

Ombudsman du Manitoba Avis de pratique

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

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

Cet avis de pratique a pour but d'orienter les organismes publics et les dépositaires en cas d'atteinte à la vie privée. Des modifications apportées à la LAIPVP et à la LRMP en janvier 2022 obligent ces organismes publics et ces dépositaires à aviser les personnes concernées par un cas d'atteinte à la vie privée lorsqu'un risque réel de grave préjudice pour ces personnes a été établi.

Cet avis de pratique donne également des conseils aux organismes publics et aux dépositaires en ce qui concerne leur obligation de prévenir l'ombudsman du Manitoba en cas d'atteinte à la vie privée, et il leur explique notamment comment remplir le [Formulaire de signalement d'atteinte à la vie privée](#).

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

La LAIPVP et la LRMP définissent toutes deux l'atteinte à la vie privée comme le vol ou la perte de renseignements (médicaux) personnels, ou bien tout accès ou toute utilisation, communication, destruction ou modification visant de tels renseignements en contravention avec ces lois.

Un cas d'atteinte à la vie privée peut se produire :

- de diverses façons, notamment lorsque les renseignements (médicaux) personnels de clients, de patients, d'élèves ou d'employés sont volés, perdus ou communiqués par erreur, par exemple lorsqu'un appareil mobile (ordinateur portatif, clé USB) est volé ou lorsque des renseignements sont transmis accidentellement (par télécopieur, courriel, courrier) à la mauvaise personne.

Table des matières

Qu'est-ce qu'une atteinte à la vie privée?	1
Que faire en cas d'atteinte à la vie privée?	2
Première étape : contenir l'incident	2
Deuxième étape : évaluer les risques	3
Nature confidentielle	3
Probabilité d'un préjudice	4
Troisième étape : aviser et signaler	5
Aviser les personnes concernées	5
Signaler les incidents à l'ombudsman du Manitoba	9
Quatrième étape : prévenir d'autres incidents	10



L'atteinte à la vie privée peut également être intentionnelle :

- notamment quand les renseignements (médicaux) personnels sont consultés, utilisés, communiqués, détruits ou modifiés d'une façon qui n'est autorisée ni par la LAIPVP, ni par la LRMP. Exemples : furetage, piratage, hameçonnage et logiciel rançonneur.

Que faire en cas d'atteinte à la vie privée?

La mesure la plus importante que vous puissiez prendre consiste à intervenir immédiatement. Les quatre étapes mentionnées ci-dessous peuvent vous aider.

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

1. **Contenir l'incident**
2. **Évaluer les risques liés à l'incident**
3. **Aviser et signaler**
4. **Prévenir d'autres incidents**

Vous devriez suivre les étapes 1, 2 et 3 – contenir, évaluer et aviser – dès que possible après l'incident. La quatrième étape – prévenir d'autres incidents – propose des solutions à plus long terme et des stratégies de prévention.

Première étape : contenir l'incident

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

- Mettez fin à la pratique non autorisée, par exemple en stoppant la transmission de courriel ou autre correspondance au mauvais destinataire.
- Retirez, déplacez ou isolez les renseignements ou dossiers vulnérables pour prévenir toute consultation ou communication ultérieure non autorisée.
- Récupérez les documents ou copies de documents communiqués ou saisis par une personne non autorisée.
- Procédez à des fouilles pour retrouver les documents perdus ou volés.
- Remettez les documents à leur emplacement d'origine ou au destinataire prévu.
- Demandez et vérifiez que le destinataire imprévu supprime deux fois tous les courriels et autres documents concernés.
- Mettez hors service le système en cause ou remédiez aux lacunes des systèmes de sécurité.
- Révoquez les codes d'accès au système.
- Changez les mots de passe.
- Communiquez avec la personne chargée de la sécurité dans votre organisation, de façon à pouvoir mettre en place d'autres mesures de protection.

