitoba* et est disponible sur notre site Web.

Quatre étapes clés de la réponse à une violation du respect de la vie privée

La mesure la plus importante que vous pouvez prendre est de répondre immédiatement à la violation. Vous devriez entreprendre les étapes 1, 2 et 3 décrites ci-après immédiatement la violation, et le faire de

¹ Ce document a été adapté avec permission à partir de *Key Steps in Responding to Privacy Breaches* et du formulaire *Privacy Breach Reporting Form*, développés par le Commissariat à l'information et la protection de la vie privée de la Colombie-Britannique (OIPC BC), décembre 2006, et l'*Outil d'évaluation de la notification d'une violation du respect de la vie privée*, produit conjointement par l'OIPC BC et le Commissaire à l'information et la protection de la vie privée de l'Ontario, décembre 2006, ainsi qu'à partir de *Key Steps in Responding to Privacy Breaches* et le formulaire *Privacy Breach Report* développés par le Bureau du Commissaire à l'information et la protection de la vie privée de l'Alberta.

façon simultanée ou en succession rapide. L'étape 4 offre des recommandations pour des solutions à plus long terme et des stratégies de prévention.

ÉTAPE 1 : CONTENIR LA VIOLATION

Prendre immédiatement des mesures pour limiter l'étendue de la violation. Ces mesures comprennent :

- Contenir immédiatement la violation en, par exemple, arrêtant les pratiques non autorisées, recouvrant les dossiers, fermant le système qui a été violé, révoquant l'accès ou corrigeant les faiblesses de la sécurité physique.
- Contacter immédiatement l'agent à la protection de la vie privée, le coordonnateur à l'accès à l'information et la protection de la vie privée, l'agent à l'accès à l'information et la protection de la vie privée ou la personne responsable de la sécurité de votre organisme.
- Avertir les policiers si la violation comprend une suspicion de vol ou d'autre activité criminelle.

ÉTAPE 2 : ÉVALUER LES RISQUES ASSOCIÉS À LA VIOLATION

Afin de déterminer quelles sont les autres mesures immédiatement nécessaires, vous devriez évaluer les risques associés à la violation. Considérez ce qui suit :

(I) LES RENSEIGNEMENTS PERSONNELS ET LES RENSEIGNEMENTS MÉDICAUX PERSONNELS IMPLIQUÉS

- Quels éléments de données ont été violés ? Généralement, plus les renseignements sont de nature délicate, plus le risque est élevé. Les renseignements médicaux, les numéros d'assurance sociale (NAS) et les renseignements financiers qui pourraient être utilisés pour le vol d'identité sont des exemples de renseignements de nature délicate.
- Quelle est l'utilisation possible de ces renseignements ? Les renseignements peuvent-ils être utilisés à des fins frauduleuses ou autrement nuisibles ?

(II) LA CAUSE ET L'ÉTENDUE DE LA VIOLATION

- Quelle est la cause de la violation ?
- Y a-t-il risque de l'exposition plus étendue ou continue des renseignements ?
- Quelle était l'étendue de la collecte, de l'utilisation ou de la communication non autorisées, y compris le nombre de destinataires possibles et le risque d'accès, d'utilisation ou de communication subséquent, y compris les médias de masse ou en ligne ?
- Les renseignements sont-ils chiffrés ou autrement non facilement accessibles ?
- Quelles mesures avez-vous déjà prises pour minimiser les dommages ?

(III) LES PARTICULIERS AFFECTÉS PAR LA VIOLATION

- Combien de particuliers sont affectés par la violation ?
- Qui a été atteint par la violation : les clients, les malades, les étudiants, les employés, les entrepreneurs, les fournisseurs de services, d'autres organismes ?

(IV) LES DOMMAGES PRÉVISIBLES DE LA VIOLATION

- Existe-t-il un lien entre les particuliers affectés et les destinataires non autorisés ?
- Quels préjudices aux particuliers affectés pourraient résulter de la violation ? Les préjudices peuvent comprendre :
 - Un risque à la sécurité (p. ex. : la sécurité physique) ;
 - Le vol d'identité ou la fraude ;
 - La perte d'occasions d'emploi ou d'affaires ;
 - La peine, l'humiliation, le dommage à la réputation ou à des relations.
- Quel préjudice pourrait résulter pour l'organisme public ou le dépositaire à la suite de la violation ? À titre d'exemple :
 - La perte de confiance dans l'organisme public ou le dépositaire ;
 - La perte d'actifs ;
 - Des enjeux financiers.
- Quel préjudice pourrait résulter pour le public à la suite de la violation ? À titre d'exemple :
 - Un risque à la santé publique ;
 - Un risque à la sécurité publique.

