SANTÉ

Lignes directrices sur les interventions en cas d'atteinte à la vie privée dans le secteur de la santé

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

TABLE DES MATIÈRES

En Ontario, les dépositaires de renseignements sur la santé (les « dépositaires ») ont l'obligation, en vertu de la *Loi sur la protection des renseignements personnels sur la santé* (*LPRPS*), de protéger les renseignements personnels sur la santé contre leur collecte, leur utilisation ou leur divulgation non autorisée, que l'on appelle une « atteinte à la vie privée ». Une telle atteinte peut se produire, par exemple, en cas de vol, de perte ou encore de copie, de modification ou d'élimination non autorisée de renseignements.

En tant que dépositaire, vous devriez établir un protocole en cas d'atteinte à la vie privée afin de prévoir une marche à suivre en cas de pareil incident. Ce protocole devrait être assez souple pour s'appliquer à un large éventail d'atteintes à la vie privée, par exemple :

- les cyberattaques;
- la perte ou le vol d'appareils portables;
- les envois par télécopieur à de mauvais destinataires;
- l'accès délibéré à des dossiers médicaux électroniques sans autorisation.

L'adoption d'un protocole en cas d'atteinte à la vie privée peut vous aider à respecter vos obligations aux termes de la *LPRPS*. Ainsi, un tel protocole permet :

- d'intervenir rapidement et de façon coordonnée;
- de définir les rôles et responsabilités de chacun;
- d'établir des processus en vue d'enquêter sur l'atteinte à la vie privée, de la maîtriser et de la corriger;
- de se préparer à l'intervention possible du Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP).

QUE FAIRE EN CAS D'ATTEINTE À LA VIE PRIVÉE

Lorsque vous apprenez qu'il y a eu atteinte à la vie privée, vous devez agir immédiatement. Bon nombre des mesures suivantes devront être prises en même temps ou en succession rapide. Vous pourriez devoir revenir en arrière et répéter certaines de ces étapes.

ÉTAPE 1 : AVISER LE PERSONNEL ET LES AUTRES DÉPOSITAIRES

- Informez immédiatement les membres du personnel concernés, y compris la directrice générale ou le directeur général de la protection de la vie privée ou la personne responsable de la protection de la vie privée.
- Selon la nature ou la gravité de l'atteinte à la vie privée, informez la haute direction, les responsables des relations avec les patients et le personnel du service de technologie et des communications.
- Si l'atteinte à la vie privée fait intervenir des renseignements personnels sur la santé sauvegardés dans un système électronique qu'utilisent plusieurs dépositaires, avisez tous ces dépositaires.

ÉTAPE 2 : DÉTERMINER LA PORTÉE DE L'ATTEINTE À LA VIE PRIVÉE ET EN LIMITER LES CONSÉQUENCES

- Déterminez la portée de l'atteinte à la vie privée ainsi que les particuliers ou organismes concernés ou qui en sont responsables, ainsi que la nature et la quantité de renseignements personnels sur la santé en cause.
- Récupérez les copies des renseignements personnels sur la santé qui ont été divulguées.
- Assurez-vous que le particulier qui n'était pas autorisé à recevoir les renseignements personnels sur la santé n'en a conservé aucune copie, et obtenir ses coordonnées au cas où il serait nécessaire de communiquer à nouveau avec lui.

Déterminez si l'atteinte à la vie privée pourrait entraîner un accès non autorisé à d'autres renseignements personnels sur la santé,

p. ex., si les renseignements se trouvent dans un système partagé. Prenez les mesures qui s'imposent, p. ex., remplacez les mots de passe et les numéros d'identification, ou mettez le système hors service temporairement.

- En cas d'accès non autorisé de la part d'un mandataire, envisagez de suspendre son droit d'accès.