Deuxième étape : évaluer les risques associés à l'incident

Depuis le 1^{er} janvier 2022, la LAIPVP et la LRMP prévoient toutes les deux que, quand un organisme public ou un dépositaire établit que l'atteinte à la vie privée pose un *risque réel de préjudice grave* pour les particuliers concernés, il *doit* aviser ces personnes et l'ombudsman de l'incident.

L'évaluation approfondie du *risque réel de préjudice grave* est essentielle pour l'organisme public et le dépositaire. Elle détermine les prochaines étapes que vous devez suivre en réponse à l'incident, et aussi si un avis doit être adressé aux personnes touchées et à l'ombudsman en vertu des lois.

Pour déterminer les mesures qu'il faut prendre en réponse à un cas d'atteinte à la vie privée, l'organisme public et le dépositaire doit d'abord déterminer si l'incident a posé un *risque réel de préjudice grave* pour les particuliers concernés. Les lois définissent la notion de *préjudice grave* et donnent des exemples de préjudices pouvant avoir un impact sur un particulier :¹

- lésion corporelle
- humiliation
- préjudice à la réputation ou aux relations du particulier
- perte de possibilités d'emploi, d'occasions d'affaires ou d'occasions professionnelles
- perte financière
- vol d'identité
- effets néfastes sur la cote ou le rapport de solvabilité du particulier
- perte d'un bien ou dommages causés à ce dernier

Les règlements énumèrent aussi les facteurs que vous devez prendre en considération pour déterminer si l'incident a posé un risque réel de préjudice grave.² Pour en avoir la certitude, veuillez consulter le règlement applicable de la LAIPVP ou de la LRMP. Le résumé ci-dessous énumère ces facteurs ainsi que les questions importantes dont il faut tenir compte.

Nature confidentielle

Les renseignements (médicaux) personnels en cause

- Quels renseignements (médicaux) personnels ont été compromis? En général, plus les renseignements sont confidentiels, plus le risque de préjudice grave est élevé pour les particuliers concernés. Les renseignements médicaux, les numéros d'assurance sociale (NAS) et les renseignements financiers sont des exemples de renseignements très confidentiels pouvant servir au vol d'identité.

¹ Consulter le paragraphe 41.1(1) de la LAIPVP et le paragraphe 19.0.1(1) de la LRMP

² Consulter l'article 3.1 du règlement de la LAIPVP et l'article 8.7 du règlement de la LRMP

Probabilité de préjudice

Cause et étendue de l'incident

- Quelles circonstances ont été la cause de l'atteinte à la vie privée et existe-t-il des preuves d'intention malveillante, par exemple que l'incident résulte d'un vol ou de l'obtention d'un accès non autorisé à un système informatique? Un employé a-t-il délibérément accédé aux renseignements à des fins non liées au travail? Ou bien, l'incident était-il accidentel?
- Combien de personnes ont accédé ou auraient accédé aux renseignements? Connaît-on leur identité?
- Y a-t-il une relation connue entre les personnes qui ont accédé ou auraient accédé aux renseignements et le ou les particuliers auxquels les renseignements se rapportent? Quelle est la nature de cette relation?

Personnes concernées par l'incident

- Combien de personnes sont concernées?
- Qui a été touché : clients, patients, élèves, employés, entrepreneurs, fournisseurs de services?
- Est-ce que des personnes potentiellement vulnérables ont été touchées : enfants ou jeunes, personnes en situation de handicap, aînés?

Sécurité des renseignements (médicaux) personnels

- Est-ce que l'organisme public ou le dépositaire est raisonnablement convaincu que la personne qui a accédé ou qui aurait accédé aux renseignements en a détruit les copies non autorisées et s'est engagée à ne pas utiliser ni communiquer ces renseignements?
- À quel moment l'incident s'est-il produit et pendant combien de temps les renseignements ont-ils pu être consultés, utilisés, communiqués, détruits ou modifiés?
- Y a-t-il un risque que les renseignements soient encore compromis ou le soient encore plus? Y a-t-il un risque qu'ils soient encore consultés, utilisés ou communiqués de façon non autorisée?
- Combien de renseignements sont en cause?
- Les renseignements ont-ils été récupérés?
- Les renseignements étaient-ils convenablement chiffrés, anonymisés ou leur accès était-il autrement difficile?

