Étapes à suivre en cas d'atteintes à la vie privée

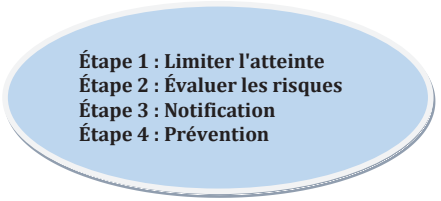
Bureau de révision de la Nouvelle-Écosse pour l’accès à l’information et la protection de la vie privée

Lignes directrices relatives aux atteintes à la vie privée[1]

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

On parle d'atteinte à la vie privée en cas d'accès non autorisé à des renseignements personnels, ou de collecte, d'utilisation, de divulgation ou d'élimination non autorisées de ces renseignements. Ces activités sont interdites si elles contreviennent à la loi sur l'accès à l'information et la protection de la vie privée (*Freedom of Information and Protection of Privacy Act* – FOIPOP), à la partie XX de la loi sur les administrations municipales (*Municipal Government Act* – MGA) ou à la loi sur les renseignements médicaux personnels (*Protection of Health Information Act* – PHIA).

Quelles sont les quatre étapes à suivre?



Les trois premières étapes devraient se produire dès la découverte d'une atteinte à la vie privée, ou rapidement l'une après l'autre. La quatrième étape, qui se produit une fois les causes de l'atteinte connues, vise à trouver des solutions à plus long terme.

But du présent document

Les atteintes à la vie privée peuvent prendre des formes très diverses. Il peut par exemple s'agir d'une télécopie mal adressée contenant des données fiscales, de la perte d'un disque dur contenant des renseignements personnels, ou encore de dossiers médicaux tombés de la benne d'un camion à ordures. En Nouvelle-Écosse, les organismes publics, les municipalités et les autorités de santé doivent être prêts à intervenir en cas d'atteintes à la vie privée. Les quatre étapes à suivre ont été adoptées par la plupart des provinces et territoires canadiens, tant dans le secteur public que privé. Il s'agit de pratiques exemplaires qui permettent d'atténuer les préjudices découlant d'une atteinte à la vie privée.

Veuillez utiliser ce document avec la liste de contrôle qui se trouve à la page 13 ainsi que sur notre site Web à http://foipop.ns.ca.

[1] Cette brochure est une adaptation du guide du Commissariat à l'information de la Colombie-Britannique, intitulé : *Privacy Breaches: Tools and Resources* disponible au https://www.oipc.bc.ca/tools-guidance/guidance-documents.

Autres ressources pour les autorités de santé

Notez que la loi sur les renseignements médicaux personnels (PHIA) prévoit aux articles 69 et 70 des exigences particulières en matière de notification. Selon ces dispositions, il devrait avoir notification dans certaines circonstances, notamment lorsque « des renseignements sont volés ou perdus ou que leur accès, utilisation, divulgation, copie ou modification ne sont pas autorisés ». Le gouvernement de la Nouvelle-Écosse a créé un outil, appelé *Privacy Breach Notification Decision Making Tool,* pour aider les autorités de santé à déterminer le type de notification requise en vertu de la loi sur les renseignements médicaux personnels (PHIA). La notification des atteintes à la vie privée fait partie des quatre étapes abordées ici. Les autorités de santé peuvent en outre se servir du présent document pour évaluer les mesures prises en cas d'atteinte à la vie privée.

Avis à l'utilisateur

Ce document a pour seul but de fournir des informations de nature générale. Son contenu ne saurait donc constituer une opinion juridique. En tant qu'organisme indépendant chargé de surveiller le respect de la loi sur l'accès à l'information et la protection de la vie privée (FOIPOP), de la loi sur les administrations municipales (MGA) et de la loi sur les renseignements médicaux personnels (PHIA), le Bureau de révision pour l'accès à l'information et la protection de la vie privée (le « Bureau ») ne peut pas approuver au préalable la proposition d'un organisme public, d'une municipalité ou d'une autorité de santé. Nous devons maintenir notre capacité à enquêter sur les plaintes et à formuler des recommandations en lien avec celles-ci. Le contenu du présent document n'entrave pas les capacités du Bureau ni ne crée d'obligations pour ce dernier, quelles que soient les questions examinées (enquête sur une plainte ou autre); et le Bureau doit faire preuve d'ouverture d'esprit dans chaque cas. Il incombe à chaque organisme public, municipalité et autorité de santé de veiller au respect des responsabilités qu'impose la loi. Les coordonnées de l'agent de révision se trouvent à la page 22 de ce document. Pour en savoir plus sur notre rôle et notre mandat, veuillez consulter le site suivant: http://foipop.ns.ca (en anglais seulement).

Étape 1 : Limiter une atteinte à la vie privée

Avant de continuer, assurez-vous de consigner toutes les mesures prises relatives à une atteinte à la vie privée (enquête, gestion, etc.). La liste de contrôle permet de compléter les mesures présentées ci-dessous ainsi que de noter toutes les informations utiles. Cette liste se trouve à la page 13 du présent document ainsi qu'au http://foipop.ns.ca.

Vous devez prendre sans tarder des mesures de bon sens pour limiter une atteinte à la vie privée.

- **Limiter une atteinte :** Limitez immédiatement l'atteinte, par exemple en mettant fin à la pratique non autorisée, en éteignant le système qui fait l'objet de la brèche, en révoquant ou en changeant les codes d'accès informatiques, en envoyant un signal d'annulation au dispositif de stockage portable perdu ou volé, en corrigeant les lacunes des systèmes de sécurité matériels ou en faisant des recherches dans un quartier ou sur un site de vente d'objets usagés (comme Kijiji) afin d'y repérer les objets qui ont été volés dans une voiture ou une maison.