ÉTAPE 3 : AVISER LES PARTICULIERS CONCERNÉS PAR L'ATTEINTE À LA VIE PRIVÉE, LE CIPVP OU LES ORGANISMES DE RÉGLEMENTATION

LA NOTIFICATION DIRECTE DES PERSONNES CONCERNÉES

- La *LPRPS* oblige le dépositaire à aviser les particuliers concernés par une atteinte à la vie privée à la première occasion raisonnable. Cet avis peut être donné par téléphone ou par écrit. Selon la situation, vous pouvez verser une note au dossier du particulier pour vous rappeler de lui en parler à son prochain rendez-vous.
- Le mode de notification des particuliers concernés repose sur de nombreux facteurs (p. ex., le caractère délicat des renseignements personnels sur la santé). Dans le doute, adressez-vous au CIPVP pour établir le mode de notification le plus approprié.
- Lorsque vous avisez les particuliers touchés par l'atteinte à la vie privée, vous devriez fournir les renseignements suivants :
    - le nom du mandataire responsable de l'accès non autorisé, s'il y a lieu;
    - la date de l'atteinte à la vie privée;
    - une description de la nature et de la portée de l'atteinte à la vie privée;
    - une description des renseignements personnels sur la santé qui ont fait l'objet de l'atteinte à la vie privée;
    - les mesures prises pour maîtriser l'atteinte à la vie privée;

- le nom et les coordonnées de la personne de votre organisme qui peut répondre aux demandes de renseignements.

- L'avis aux particuliers concernés doit comprendre une déclaration indiquant qu'ils ont le droit de porter plainte au CIPVP.
- Si des renseignements financiers ou des renseignements provenant de documents délivrés par le gouvernement sont en cause, ajoutez le message suivant dans l'avis :

> Par précaution, nous vous recommandons fortement d'informer de cette atteinte à la vie privée les banques, sociétés émettrices de cartes de crédit et services gouvernementaux avec qui vous traitez.
>
> Vous devriez vérifier vos états de comptes bancaires, de cartes de crédit et d'autres opérations financières pour déceler toute activité louche.
>
> Si vous soupçonnez une utilisation abusive de renseignements personnels qui vous concernent, vous pouvez obtenir une copie de votre dossier de crédit auprès d'une agence d'évaluation du crédit pour vérifier si les opérations contenues dans votre dossier sont légitimes.
>
> - Equifax, au 1 800 465-7166 ou à **www.equifax.ca**
> - TransUnion, au 1 800 663-9980 ou à **www.transunion.ca**
>
> Si vous croyez avoir été victime de fraude, vous pouvez demander à ces agences d'annexer une « alerte à la fraude » à votre dossier, qui demande aux prêteurs de communiquer avec vous avant d'ouvrir un nouveau compte.
>
> Si votre numéro de carte Santé a été perdu ou volé, appelez la ligne INFO de ServiceOntario au 1 866

532-3161 ou au 1 800 387-5559 pour le signaler. Si vous soupçonnez un abus de votre numéro de carte Santé, vous pouvez signaler les cas de fraude au ministère de la Santé et des Soins de longue durée au 1 888 781 5556 ou, par courriel, **reportohipfraud@moh.gov.on.ca**.

Vous pouvez également consulter la publication du Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario intitulée ***Le vol d'identité : un crime de situation***.

LA NOTIFICATION INDIRECTE DES PERSONNES CONCERNÉES

La notification directe, par exemple, par téléphone, par la poste, par courriel ou en personne, constitue pour les dépositaires de renseignements sur la santé le moyen habituel d'aviser les personnes concernées en cas d'atteinte à la vie privée. Cependant, dans des circonstances exceptionnelles, le dépositaire peut envisager d'aviser indirectement ces personnes.

Les personnes concernées doivent être avisées de l'atteinte à la vie privée dès que possible, même si elles le sont indirectement.

Si votre organisation envisage la notification indirecte, vous devriez consulter le CIPVP, et être disposé à expliquer pourquoi vous croyez qu'un avis indirect est raisonnable dans les circonstances et comment vous envisagez de le donner, en précisant le contenu de votre avis proposé et son mode de diffusion.

Votre organisation peut envisager de donner un avis indirect dans une plusieurs des circonstances exceptionnelles suivantes :

- L'atteinte à la vie privée a touché un grand nombre de personnes qu'il serait difficile d'aviser directement.
- Il a été établi que le risque de préjudice pour les personnes concernées est faible.
- Vous n'avez pas pu confirmer l'identité des personnes concernées même après avoir pris des mesures raisonnables pour le faire.