Preuve de préjudice découlant de l'incident

- Un préjudice a-t-il été subi (du genre qui est inclus dans la définition de préjudice grave)?

Une évaluation de tous les facteurs de risque décrits dans les règlements applicables, tels qu'ils sont résumés ci-dessus, vous permettra de déterminer si l'incident a posé un risque réel de préjudice grave pour un particulier.

Pour déterminer qu'un cas d'atteinte à la vie privée pose un risque réel de préjudice grave, il est important de noter ce qui suit :

- La détermination repose sur la nature confidentielle des renseignements (médicaux) personnels en cause et de la probabilité que ces renseignements puissent être utilisés de façon à causer un préjudice grave pour le ou les particuliers.
- On utilise le terme « grave » parce qu'il faut que la personne soit exposée à un certain risque de dommages, de torts ou de blessures qui sont graves de nature.
- Pour que le risque soit « réel », il faut des preuves solides indiquant que les renseignements en question ont été ou seront utilisés à mauvais escient. Il ne faut pas considérer le « risque réel de préjudice grave » comme une vague possibilité ni comme une simple supposition ou hypothèse.

L'ombudsman du Manitoba a mis à jour ses ressources à l'intention des organismes publics et des dépositaires en cas d'atteinte à la vie privée. Nos [Outils d'évaluation des risques d'atteinte à la vie privée](#) incluent désormais les facteurs de risque énoncés dans les règlements et établissent un niveau de risque **possible** pour chaque facteur. Chacun des outils décrits dans la LAIPVP et la LRMP fournit des exemples de facteurs de risque et des façons de les évaluer. Il est important de souligner que chaque organisme public et dépositaire doit procéder à sa propre évaluation des risques du fait des circonstances uniques de chaque cas d'atteinte à la vie privée. Les outils visent à donner un aperçu général des niveaux de risque et ils n'ont rien d'exhaustif.

Encore une fois, il est essentiel pour les organismes publics et les dépositaires de procéder à une évaluation complète du risque réel de préjudice grave. Cette évaluation déterminera les prochaines étapes que vous devrez suivre en réponse à l'incident et aussi si vous devez adresser un avis aux personnes touchées et à l'ombudsman en vertu des lois.

Troisième étape : aviser et signaler

Aviser les personnes touchées³

Depuis le 1^{er} janvier 2022, la LAIPVP et la LRMP prévoient toutes les deux que, quand un organisme public ou un dépositaire établit que l'atteinte à la vie privée pose un risque réel de préjudice grave pour les particuliers concernés, il *doit* aviser ces personnes et l'ombudsman de l'incident.

En vertu de la LAIPVP et de la LRMP, il est obligatoire d'aviser les personnes concernées lorsqu'un cas d'atteinte à la vie privée pose un risque réel de préjudice grave pour ces personnes. Dans certaines circonstances, l'avis peut également servir d'importante stratégie d'atténuation des risques, qu'il soit obligatoire ou non. Pour décider s'il convient d'aviser les

³ Consulter le paragraphe 41.1(2) de la LAIPVP et le paragraphe 19.0.1(2) de la LRMP

personnes concernées, il est essentiel de se demander si l'avis est nécessaire pour éviter ou atténuer le préjudice causé aux personnes dont les renseignements (médicaux) personnels ont été compromis par l'incident.

L'avis adressé à la personne concernée peut également vous aider à évaluer plus précisément le risque de préjudice, car il arrive parfois que la personne communique des renseignements sur les possibilités de préjudice auxquelles vous ne penseriez pas forcément. Revoyez l'évaluation des risques que vous avez effectuée à la deuxième étape pour déterminer s'il y a lieu de remettre un avis.

Il existe peut-être d'autres facteurs qui influent sur la décision de l'organisme public ou du dépositaire d'aviser les particuliers d'un cas d'atteinte à la vie privée, par exemple une politique, une obligation contractuelle ou la volonté de se montrer transparent.