- **Enquête initiale :** Désignez une personne qualifiée pour la tenue de l'enquête initiale. Lancez ce processus le jour de la découverte de l'atteinte à la vie privée. Cette personne devrait avoir la latitude voulue au sein de l'organisation pour mener l'enquête initiale et formuler des recommandations. Une enquête plus minutieuse pourrait être réalisée par la suite, si besoin est.

- **Notifiez le responsable de la protection des renseignements personnels et d'autres personnes :** Contactez immédiatement votre responsable de la protection des renseignements personnels ainsi que la personne responsable de la sécurité dans votre organisation. Déterminez qui doit être mis au courant de l'incident à l'interne. Il est utile de préparer une liste de toutes les personnes devant être contactées, avec les coordonnées correspondantes.

- **Équipe d'intervention :** Déterminez s'il est nécessaire de mettre sur pied une équipe composée de représentants des différents échelons et services de l'entreprise (relations de travail, service juridique, communications, haute direction). Des représentants du service de protection de la vie privée et de la sécurité doivent toujours faire partie de cette équipe, et celle-ci est généralement responsable de coordonner le travail d'intervention.

- **Police :** Si l'atteinte à la vie privée est associée à un vol ou à une autre activité criminelle, la police doit en être avisée.

- **Préservez les preuves :** Ne nuisez pas à la capacité d'enquêter sur l'incident. Prenez garde de ne pas détruire des éléments de preuve pouvant permettre de déterminer la cause de l'incident ou vous permettre de prendre les mesures correctives qui s'imposent.

Étape 2 : Évaluez les risques

Pour déterminer toute autre mesure devant être prise immédiatement, vous devez évaluer les risques qui existent. Il faut donc tenir compte des facteurs suivants :

Renseignements personnels en cause :

- Obtenez dès que possible la liste complète des renseignements personnels à risque. En général, cela signifie dresser la liste des données perdues, volées ou auxquelles on a accédé sans autorisation. Il peut par exemple s'agir des renseignements suivants : nom, adresse, date de naissance, diagnostic médical et numéro de carte de santé (MSI). À ce stade, il est important que l'enquêteur confirme le plus rapidement possible les données à risque. Sachez que si le problème provient d'une erreur ou de la négligence d'un employé, il se peut que celui-ci hésite à divulguer tout ce qui a été perdu.

- Évaluez ensuite la mesure dans laquelle les renseignements personnels sont sensibles. Certains renseignements personnels sont plus sensibles que d'autres. Il s'agit en général de renseignements sur la santé, pièces d'identité émises par le gouvernement, comme les numéros d'assurance sociale, de carte d'assurance-maladie et de comptes de banque ou de cartes de crédit.

- Tenez compte également du contexte lié aux renseignements personnels. Par exemple, il se peut que la liste d'un livreur de journaux comportant des noms d'abonnés ne soit pas de nature sensible. Toutefois, la liste des abonnés ayant demandé une interruption de service pendant leurs vacances est plus sensible.

- Tenez compte enfin de l'utilisation possible des renseignements personnels. Il arrive parfois que des renseignements, pris ensemble, deviennent sensibles ou puissent servir à des fins frauduleuses ou autrement préjudiciables.

- Plus des renseignements sont sensibles, plus le risque est élevé.

Cause et étendue d'une atteinte à la vie privée :

L'analyse des risques doit tenir compte de la cause et de l'étendue de l'atteinte. Répondez aux questions suivantes :

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

aux renseignements personnels, leur utilisation ou leur communication risquent de se poursuivre, y compris par l'entremise de médias de masse ou en ligne?
- Les renseignements ont-ils été perdus ou volés? S'ils ont été volés, peut-on déterminer s'ils étaient la cible du vol?
- Les renseignements sont-ils chiffrés ou difficiles d'accès?
- Les renseignements personnels ont-ils été retrouvés?
- Quelles mesures ont déjà été prises pour atténuer les préjudices?
- S'agit-il d'un problème systémique ou d'un incident isolé?

Personnes concernées par l'atteinte à la vie privée

Savoir qui est concerné permet d'élaborer une stratégie d'intervention et de déterminer les personnes chargées d'intervenir (p. ex. si les personnes concernées par l'atteinte sont syndiquées, des responsables des relations de travail devraient faire partie de l'équipe d'intervention). Cela permet de plus de déterminer les personnes à notifier (p. ex. si des partenaires de votre entreprise sont concernés, il faudra alors probablement les informer).

- Combien de personnes sont concernées par l'atteinte?
- Qui est concerné (employés, public, entrepreneurs, clients, prestataires de services, autres organisations)?

Préjudices prévisibles découlant de l'atteinte

- Qui a reçu les renseignements? Par exemple, un anonyme qui reçoit accidentellement des renseignements personnels et signale de lui-même l'erreur est moins susceptible d'en faire un usage abusif qu'un individu soupçonné d'activités criminelles.

- Existe-t-il un lien entre les destinataires non autorisés et la personne concernée? L'existence d'une relation étroite entre la victime et le destinataire des renseignements peut accroître la probabilité du préjudice, p. ex. un ancien conjoint est plus susceptible qu'un voisin de mal utiliser des renseignements.