ÉTAPE 3 : AVISER LES PERSONNES CONCERNÉES

L'avis peut être une stratégie d'atténuation importante dans les circonstances appropriées. Une considération clé dans la prise de décision d'aviser les personnes concernées devrait être si l'avis est nécessaire pour éviter ou atténuer le préjudice à un particulier dont les renseignements personnels ou les renseignements médicaux personnels ont été recueillis, utilisés ou communiqués de façon inappropriée. Révisez votre évaluation du risque à l'étape 2 afin de déterminer si l'avis est requis ou non.

Si la violation se produit chez une tierce entité qui a été engagée par contrat pour maintenir ou traiter les renseignements personnels ou les renseignements médicaux personnels, la violation devrait être déclarée à l'organisme public ou le dépositaire qui en est l'origine. Lorsqu'un avis est fourni, il relève de la responsabilité des organismes publics ou des dépositaires d'aviser les particuliers concernés lorsqu'une violation se produit.

(i) Aviser les personnes concernées

Comme noté plus haut, l'avis des personnes concernées devrait être fait s'il est nécessaire pour éviter ou atténuer le préjudice à leur égard. Certaines considérations dans la détermination d'aviser ou non les personnes concernées par la violation comprennent :

- **La législation exige la notification** : est-ce que l'organisme public ou le dépositaire fait l'objet de législation qui exige l'avis aux personnes concernées ? Prière de noter que la LAIPVP et la LRMP n'exigent pas la notification.
- **Les obligations contractuelles exigent la notification** : est-ce que l'organisme public ou le dépositaire a une obligation contractuelle d'aviser les personnes concernées dans le cas d'une violation de la protection de la vie privée ?

- **Le risque de vol d'identité ou de fraude** : À quel point ce risque est-il raisonnable ? Le vol d'identité est une préoccupation si la violation comprend des informations non chiffrées telles que des noms conjointement avec des numéros d'assurance sociale (NAS), des numéros de carte de crédit, des numéros de permis de conduire, des numéros de renseignements médicaux personnels (NRMP), des numéros de carte de débit avec des informations de mot de passe ou toute autre information qui peut être utilisée pour fraude par des tiers (p. ex. : financière).
- **Le risque de dommage corporel** : La violation de la protection de la vie privée place-t-elle la personne à risque de dommage corporel, de harcèlement avec ou sans menaces ?
- **Le risque de peine, d'humiliation ou de dommage à la réputation** : Est-ce que la violation de la protection de la vie privée peut mener à de la peine, de l'humiliation ou des dommages à la réputation d'une personne ? Ce type de dommages peut se produire lors de la perte de renseignements comme des dossiers médicaux ou des dossiers disciplinaires.
- **Le risque de perte d'occasions d'affaires ou d'emploi** : Est-ce que la violation de la protection de la vie privée peut entraîner des dommages à la réputation d'une personne, ayant un effet sur ses occasions d'affaires et d'emploi ?

(II) QUAND ET COMMENT AVISER

Quand ?

Lorsqu'un avis est fourni aux personnes affectées par la violation, ceci devrait se produire dès que possible après la violation. Toutefois, si vous avez contacté les autorités policières, vous devriez déterminer auprès de ces autorités si la notification devrait être retardée afin de ne pas nuire à l'enquête criminelle.

Comment ?

La méthode de notification dépendra des circonstances. L'utilisation de méthodes de notification multiples dans certains cas peut s'avérer l'approche la plus efficace. Suivent certains facteurs à prendre en considération lors de la décision d'aviser les personnes concernées.

Avis direct

La méthode préférée d'avis est directement — par téléphone, par lettre ou en personne — aux personnes concernées. Cette méthode est préférable lorsque :

- les identités des personnes sont connues ;
- les coordonnées actuelles des personnes concernées sont disponibles ;
- les personnes concernées par la violation nécessitent des informations détaillées afin de se protéger adéquatement du dommage issu de la violation ;
- les personnes concernées par la violation peuvent avoir de la difficulté à comprendre un avis indirect (dû aux capacités mentales, à l'âge, à la langue, etc.)