- La fiabilité ou l'exactitude des coordonnées des personnes concernées est douteuse.
    - Remarque : Toutes les personnes concernées ne devraient pas être avisées indirectement, même si les coordonnées de certaines d'entre elles ne sont plus valables. Lorsque certaines coordonnées sont valables mais que d'autres ne le sont plus, une démarche de notification hybride (directe et indirecte) pourrait être appropriée.
- La notification directe entraverait abusivement et considérablement les activités de votre organisation.
    - Remarque : Tous les processus de notification en cas d'atteinte à la vie privée nécessitent du temps et des ressources. C'est uniquement lorsque le temps et les ressources requises pour fournir un avis direct entraveraient abusivement et considérablement vos activités qu'il pourrait être justifié de donner un avis indirect.
- Il serait raisonnable de s'attendre à ce que la notification directe cause un préjudice aux personnes concernées.

CONTENU D'UN AVIS INDIRECT (S'APPLIQUE ÉGALEMENT AUX AVIS DIRECTS)

S'il est établi, en consultation avec le CIPVP, qu'il est raisonnable de donner un avis indirect après avoir évalué les circonstances précises de l'atteinte à la vie privée, il faut s'assurer que cet avis :

- est rédigé en langage simple;
- contient assez de renseignements pour permettre au lecteur de déterminer facilement l'incidence possible de l'atteinte à la vie privée sur lui;
- décrit les circonstances de l'atteinte à la vie privée;
- décrit la cause de l'atteinte à la vie privée, si elle est connue;
- indique la date ou la période où est survenue l'atteinte à la vie privée;

- indique la date où l'institution a été informée de l'atteinte à la vie privée;
- décrit le plus précisément possible les renseignements personnels ou les renseignements personnels sur la santé qui sont en cause;
- décrit l'impact sur les renseignements personnels ou les renseignements personnels sur la santé en cause (p. ex., accès, chiffrement, exfiltration, publication en ligne, etc.);
- décrit le risque de préjudice pour les personnes concernées, s'il est connu;
- décrit les mesures que votre institution a prises pour maîtriser l'atteinte à la vie privée et réduire le risque de préjudice pour les personnes concernées;
- mentionne d'autres mesures que les personnes peuvent prendre pour atténuer encore plus le risque de préjudice;
- mentionne aux personnes concernées qu'elles peuvent porter plainte au Commissaire à l'information et à la protection de la vie privée (en vertu de la LPRPS et de la LSEJF et, à compter du 1er juillet 2025, de la LAIPVP) et fournit un lien vers le site Web du CIPVP;
- donne les coordonnées d'une personne de l'institution pouvant répondre à des questions et fournir des renseignements supplémentaires sur l'atteinte à la vie privée;
- indique si vous avez signalé l'atteinte à la vie privée au CIPVP et à d'autres organismes de réglementation concernés, le cas échéant.

DIFFUSION D'UN AVIS INDIRECT

L'avis indirect doit être diffusé de façon à ce qu'il soit raisonnable de s'attendre à ce que les personnes concernées puissent en prendre connaissance.

Il importe de bien réfléchir à la stratégie qui serait la plus efficace pour rejoindre les personnes concernées. Il est généralement préférable et plus efficace de recourir à plusieurs méthodes.

Ainsi, une stratégie de notification du public pourrait comprendre une partie ou la totalité des méthodes suivantes afin de porter l'avis à l'attention des personnes concernées :

- Un avis publié de façon bien visible dans le site Web de votre organisation ou un site Web spécialisé contenant des renseignements sur l'atteinte à la vie privée.
    - Si vous publiez l'avis dans le site Web de votre organisation, veillez à ce que cet avis ou un lien l'y menant figure à un endroit bien visible de la page d'accueil, et qu'il ne soit pas nécessaire de défiler ou d'effectuer une recherche pour le localiser.
    - Si vous publiez l'avis dans un site Web spécialisé, vous devriez afficher un lien vers ce site sur la page d'accueil du site Web de votre organisation, afin qu'il soit clairement visible et que les visiteurs puissent cliquer dessus pour se rendre au site Web sur l'atteinte à la vie privée.
    - L'avis numérique doit demeurer en ligne pendant une période raisonnable, afin de permettre aux personnes concernées de le lire.
- Prenez des mesures raisonnables pour porter l'avis numérique à l'attention des personnes concernées. Celles-ci seront peu susceptibles de visiter votre site Web ou de lire l'avis d'atteinte à la vie privée à moins d'être invitées à le faire par des annonces dans les médias, des publications dans les médias sociaux ou d'autres moyens.
- Organisez d'autres activités d'information du public afin de porter l'avis à l'attention des personnes concernées :
- Installez des avis ou des affiches dans les secteurs fréquentés de votre établissement pendant une certaine période, afin que les personnes concernées puissent les lire.
- Publiez des avis dans des journaux nationaux ou locaux.
- Faites paraître des publications dans les médias sociaux pertinents.