- Quel préjudice l'atteinte peut-elle causer aux personnes concernées? Exemples :
    - risque pour la sécurité (p. ex. la sécurité physique);
    - vol d'identité ou fraude;
    - pertes d'activités commerciales ou de possibilités d'emploi;
    - souffrance, humiliation, atteinte à la réputation ou détérioration des relations;
    - action discriminatoire possible à l'endroit de la personne;
    - Préjudice social ou relationnel (détérioration des relations de la personne).

- Quel préjudice l'atteinte peut-elle causer à l'organisme public ou à l'organisation concerné? Exemples :
    - perte de confiance dans l'organisme public ou l'organisation;
    - perte de biens;

- risques financiers, dont poursuites en recours collectifs;
- perte de contrats ou d'activités commerciales.

- Quel préjudice l'atteinte peut-elle causer au public? Exemples :
  - risque pour la santé publique;
  - risque pour la sécurité publique.

Une fois les risques en question évalués, vous pouvez déterminer si la notification constitue une stratégie d'atténuation adaptée. En outre, l'évaluation des risques permet de déterminer les stratégies de prévention appropriées.

Le tableau qui suit résume les facteurs de risque et propose des niveaux de risque **possibles.** Chaque organisme public, autorité de santé et municipalité doit procéder à une évaluation des risques propres aux circonstances. Ce tableau offre une description générale de chaque niveau de risque.

Survol des niveaux de risque			
Facteur	**Niveaux de risque**		
	Faible	Moyen	Élevé
Nature des renseignements personnels	✓ Renseignements personnels auxquels le public a accès, non associés à d'autres renseignements	✓ Renseignements personnels, non médicaux ou financiers, propres à l'organisation	✓ Renseignements médicaux, psychologiques, liés à du counselling ou financiers; ou numéros d'identification propres au gouvernement
Relations	✓ Communication accidentelle à un autre professionnel qui a signalé l'atteinte à la vie privée et a confirmé la destruction ou le retour des renseignements	✓ Communication accidentelle à un anonyme qui a signalé l'atteinte à la vie privée et a confirmé la destruction ou le retour des renseignements	✓ Divulgation à une personne ayant une relation avec le ou les individus concernés ou connaissant ces derniers, en particulier un(e) ancien(ne) conjoint(e), des membres de la famille, des voisins ou des collègues ✓ Vol par une personne inconnue
Cause de l'atteinte à la vie privée	✓ Erreur technique qui a été résolue	✓ Perte ou divulgation accidentelle	✓ Atteinte intentionnelle. ✓ Cause inconnue. ✓ Erreur technique - non résolue
Étendue	✓ Très peu de personnes concernées	✓ Groupe limité et identifié de personnes concernées	✓ Grand groupe ou totalité d'un groupe, personnes non identifiées

Survol des niveaux de risque			
Facteur	**Niveaux de risque**		
	Faible	Moyen	Élevé
Efforts pour limiter l'atteinte	✓ Les données étaient convenablement chiffrées ✓ Le contenu du dispositif de stockage portable a été effacé à distance, et il est établi que personne n'a accédé au contenu avant sa suppression ✓ Les documents papier ou le dispositif ont été récupérés presque immédiatement, et tous les fichiers semblent intacts ou ne pas avoir été lus	✓ Le contenu du dispositif de stockage portable a été effacé à distance dans les heures qui ont suivi la perte, mais rien ne permet d'établir que ce contenu n'a pas été lu avant sa suppression ✓ Les documents papier ou le dispositif ont été récupérés, mais suffisamment de temps s'est écoulé entre la perte du dispositif et sa récupération pour pouvoir accédé à son contenu	✓ Les données n'étaient pas chiffrées ✓ Les données, les fichiers ou le dispositif n'ont pas été récupérés ✓ Les données risquent d'être communiquées à un plus grand nombre de personnes, à travers des médias de masse ou en ligne
Préjudices prévisibles découlant de l'atteinte	✓ Pas de préjudices prévisibles découlant de l'atteinte	✓ Pertes d'activités commerciales ou de possibilités d'emploi ✓ Souffrance, humiliation, atteinte à la réputation ou détérioration des relations ✓ Préjudice social/relationnel. ✓ Perte de confiance dans l'organisme public ✓ Perte de biens appartenant à l'organisme public. ✓ Perte de contrats ou d'activités commerciales par l'organisme public ✓ Risques financiers, dont poursuites en recours collectifs	✓ Risque pour la sécurité (p. ex. la sécurité physique). ✓ Vol d'identité ou risque de fraude ✓ Souffrance, humiliation, atteinte à la réputation : risque élevé selon les circonstances ✓ Risque pour la sécurité ou la santé publique

Étape 3 : Notification

La notification peut constituer une stratégie d'atténuation des risques et donc offrir des avantages à toutes les entités (organisme public, municipalité, autorité de santé) et personnes concernées. Notifier rapidement les personnes concernées leur permet de prendre des mesures pour se protéger. La difficulté consiste à déterminer le moment auquel il faut procéder à la notification. Chaque incident doit être examiné au cas par cas afin de déterminer si l'atteinte à la vie privée doit faire l'objet d'une notification. Par ailleurs, les organismes publics, municipalités et autorités de santé sont invités à communiquer avec le Bureau de révision pour l'accès à l'information et la protection de la vie privée afin d'obtenir de l'aide concernant la gestion des atteintes à la vie privée.[2]

Passez en revue votre évaluation des risques pour déterminer si la notification est appropriée. Si des renseignements sensibles sont à risque, si ces renseignements sont susceptibles d'être mal utilisés ou s'il y a des préjudices prévisibles, vous voudrez alors probablement notifier les personnes concernées. La liste ci-dessous contient des informations destinées à faciliter vos prises de décisions.