Avis indirect

Offrir un avis indirect — avis affichés, information sur le site Web, médias — peut être approprié dans certaines circonstances. Ceci ne devrait se produire que lorsque :

- l'avis direct pourrait causer plus de dommages, est prohibitif en coût ou il y a manque de coordonnées ;

- un très grand nombre de personnes sont concernées par la violation de façon telle que l'avis direct ne serait pas pratique.

Que devrait comprendre l'avis ?

Les renseignements suivants devraient être compris dans l'avis :

- La date de la violation ;
- Une description générale de la violation ;
- La description des renseignements recueillis, utilisés ou communiqués de façon inappropriée (p. ex. : le nom, les numéros de carte de crédit, les NAS, les dossiers médicaux, les renseignements financiers, etc.) ;
- Les mesures prises jusqu'ici pour atténuer les dommages ;
- Les prochaines mesures prévues et toute planification à long terme pour prévenir les violations à l'avenir ;
- Les mesures que la personne peut prendre pour atténuer davantage le risque de dommages. Fournir les coordonnées pour les agences de rapport de crédit (pour établir une surveillance de crédit) et pour changer un numéro de renseignements médicaux personnels (NRMP) ou un numéro de permis de conduire ;
- Les coordonnées d'une personne au sein de l'organisme public ou du dépositaire qui peut répondre aux questions ou donner de plus amples renseignements ;
- Des informations sur la façon de contacter ou de déposer une plainte auprès de l'Ombudsman du Manitoba.

(III) AUTRES ENTITÉS À CONTACTER

Sans égard à ce que vous déterminez être vos obligations en ce qui a trait à l'avis des personnes, vous devriez considérer si les autorités ou organismes suivants devraient aussi être avisés :

- **Les autorités policières** : S'il y a suspicion de vol ou d'autre crime ;
- **Les assureurs ou autres** : Si les exigences contractuelles l'exigent ;
- **Les organismes professionnels ou de réglementation** : Si les normes professionnelles ou de réglementation exigent un avis à ces organismes ;
- **Les fournisseurs de technologie** : Si la violation était due à une défectuosité technique et un rappel ou une correction technique est exigé.
- **L'Ombudsman du Manitoba** : Le rapport d'une violation de la protection de la vie privée à l'Ombudsman du Manitoba n'est pas obligatoire en vertu de la LAIPVP et de la LRMP. Les facteurs suivants sont pertinents dans la décision de faire rapport ou non d'une violation, à l'Ombudsman :
 - La nature délicate des renseignements personnels ou des renseignements médicaux personnels ;
 - Si les renseignements communiqués peuvent être utilisés pour commettre un vol d'identité ;
 - S'il y a une possibilité raisonnable de dommages dus à la communication, y compris les pertes non financières ;
 - Le nombre de personnes concernées par la violation ;

- Si les renseignements ont été pleinement recouverts sans autre communication.

Le rapport d'une violation de la protection de la vie privée à l'Ombudsman du Manitoba peut être perçu comme une action positive. Il démontre au public que l'organisme public ou le dépositaire tient la protection des renseignements personnels et des renseignements médicaux personnels comme une affaire importante et grave. L'Ombudsman du Manitoba peut vous aider à développer une procédure de réponse à la violation de la protection de la vie privée et à assurer que des mesures sont prises pour prévenir les violations à l'avenir. Elle vous aidera de plus à répondre aux requêtes du public et à gérer toute plainte reçue comme résultat de la violation.

Pour aviser l'Ombudsman, vous voudrez peut-être utiliser le Formulaire de violation de la protection de la vie privée contenu dans notre Avis de pratique *Rapport d'une violation de la protection de la vie privée à l'Ombudsman du Manitoba*, situé sur notre site Web.

ÉTAPE 4 : PRÉVENIR

Une fois que les mesures sont prises pour atténuer les risques associés à la violation, vous devez prendre le temps d'étudier en profondeur les causes de la violation. Ceci peut exiger une vérification de sécurité des mesures de sécurité physique et technique. Comme résultat de cette évaluation, vous devriez développer ou améliorer, selon la pertinence, des mesures de protection à long terme contre les violations additionnelles. Les politiques devraient être révisées et mises à jour afin de refléter les leçons apprises au cours de l'enquête, et ceci, sur une base régulière. La planification qui en résultera devrait aussi comprendre une exigence de vérification à la fin de processus pour s'assurer que le plan de prévention a été complètement mis en œuvre. Le personnel devrait être formé pour qu'il connaisse ses responsabilités en vertu de la LAIPVP et de la LRMP.