- Faites diffuser des annonces et messages publicitaires à la radio ou à la télévision à l'intention des personnes concernées.
- Publiez des communiqués de presse et des avis communautaires destinés aux personnes concernées.
- Tenez des séances d'information ou des webinaires afin de renseigner la population.
- Recourez à d'autres stratégies de communication publique qui pourraient être efficaces afin de joindre les personnes concernées par l'atteinte à la vie privée.

CIPVP

Aux termes de la *LPRPS*, le dépositaire doit signaler certaines atteintes à la vie privée au CIPVP et collaborer avec ce dernier, comme il est décrit dans le document ***Le signalement d'une atteinte à la vie privée au commissaire : lignes directrices pour le secteur de la santé***.

ORDRES PROFESSIONNELS

- Vous devez donner un avis à l'ordre professionnel d'un praticien de la santé dans les 30 jours dans l'une ou l'autre des circonstances suivantes :
    - Le praticien était un employé ou un mandataire du dépositaire et il a été congédié ou suspendu ou il a fait l'objet d'une mesure disciplinaire en raison d'une atteinte à la vie privée.
    - Les privilèges ou l'affiliation du praticien sont révoqués, suspendus ou assortis de restrictions en raison d'une atteinte à la vie privée.
    - Le praticien a démissionné et le dépositaire a des motifs de croire que la démission est liée à une enquête ou à une autre mesure qu'il a prise relativement à une prétendue atteinte à la vie privée.
    - Le praticien renonce à ses privilèges ou à son affiliation, ou les restreint volontairement, et le dépositaire a des motifs de croire que la renonciation ou la restriction est

liée à une enquête ou à une autre mesure qu'il a prise relativement à une prétendue atteinte à la vie privée.

ÉTAPE 4 : MENER UNE ENQUÊTE ET PRENDRE DES MESURES CORRECTIVES

- Menez une enquête interne pour :
  - vous assurer que les mesures immédiates de maîtrise de la situation et de notification ont été prises;
  - passer en revue les circonstances qui ont entouré l'atteinte à la vie privée;
  - déterminer si les politiques et procédures en vigueur sont suffisantes pour protéger les renseignements personnels sur la santé.
- Envisagez la situation de façon systémique; dans certains cas, il pourrait être justifié de réexaminer les procédures à l'échelle du programme. Par exemple, les contrôles administratifs ou les caractéristiques de sécurité d'un système électronique pourraient être insuffisants et devoir être mis à niveau ou améliorés.
- Si vous avez avisé le CIPVP d'une atteinte à la vie privée, vous serez appelé à décrire votre enquête et à collaborer avec lui pour établir les mesures correctives qui s'imposent et vous engager à les prendre.
- Dressez une liste de toutes les atteintes à la vie privée, et désignez un employé qui sera chargé de la tenir à jour. Pour chaque atteinte à la vie privée, prenez note des renseignements suivants :
  - le nom de l'employé ou du mandataire qui a causé l'atteinte à la vie privée lorsque cela est pertinent, notamment en cas d'accès non autorisé;
  - la date de l'atteinte à la vie privée;
  - la nature, la portée et la cause de l'atteinte à la vie privée;
  - le nombre de particuliers touchés par l'atteinte à la vie privée;

- une description des renseignements personnels sur la santé qui ont fait l'objet de l'atteinte à la vie privée;
- un résumé des mesures prises en réponse à l'atteinte à la vie privée.

- Vous pourriez également être tenu de collaborer à toute enquête du CIPVP sur l'atteinte à la vie privée.

Aux termes de la *LPRPS*, vous devez recueillir des statistiques sur les atteintes à la vie privée et les communiquer au CIPVP. Le document ***Rapport statistique annuel au commissaire sur les atteintes à la vie privée*** décrit les statistiques qu'il faut recueillir et fournir au CIPVP.