Remarque pour les autorités de santé : La loi sur les renseignements médicaux personnels (PHIA) impose certaines exigences, car selon les articles 69 et 70, les personnes concernées par une atteinte à la vie privée ou le Bureau de révision doivent en être notifiés.

La loi sur l'accès à l'information et la protection de la vie privée (FOIPOP) et la partie XX de la loi sur les administrations municipales (MGA) n'imposent pas une telle notification. Comme il est indiqué ci-dessus toutefois, procéder à une notification, dans les circonstances appropriées, constitue une bonne pratique qui contribue à atténuer les pertes subies par des personnes suite à une atteinte à la vie privée. Les mesures prises alors peuvent considérablement réduire le préjudice, ce qui sera pris en compte lors d'une action en justice pour atteinte à la vie privée.

Notifier les personnes concernées

Comme il est indiqué ci-dessus, il faut notifier les personnes concernées si cela est nécessaire pour éviter ou atténuer tout préjudice. Voici certains facteurs dont il faut tenir compte pour décider s'il convient de notifier les personnes concernées :

- La loi exige une notification — p. ex. en vertu des articles 69 et 70 de la loi sur les renseignements médicaux personnels (PHIA);
- obligations contractuelles exigeant une notification;

[2] Le Bureau de révision est chargé de surveiller l'application des dispositions en matière de confidentialité et peut donner des conseils et faire des observations sur ces dispositions lorsqu'un organisme public ou une autorité de santé lui en fait la demande. Voir nos coordonnées à la page 22.

- il y a risque de vol d'identité ou de fraude — le plus souvent en raison du type de renseignements perdus, volés, consultés ou divulgués, comme un NAS, des données bancaires ou des numéros d'identification;
- il y a risque de préjudice physique — si en raison de la perte des renseignements un individu peut être harcelé;
- il y a risque de souffrance, d'humiliation ou d'atteinte à la réputation — p. ex. lorsque les renseignements perdus proviennent de dossiers médicaux et de mesures disciplinaires;
- il y a risque de pertes d'activités commerciales ou de possibilités d'emploi — si la perte des renseignements peut entraîner une atteinte à la réputation d'une personne;
- il y a risque de perte de confiance dans l'organisme public ou l'organisation, ou la notification est appropriée pour préserver de bonnes relations entre citoyens.

Quand et comment notifier

Les personnes concernées devraient être notifiées le plus tôt possible après l'atteinte, c'est-à-dire dans les jours qui suivent (dans la mesure du possible). Cependant, si vous avez communiqué avec des responsables de l'application de la loi, il conviendrait de leur demander si la notification devrait être différée pour ne pas compromettre la tenue de l'enquête.

En de très rares occasions, il arrive qu'en raison de preuves médicales on puisse raisonnablement s'attendre à ce que la notification de la personne concernée entraîne chez elle un préjudice grave et immédiat à sa santé mentale ou physique. En l'occurrence, il faut envisager d'autres approches, p. ex. demander à un médecin de notifier la personne ou attendre que les risques immédiats disparaissent.

Il est préférable de notifier directement les personnes concernées (par téléphone, courrier ou en personne). On ne devrait généralement recourir à la notification indirecte (au moyen de sites Web, d'avis publics, de médias) qu'exceptionnellement, par exemple si la notification directe est susceptible de causer davantage de préjudices ou que les coordonnées des personnes concernées sont inconnues.

Il pourrait être approprié, dans certains cas, d'utiliser plusieurs méthodes de notification.

Quel devrait être le contenu d'une notification?

Une notification doit contenir les renseignements suivants :

- date de l'atteinte;
- description de l'atteinte;
- description des renseignements auxquels on a accédé et collectés, utilisés et divulgués sans autorisation;

- risque(s) pour l'individu en raison de l'atteinte;
- mesures prises jusqu'à présent pour contrôler ou réduire les préjudices;
- en cas de risque de vol d'identité, la notification devrait en général, dans le cadre de la stratégie d'atténuation, suggérer des mesures gratuites de protection de crédit;
- autres mesures envisagées pour prévenir les futures atteintes à la vie privée;
- mesures que la personne peut prendre pour atténuer encore plus le risque de préjudice (p. ex. comment contacter les agences d'évaluation du crédit pour mettre en place des mesures de surveillance, expliquer comment obtenir un nouveau numéro d'assurance-maladie ou de permis);
- coordonnées d'une personne au sein de l'organisme public, de la municipalité ou de l'autorité de santé pouvant répondre aux questions ou fournir des renseignements supplémentaires;
- coordonnées de l'agent de révision; indiquer le droit des personnes de porter plainte auprès de l'agent de révision en vertu de la loi sur l'agent de révision à la protection de la vie privée (*Privacy Review Officer Act*) et de la loi sur les renseignements médicaux personnels (PHIA). Si l'organisme public, la municipalité ou l'autorité de santé a déjà pris contact avec l'agent de révision, indiquez-le dans la lettre de notification.

Autres sources d'information

Comme il est indiqué plus haut, la lettre de notification devrait comprendre le numéro de téléphone de l'organisme public, de la municipalité ou de l'autorité de santé, au cas où les personnes concernées souhaitent obtenir un complément d'information. Il est de plus utile de dresser une liste des questions fréquemment posées ainsi que des réponses correspondantes pour aider le personnel à traiter les demandes de renseignements.