Sachez que les modifications apportées en 2022 aux lois du Manitoba sur la protection de la vie privée **obligent** les organismes publics et les dépositaires à aviser les personnes concernées par une atteinte à la vie privée s'il est raisonnable de s'attendre à ce que l'incident pose un risque réel de préjudice grave pour ces personnes.

Un tiers chargé, en vertu d'un contrat, de maintenir ou de traiter des renseignements (médicaux) personnels devrait collaborer avec l'organisme public ou le dépositaire pour déterminer le risque réel de préjudice grave et pour aviser les personnes concernées et l'ombudsman du Manitoba lorsqu'un cas d'atteinte à la vie privée se produit.

Quand et comment aviser les personnes concernées

Quand?

Quand un avis **obligatoire** est remis aux personnes concernées par un cas d'atteinte à la vie privée, parce que l'organisme public ou le dépositaire a déterminé que l'incident posait un risque réel de préjudice grave, la LAIPVP et la LRMP exigent que l'avis soit remis **dès que possible**.⁴

Si l'organisme public n'est pas tenu de remettre un avis, mais choisit d'aviser les personnes touchées par l'atteinte à la vie privée – pour se montrer transparent, par prudence à l'égard du risque pour les personnes ou parce que c'est sa politique ou sa pratique – il faut aussi que cela se produise dès que possible.

Si l'organisme public ou le dépositaire a fait part de l'incident aux autorités chargées de l'application de la loi, il doit discuter du moment opportun de l'avis avec ces autorités pour s'assurer de ne pas nuire malencontreusement à une enquête criminelle éventuelle.

⁴ Consulter le paragraphe 41.1(3) de la LAIPVP et le paragraphe 19.0.1(3) de la LRMP

Comment?

Quand un avis **obligatoire** est remis aux personnes touchées par l'incident, les lois exigent qu'il renferme des renseignements précis et qu'il soit remis sous une forme et d'une manière conformes aux règlements. Selon les règlements, l'avis doit être remis par **écrit et inclure** :⁵

- une description des circonstances de l'incident;
- la date à laquelle ou la période pendant laquelle l'incident s'est produit ou se serait produit;
- le nom de l'organisme public ou du dépositaire de qui relevaient les renseignements (médicaux) personnels au moment où l'incident s'est produit;
- une description des renseignements (médicaux) personnels en cause;
- une description des mesures que l'organisme public ou le dépositaire a prises ou a l'intention de prendre à la date de l'avis afin de
 - réduire le risque de préjudice que pose l'incident pour le particulier
 - réduire le risque qu'un incident semblable se reproduise
- une description des mesures que le particulier peut prendre pour réduire le risque de préjudice pouvant résulter de l'incident ou pour atténuer le préjudice;
- une déclaration attestant que l'ombudsman du Manitoba a été ou sera avisé de l'incident, comme l'exige le paragraphe 19.0.1(4) de la LRMP ou le paragraphe 41.1(4) de la LAIPVP.
- le nom et les coordonnées d'un cadre ou d'un employé de l'organisme public ou du dépositaire qui peut répondre aux questions concernant l'incident;
- les autres renseignements que l'organisme public ou le dépositaire estime pertinents.

La version révisée de notre [Aide-mémoire pour rédiger un avis d'atteinte à la vie privée](#) résume les exigences d'un tel avis.

La notification obligatoire prévue par les lois exige également que l'avis soit remis **directement** au particulier, sauf dans les circonstances précises qui sont énoncées dans les règlements (consulter ci-dessous les « exceptions à la règle » pour les cas d'avis remis indirectement en la forme et selon la manière réglementaires).

Il vaut mieux aviser directement les personnes par écrit lorsque :

- leur identité est connue
- leurs coordonnées actuelles sont connues
- elles ont besoin de renseignements détaillés pour se protéger adéquatement contre les préjudices découlant de l'incident
- elles ont peut-être de la difficulté à comprendre un avis indirect (en raison de leur capacité mentale, de leur âge, de leur langue, etc.)