COMMENT MINIMISER LE RISQUE D'ATTEINTE À LA VIE PRIVÉE

- Renseignez le personnel sur les dispositions de la *LPRPS* qui régissent la collecte, l'utilisation, la divulgation, la conservation, le transfert et l'élimination de renseignements personnels sur la santé.
- Veillez à instaurer des politiques et des procédures conformes aux dispositions de la *LPRPS* sur la protection de la vie privée et à donner au personnel une formation suffisante à leur sujet.
- Protégez les renseignements personnels sur la santé qui doivent être utilisés hors du bureau ou de l'établissement. Assurez-vous que tous les ordinateurs portables et appareils personnels sont protégés par mot de passe et que les données sont chiffrées.
- Veillez à ne pas recueillir, utiliser ou divulguer plus de renseignements personnels sur la santé qu'il n'est raisonnablement nécessaire, afin d'atténuer les conséquences de toute atteinte à la vie privée.
- Assurez-vous de ne pas recueillir, utiliser ou divulguer de renseignements personnels sur la santé si d'autres renseignements peuvent servir aux mêmes fins.

- Intégrez dans tous les systèmes électroniques contenant des dossiers de santé une fonction de consignation et de vérification, et informez le personnel que les systèmes seront vérifiés régulièrement.

Menez, s'il y a lieu, une évaluation de l'incidence sur la vie privée, qui permet de déterminer si les nouvelles technologies, les nouveaux systèmes d'information et les programmes ou politiques proposés répondent à des exigences de base en matière de protection de la vie privée. Pour des précisions à ce sujet, consulter la publication du CIPVP intitulée ***Lignes directrices concernant l'évaluation de l'incidence sur la vie privée sous le régime de la Loi sur la protection des renseignements personnels sur la santé de l'Ontario***.

En cas de doute, demandez conseil au service juridique et à la directrice générale ou au directeur général de la protection de la vie privée de votre organisme.

Les dépositaires peuvent aussi consulter le CIPVP pour obtenir ses commentaires sur leurs pratiques actuelles ou proposées relatives aux renseignements.

AUTRES PUBLICATIONS PERTINENTES

Pour en savoir davantage sur l'obligation légale du dépositaire de produire des statistiques sur les atteintes à la vie privée, consultez le document ***Rapport statistique annuel au commissaire sur les atteintes à la vie privée***.

Le signalement d'une atteinte à la vie privée au commissaire : lignes directrices pour le secteur de la santé décrit les circonstances dans lesquelles il est obligatoire de signaler une atteinte à la vie privée au CIPVP.

Pour savoir comment déceler et prévenir les accès non autorisés à des renseignements personnels sur la santé, consultez ***Detecting and Deterring Unauthorized Access to Personal Health Information et Se protéger contre les rançongiciels***. Pour toute question sur les interventions en cas d'atteinte à la vie privée ou sur les obligations des dépositaires, veuillez communiquer avec nous à **info@ipc.on.ca** ou au 1 800 387-0073.

RESSOURCES SUPPLÉMENTAIRES

Le CIPVP a rédigé des documents d'orientation pour aider votre organisme à respecter ses obligations en matière de protection de la vie privée et à éviter les atteintes à la vie privée. Ils se trouvent dans la section des documents d'orientation du site Web du CIPVP (**www.ipc.on.ca**).

Au sujet du CIPVP

Le Commissaire à l'information et à la protection de la vie privée de l'Ontario est nommé par l'Assemblée législative de l'Ontario et est indépendant du gouvernement au pouvoir. Son mandat consiste à régler les appels de décisions en matière d'accès à l'information et les plaintes concernant la protection de la vie privée, à renseigner le public sur les questions touchant l'accès à l'information et la protection de la vie privée, à examiner les pratiques relatives aux renseignements et à formuler des commentaires sur les textes de loi, pratiques et programmes proposés.

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

2, rue Bloor Est, bureau 1400
Toronto (Ontario) Canada M4W 1A8
Téléphone : 416 326-3333 / 1 800 387-0073
ATS : 416 325-7539

www.ipc.on.ca
info@ipc.on.ca

Mis à jour mars 2025