Autres personnes à notifier

Quelles que soient, selon vous, vos obligations quant à la notification des personnes concernées par l'atteinte, vous devriez déterminer si les autorités ou organismes suivants doivent être informés de l'atteinte à la vie privée :

- Police — en cas de vols ou d'activités criminelles présumés;
- Compagnies d'assurances ou autres — si des obligations contractuelles l'exigent;
- Ordres professionnels ou organismes de réglementation — si les normes professionnelles ou réglementaires l'exigent;

- Autres parties internes ou externes qui n'ont pas déjà été notifiées — l'enquête et l'analyse des risques ont peut-être permis d'identifier d'autres parties concernées par l'atteinte, comme des entrepreneurs tiers, des unités commerciales internes ou des syndicats;

- Bureau de révision — dont le mandat est de surveiller l'application des dispositions en matière de confidentialité ainsi que de donner des conseils et de faire des observations sur ces dispositions lorsqu'un organisme public ou une autorité de santé lui en fait la demande.

  Les facteurs suivants permettent de déterminer si une atteinte à la vie privée doit être signalée au Bureau de révision :

  - pour les autorités de santé, l'article 70 de la loi sur les renseignements médicaux personnels (PHIA) énonce les situations pour lesquelles le Bureau de révision doit être notifié. Les autorités de santé peuvent, en fonction des facteurs énumérés ci-dessous, communiquer avec le Bureau de révision, même lorsque la notification de ce dernier n'est pas nécessaire.

  - degré de sensibilité des renseignements — en général, plus les renseignements à risque sont sensibles, plus il est probable que le Bureau de révision doive être notifié;

  - les renseignements divulgués peuvent servir à un vol d'identité;

  - il existe un risque raisonnable de préjudice découlant de l'atteinte à la vie privée, y compris des pertes non financières;

  - le nombre de personnes concernées par l'atteinte;

  - on a récupéré tous les renseignements et donc limité leur communication;

  - l'organisme public, la municipalité ou l'autorité de santé souhaite obtenir des conseils ou des commentaires de la part de l'agent de révision pour l'aider à gérer l'atteinte à la vie privée;

  - l'organisme public, la municipalité ou l'autorité de santé a besoin d'aide pour créer une procédure d'intervention relative aux atteintes à la vie privée, y compris la notification;

  - l'organisme public, la municipalité ou l'autorité de santé craint que la notification ne puisse entraîner d'autres préjudices;

  - s'assurer que les mesures prises sont conformes aux obligations qu'imposent à l'organisme public les lois en matière de vie privée.

Étape 4 : Prévention

Une fois que les mesures immédiates sont prises pour réduire les risques associés à l'atteinte à la vie privée, il faut prendre le temps d'enquêter sur les causes de l'incident, ce qui peut nécessiter un audit de sécurité physique et technique. Cette évaluation peut servir à mettre en place des mesures de prévention adéquates à long terme ou améliorer celles qui existent déjà.

En général, les stratégies de prévention ciblent les contrôles de la protection des renseignements personnels pour tous les aspects suivants :

- physique;
- technique;
- administratif;
- personnel.

Ainsi, si par exemple une atteinte à la vie privée découle de lacunes au plan de la sécurité physique, il faut alors procéder à des changements pour empêcher toute récidive. Il faut également examiner les mesures de contrôle des systèmes pour s'assurer que toutes les mesures de protection techniques nécessaires sont en place. Il peut par exemple s'agir de chiffrer les données contenues dans les dispositifs de stockage portables ou d'améliorer le pare-feu d'une base de données.

En ce qui concerne les mesures de contrôle administratif, il peut par exemple s'agir de mettre à jour des politiques à partir des leçons tirées de l'enquête, puis procéder ensuite à des mises à jour régulières. Votre plan d'action devrait également prévoir une obligation de vérification à la fin du processus, pour s'assurer de la mise en œuvre intégrale du plan de prévention. Si un protocole relatif aux atteintes à la vie privée n'est pas déjà en place, assurez-vous que votre plan d'action prévoie l'élaboration d'un tel protocole.

Le personnel des organismes publics, des municipalités et des autorités de santé doit être formé aux obligations qu'imposent, en matière de protection de la vie privée, la loi sur l'accès à l'information et la protection de la vie privée (FOIPOP), la partie XX de la loi sur les administrations municipales (MGA) ainsi que la loi sur les renseignements médicaux personnels (PHIA).

À plus long terme, les organismes, les municipalités et les autorités de santé devraient mettre à jour leur cadre de gestion de la vie privée pour veiller à ce qu'ils continuent à satisfaire à leurs obligations en matière confidentialité. Pour plus d'information sur les cadres de gestion de la vie privée, veuillez consulter le site Web du Bureau de révision à l'adresse suivante : http://foipop.ns.ca (en anglais seulement).

Liste de contrôle concernant les atteintes à la vie privée

Bureau de révision de la Nouvelle-Écosse pour l'accès à l'information et la protection de la vie privée

Liste de contrôle concernant les atteintes à la vie privée

Veuillez vous servir de cette liste pour évaluer la façon dont vous gérez les atteintes à la vie privée et pour décider si vous devez signaler une atteinte au Bureau de révision de la Nouvelle-Écosse pour l'accès à l'information et la protection de la vie privée[3]. Pour obtenir davantage d'explications sur la gestion d'une atteinte à la vie privée, veuillez consulter le document *Étapes à suivre en cas d'atteintes à la vie privée*, sur le site http://foipop.ns.ca.