⁵ Consulter le paragraphe 3.2(1) du règlement de la LAIPVP et le paragraphe 8.8(1) du règlement de la LRMP

Exceptions à la règle

Même si la remise directe d'un avis écrit est parfois obligatoire ou si c'est la meilleure façon de faire, la LAIPVP et la LRMP prévoient des exceptions dans des circonstances bien précises :

1. Si l'organisme public ou le dépositaire a des motifs raisonnables de croire que le **délai** nécessaire pour remettre l'avis écrit au particulier risque d'accroître considérablement le risque réel de préjudice grave pour ce dernier, il **peut** lui donner l'avis verbalement à condition, selon le cas :⁶
 - a) au moment de le faire, qu'il consigne les renseignements fournis et la date à laquelle l'avis a été donné
 - b) dans un délai raisonnable après l'avoir fait, qu'il remette l'avis par écrit conformément au paragraphe (1)
2. L'avis peut être donné **indirectement** à un ou plusieurs particuliers dans les circonstances suivantes :
 - l'organisme public ou le dépositaire a des motifs raisonnables de croire que l'incident pourrait entraîner un risque pour la santé ou la sécurité publique
 - l'identité ou les coordonnées actuelles du particulier ne sont pas connues
 - l'organisme public ou le dépositaire a des motifs raisonnables de croire que la remise de l'avis directement et par écrit, selon le cas :
 - est peu pratique ou excessivement coûteuse en raison du grand nombre de particuliers ayant pu être touchés par l'incident
 - pourrait menacer la santé physique ou mentale du particulier, ou y nuire⁷
3. Dans les circonstances où l'avis peut être remis indirectement, il doit, selon le cas :
 - être remis au moyen d'une communication publique ou d'une autre mesure semblable permettant vraisemblablement de joindre le ou les particuliers touchés et ne divulguant aucun renseignement susceptible de les identifier;
 - dans le cas où l'atteinte à la vie privée risquerait vraisemblablement de menacer la santé physique ou mentale du destinataire ou d'y nuire, être remis au particulier qui fournit des soins au destinataire ou au particulier avec lequel le destinataire entretient des liens personnels étroits⁸ (par exemple, l'avis pourrait être donné au médecin, au fournisseur de services, au parent ou tuteur, ou à l'aidant de la personne)

Une communication publique consiste par exemple à publier un avis dans le site web de l'organisme public ou du dépositaire, dans les médias sociaux ou dans l'aire commune ou publique d'un immeuble ou d'une localité, ou à diffuser un communiqué de presse. Sachez que

⁶ Consulter le paragraphe 3.2(2) de la LAIPVP et le paragraphe 8.8(2) de la LRMP

⁷ Consulter le paragraphe 3.3(1) du règlement de la LAIPVP ou le paragraphe 8.8.1(1) du règlement de la LRMP

⁸ Consulter le paragraphe 3.3(2) du règlement de la LAIPVP ou le paragraphe 8.8.1(2) du règlement de la LRMP

le lieu de la communication publique devrait être choisi en fonction de sa capacité à joindre les personnes touchées par l'incident. L'emploi de plusieurs méthodes de notification publique est parfois la façon la plus efficace d'aviser toutes les personnes concernées.

Signaler les cas d'atteinte à la vie privée à l'ombudsman du Manitoba

Si votre évaluation détermine que le cas d'atteinte à la vie privée ne pose pas de *risque réel de préjudice grave* pour les personnes concernées, alors il n'est pas nécessaire de signaler l'incident à l'ombudsman du Manitoba. Cependant, nous vous encourageons à nous signaler ce genre d'incident lorsqu'il y a risque de préjudice pour la ou les personnes touchées et que vous n'êtes pas certain qu'un risque réel de préjudice grave a été subi ou qu'une consultation soit utile.