Date du rapport : _____

Date à laquelle l'atteinte a été découverte : _____

Coordonnées :

Organisme public/Autorité de santé/Municipalité : _____

Personne-ressource (auteur du rapport) : _____

Titre : _____

Téléphone : _____ Télécopieur : _____

Courriel : _____

Adresse postale : _____

Description de l'incident

Décrire la nature de l'atteinte à la vie privée et sa cause. Comment l'atteinte a-t-elle été découverte et quand? Où l'atteinte a-t-elle eu lieu?

_____

_____

_____

[3] Dans le cadre de son mandat, le Bureau de révision est chargé de surveiller l'application des dispositions en matière de confidentialité et peut donner des conseils et faire des observations sur ces dispositions lorsqu'un organisme public ou une autorité de santé lui en fait la demande.

Étapes 1 et 2 : Limitation de l'atteinte à la vie privée et évaluation des risques

Répondez à chacune des questions suivantes puis faites l'évaluation des risques (page 17) en fonction de vos réponses.

(1) Limitation

Cochez tous les facteurs qui s'appliquent:

- ❑ Les renseignements personnels ont été récupérés et toutes les copies sont maintenant sous notre garde et notre contrôle
- ❑ Nous avons la confirmation qu'aucune copie n'a été faite
- ❑ Nous avons la confirmation que les renseignements personnels ont été détruits
- ❑ Nous pensons (sans en avoir la confirmation) que les renseignements personnels ont été détruits
- ❑ Les renseignements personnels sont chiffrés
- ❑ Les renseignements personnels n'étaient pas chiffrés
- ❑ Selon les preuves recueillies pour l'instant, l'incident provient probablement d'un problème systémique
- ❑ Selon les preuves recueillies pour l'instant, il s'agit probablement d'un incident isolé
- ❑ Les renseignements personnels n'ont pas été retrouvés, mais les mesures de limitation suivantes ont été prises (cochez tout ce qui s'applique):
  - ❑ Le voisinage immédiat du vol a été entièrement fouillé
  - ❑ Les sites Web de vente d'objets usagés sont surveillés, mais l'article n'y a pas encore été annoncé
  - ❑ Les prêteurs sur gages sont surveillés
  - ❑ Un signal de suppression à distance a été envoyé vers l'appareil, mais aucune confirmation liée à l'efficacité de ce signal n'a été reçue
  - ❑ Un signal de suppression à distance a été envoyé vers l'appareil, et nous avons la confirmation que le signal a fonctionné
  - ❑ Notre vérification des systèmes confirme que personne n'a accédé au contenu du dispositif de stockage portable
  - ❑ Nous n'avons pas de vérification confirmant que personne n'a accédé au contenu du dispositif de stockage portable
  - ❑ Tous les mots de passe et noms d'utilisateur ont été modifiés

Décrivez toutes les autres stratégies de limitation:

_____

_____

_____

_____

(2) Nature des renseignements personnels

Liste de toutes les données concernées (p. ex. noms, dates de naissance, numéros d'assurance sociale, adresses, diagnostics médicaux, liens avec des prestataires de service comme l'aide sociale ou des services de counselling, etc.)

- ❑ Nom
- ❑ Adresse
- ❑ Date de naissance
- ❑ Numéros de pièces d'identité gouvernementales (préciser) _____
- ❑ NAS
- ❑ Données financières
- ❑ Données médicales
- ❑ Caractéristiques personnelles comme la race, la religion, l'orientation sexuelle
- ❑ Autre (décrire)

_____

_____

_____

_____

(3) Relation

Quelle est la relation entre le destinataire des renseignements et les personnes concernées par l'atteinte à la vie privée?

- ❑ Personne inconnue
- ❑ Ami
- ❑ Voisin
- ❑ Ancien(ne) conjoint(e)
- ❑ Collègue
- ❑ Relation inconnue
- ❑ Autre (décrire)

_____

_____

_____

_____

(4) Cause de l'atteinte à la vie privée

Selon votre enquête initiale, quelle est votre première évaluation de la cause de l'atteinte à la vie privée?

- ❑ Accident ou négligence
- ❑ Erreur technique
- ❑ Vol intentionnel ou faute
- ❑ Navigation non autorisée
- ❑ Cause inconnue
- ❑ Autre (décrire)

_____

_____

_____

(5) Étendue de l'atteinte à la vie privée

Combien de personnes sont concernées par l'atteinte?

- ❑ Très peu (moins de 10)
- ❑ Groupe limité et identifié (>10 et <50)
- ❑ Nombre important de personnes touchées (>50)
- ❑ Le nombre de personnes touchées n'est pas connu.

(6) Préjudices prévisibles

Déterminez les types de préjudice pouvant découler de l'atteinte. Certains préjudices se rapportent seulement aux personnes concernées, mais l'organisme public et d'autres personnes peuvent subir un préjudice s'il n'y a pas notification :

- ❑ **Vol d'identité** (le plus susceptible de se produire lorsque l'atteinte concerne la perte d'un NAS, de numéros de cartes de crédit, de numéros de permis de conduire, de renseignements sur une carte de débit, etc.)
- ❑ **Préjudice physique** (la personne concernée risque d'être harcelée)
- ❑ **Souffrance, humiliation, atteinte à la réputation** (associées à la perte de renseignements comme des dossiers sur la santé mentale, des dossiers médicaux, des dossiers de mesures disciplinaires)
- ❑ **Perte d'activités commerciales ou de possibilités d'emploi** (généralement à la suite d'une atteinte à la réputation d'un individu)
- ❑ **Violation d'obligations contractuelles** (les dispositions contractuelles peuvent exiger la notification de tiers en cas de pertes de données ou d'une atteinte à la vie privée)
- ❑ **Atteintes futures causées par des défaillances techniques** (il peut être nécessaire de notifier le fabricant si un rappel est justifié, ou pour empêcher toute autre atteinte de la part d'autres utilisateurs)
- ❑ **Non-respect de normes professionnelles ou de normes de certification** (notifier l'organe professionnel de réglementation ou l'autorité de certification peut être nécessaire)
- ❑ **Autre** (préciser)
  _____

(7) Autres facteurs

La nature de la relation entre l'organisme public et les personnes concernées peut être telle que l'organisme souhaite notifier ces personnes par souci de préserver des relations de confiance avec elles, peu importe les autres facteurs. Prenez en compte les types de personnes concernées par l'atteinte.

- ❑ Clients/patients
- ❑ Employés
- ❑ Étudiants ou bénévoles
- ❑ Autre (décrire)

_____

Résumé de l'évaluation des risques :

Déterminez la cote de risque pour chacun des facteurs indiqués ci-dessus. Pour ce faire, servez-vous de l'Annexe 1 : Survol des facteurs de risque.

Facteurs de risque	**Cote de risque**		
	Faible	Moyen	Élevé
1) Limitation			
2) Nature des renseignements personnels			
3) Relation			
4) Cause de l'atteinte à la vie privée			
5) Étendue de l'atteinte à la vie privée			
6) Préjudices prévisibles découlant de l'atteinte à la vie privée			
7) Autres facteurs			
Cote de risque globale			

Servez-vous de la cote de risque pour décider si une notification est nécessaire ainsi que pour créer des stratégies de prévention. La décision de notifier les personnes concernées dépend généralement des préjudices prévisibles découlant de l'atteinte à la vie privée. Voir l'analyse détaillée à l'étape 3. En général cependant, une cote de risque moyenne ou élevée entraîne toujours la notification des personnes concernées. Une cote de risque faible peut également entraîner la notification des personnes concernées, selon les circonstances propres à chaque cas.

Étape 3 : Notification

1. Les personnes concernées doivent-elles être notifiées?

Une fois la cote de risque globale établie, déterminez s'il faut notifier les personnes concernées. Si l'un des facteurs suivants s'applique, la notification doit avoir lieu. Si le test relatif à la loi sur les renseignements médicaux personnels (PHIA) est concluant, il doit y avoir notification.

Aspects	Description	Facteur pertinent
Lois	En Nouvelle-Écosse, les autorités de santé doivent se conformer aux articles 69 et 70 de la loi sur les renseignements médicaux personnels (PHIA), lesquels exigent une notification des personnes concernées	
Risque de vol d'identité	Le plus susceptible de se produire lorsque l'atteinte concerne la perte d'un NAS, de numéro de cartes de crédit, de numéro de permis de conduire, de renseignements sur une carte de débit, etc.	
Risque de préjudice physique	La personne concernée risque d'être harcelée	
Risque de souffrance, d'humiliation, d'atteinte à la réputation	Souvent associé à la perte de renseignements comme des dossiers sur la santé mentale, des dossiers médicaux ou des dossiers de mesures disciplinaires	
Pertes d'activités commerciales ou de possibilités d'emploi	Lorsque l'atteinte peut nuire à la réputation d'une personne au plan professionnel	
Explication requise	L'organisme public peut souhaiter notifier les personnes concernées si celles-ci sont vulnérables ou si elles ont besoin d'informations pour bien comprendre les événements, même si on juge les risques peu élevés	
Réputation de l'organisme public	Lorsque l'organisme public craint que la violation ne sape la confiance des citoyens, il peut alors décider de les notifier afin d'apaiser leurs inquiétudes ainsi que leur fournir des informations claires sur les risques et les stratégies d'atténuation mises en place, même lorsque les risques évalués sont faibles	

2. Quand et comment notifier

Quand : La notification doit avoir lieu dès que possible après une atteinte. Cependant, si vous avez communiqué avec des responsables de l'application de la loi, il conviendrait de leur demander si la notification devrait être différée pour ne pas compromettre la tenue de l'enquête.

Comment : Il est préférable de notifier une personne par téléphone, courrier, courriel ou en personne. On ne devrait généralement recourir à la notification indirecte (au moyen de sites Web, d'avis publics, de médias) que si la notification directe est susceptible de causer davantage de préjudices, que les coûts afférents sont excessifs ou que les coordonnées sont inconnues. Il pourrait être approprié, dans certains cas, d'utiliser plusieurs méthodes de notification.