Lorsqu'il y a signalement à l'ombudsman du Manitoba d'un cas d'atteinte à la vie privée, la législation exige qu'il soit fait en la forme et de la manière prévues par l'ombudsman. Par conséquent, nous avons créé un [Formulaire de signalement d'atteinte à la vie privée](#). Veuillez utiliser ce formulaire, qui est publié dans notre site Web, pour signaler un tel incident, car il vous aidera à nous communiquer les renseignements dont nous avons besoin.

Pourquoi aviser l'ombudsman du Manitoba d'un cas d'atteinte à la vie privée?

En plus de respecter les obligations prévues en matière de signalement, le signalement à l'ombudsman du Manitoba d'un cas d'atteinte à la vie privée peut être considéré comme un acte positif :

- Le fait d'aviser les personnes concernées, ainsi que l'ombudsman, d'un cas d'atteinte à la vie privée est fondamentalement révélateur d'une culture d'entreprise qui respecte la vie privée.
- Cela montre que l'organisme public ou le dépositaire prend au sérieux la protection des renseignements (médicaux) personnels.
- Nous pouvons peut-être vous aider à établir un plan pour intervenir en cas d'atteinte à la vie privée et pour veiller à ce que des mesures soient prises afin d'empêcher que ce genre d'incident se reproduise.

En nous signalant l'incident, vous nous aidez aussi à répondre aux demandes de renseignements du public, à gérer les plaintes éventuelles que nous recevons à la suite de l'incident et à déterminer le type d'intervention que nous devons adopter, par exemple une discussion informelle ou la tenue d'une enquête.

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

Autres personnes à contacter

Que vous décidiez ou non qu'il est de votre devoir d'aviser 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 services technologiques** : 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 aviser en vertu d'obligations contractuelles.
- **Les organismes professionnels ou de réglementation** : s'il faut les aviser en vertu de normes professionnelles ou d'une réglementation.

Quatrième étape : prévenir d'autres atteintes à la vie privée

Après avoir pris des mesures immédiates pour limiter les risques associés au cas d'atteinte à la vie privée, l'organisme public ou le dépositaire devrait prendre le temps d'enquêter sur les causes de l'incident. Cela peut consister en une vérification des garanties physiques, techniques et administratives, comme celles qui suivent :

Garanties physiques – classeurs ou portes verrouillés, alarmes, accès des visiteurs
 Garanties techniques – chiffrement, mots de passe, accès des utilisateurs
 Garanties administratives – examen des politiques, formation sur la protection des renseignements

À la suite de l'enquête sur les causes et l'étendue de l'incident, il faut prévoir des mesures de protection à long terme contre de futures atteintes à la vie privée. Une liste de mesures couramment employées est publiée (en anglais) dans le site de Santé et Soins aux personnes âgées Manitoba.⁹

Il faut également passer en revue et mettre à jour régulièrement les politiques de façon qu'elles reflètent les leçons tirées de l'incident. Le plan qui en résulte devrait notamment prévoir une vérification obligatoire à la fin du processus pour veiller à ce que toutes les mesures de prévention ont été mises en œuvre.

Enfin, il faut que les membres du personnel reçoivent une formation pour être informés de leurs responsabilités dans le cadre de la LAIPVP et de la LRMP, et cette formation devrait être renouvelée périodiquement.

Révision - Janvier 2022

⁹ https://www.gov.mb.ca/health/phia/docs/security_safeguards.pdf

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 2018 par le CIPVP de l'Alberta; *Keys Steps to Responding to Privacy Breaches*, élaboré en mars 2015 par le CIPVP de la Nouvelle-Écosse et *Privacy Breach Guidelines for Government Institutions and Local Authorities*, élaboré en septembre 2021 par le CIPVP de la Saskatchewan. Nous sommes particulièrement redevables au Commissariat à la protection de la vie privée du Canada (CPVP) et au CIPVP de l'Alberta pour leur soutien et leur assistance dans notre travail de préparation en vue de la modification des lois du secteur public du Manitoba qui traitent du signalement des cas d'atteinte à la vie privée.