Aspects pour lesquels une notification directe est préférable	**Cochez si applicable**
L'identité des personnes est connue	
Les coordonnées des personnes concernées sont disponibles	
Les personnes concernées par l'atteinte à la vie privée ont besoin d'informations détaillées afin de pouvoir bien se protéger contre le préjudice découlant de l'atteinte	
Les personnes concernées par l'atteinte peuvent avoir du mal à comprendre une notification indirecte (en raison de leur capacité mentale, âge, langue, etc.)	
Aspects pour lesquels une notification indirecte est préférable	
Les personnes concernées par l'atteinte sont très nombreuses, rendant ainsi peu pratique une notification directe	
La notification directe pourrait aggraver les préjudices découlant de l'atteinte	

3. Contenu d'une lettre de notification

Le contenu de la lettre de notification doit aider les personnes concernées à réduire ou à prévenir les préjudices pouvant découler de l'atteinte. Indiquez dans la lettre tout ce qui suit:

Éléments essentiels d'une lettre de notification d'atteinte à la vie privée	**Inclus(e)**
Date de l'atteinte	
Description de l'atteinte	
Description des renseignements personnels concernés	
Mesures prises pour l'instant pour contrôler ou réduire les préjudices (limitation)	
Autres mesures envisagées pour prévenir les futures atteintes à la vie privée	
Mesures que les personnes peuvent prendre — envisagez d'offrir des mesures de surveillance du crédit, le cas échéant	
Coordonnées de l'agent de révision — les personnes ont le droit de porter plainte auprès de l'agent de révision	
Coordonnées de l'organisme public, de la municipalité ou de l'autorité de santé — pour tout aide supplémentaire	

4. Autres personnes à notifier

Autorité ou organisation	Raison	Applicable
Forces de l'ordre	Si un vol ou un crime est soupçonné	
Agent de révision	• Pour obtenir de l'aide relative à l'élaboration d'une procédure d'intervention en cas d'atteinte à la vie privée, y compris une notification; pour s'assurer que les mesures prises sont conformes aux obligations prévues par les lois encadrant le respect de la vie privée • Les renseignements personnels sont sensibles • Il y a risque de vol d'identité ou d'autres préjudices importants • Les personnes concernées sont nombreuses. • Les renseignements personnels n'ont pas encore été tous retrouvés • L'atteinte découle d'un problème systémique, ou une atteinte semblable à déjà eu lieu	
Organes professionnels ou réglementaires	Si les normes professionnelles ou réglementaires exigent la notification de l'organe de réglementation ou professionnel	
Compagnies d'assurance	Si nécessaire et conformément à une police d'assurance	
Fournisseurs de technologies	Si l'atteinte découle d'une défaillance technique et qu'un rappel ou une modification technique est nécessaire	

Confirmation de la notification :

Principale personne-ressource	Notifié(e)
Responsable de la protection des renseignements personnels au sein de votre organisme public, municipalité ou autorité de santé	
Police (selon les besoins)	
Personnes concernées	
Agent de révision	
Organe professionnel ou réglementaire — préciser:	
Fournisseurs de technologies	
Autres (indiquer)	

Étape 4 : Prévention

Une fois que les mesures immédiates sont prises pour réduire les risques associés à une atteinte à la vie privée, il faut prendre le temps d'enquêter sur les causes de l'incident, ce qui peut nécessiter un audit de sécurité physique et technique. Cette évaluation peut servir à mettre en place des mesures de prévention adéquates à long terme ou améliorer celles qui existent déjà.

Envisagez d'améliorer chacun des aspects suivants. Profitez-en également pour revoir votre cadre de gestion de la vie privée [4] et déterminer s'il faut apporter des modifications à votre stratégie de prévention.

Contrôles physiques
Quels étaient les contrôles physiques au moment de l'atteinte à la vie privée? Décrivez les modifications apportées aux contrôles physiques, comme les serrures, les alarmes, la surveillance de la sécurité ou le contrôle de l'accès des visiteurs.

Contrôles techniques
Y avait-il, lorsque l'atteinte à la vie privée s'est produite, une stratégie de sécurité relative à la TI? Décrivez toutes les modifications apportées aux contrôles techniques destinées à prévenir de futures atteintes.

Contrôles administratifs
Les contrôles administratifs se rapportent aux mesures de protection procédurales mises en œuvre pour le traitement des renseignements personnels en toute sécurité, ce qui comprend l'application de politiques, de directives et de processus relatifs à la protection des renseignements personnels tout au long de leur cycle de vie. Décrivez les contrôles administratifs qui existaient au moment de l'atteinte à la vie privée? Décrivez les améliorations apportées aux contrôles administratifs suite à l'atteinte. Si un protocole relatif aux atteintes à la vie privée n'est pas déjà en place, assurez-vous que votre plan d'action prévoie l'élaboration d'un tel protocole.

Mesures de contrôle de la sécurité du personnel
Les mesures de contrôle de la sécurité du personnel se rapportent à ce que fait un organisme public (ou une autorité de santé) pour gérer son personnel : compétences, formation adéquate, supervision et procédures disciplinaires. Quelles étaient les mesures de contrôle de la sécurité du personnel au moment de l'atteinte, p. ex. autorisations de sécurité, ententes de confidentialité et exigences de formation relatives au respect de la vie privée? Quelles mesures ont été prises, dans ce cas particulier, pour améliorer les mesures de contrôle de la sécurité du personnel; et de façon générale pour prévenir d'autres atteintes?

[4] Pour obtenir des renseignements sur les éléments d'un cadre de gestion de la vie privée, consultez l'onglet « Tools » du site Web du Bureau de révision: http://foipop.ns.ca.

Ce document a été préparé par le Bureau de révision de la Nouvelle-Écosse pour l'accès à l'information et la protection de la vie privée. Nous joindre :

C.P. 181, Halifax (N.-É.), B3J 2M4

Édifice Centennial, 1660, rue Hollis, bureau 1002, Halifax

Téléphone : 902-424-4684
Numéro sans frais : 1-866-243-1564
ATS/ATME : 1-800-855-0511
www.foipop.ns.ca