# Nouvelles exigences de signalement concernant l'atteinte à la vie privée

Le 1er octobre 2017, aux termes de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS), le gouvernement de l'Ontario a mis en place des exigences de signalement concernant l'atteinte à la vie privée. Ces modifications font en sorte que les Dt.P. agissant à titre de dépositaires de renseignements sur la santé (DRS) doivent déposer des rapports dans sept catégories d'atteintes à la vie privée au commissaire à l'information et à la protection de la vie privée de l'Ontario (le commissaire). Ces nouvelles exigences de signalement sont distinctes de l'obligation des DRS d'aviser les particuliers du vol ou de la perte des renseignements personnels sur la santé ou de leur utilisation ou divulgation sans autorisation, prévue au paragraphe 12 (2) de la LPRPS.

Le commissaire a conçu une ressource utile intitulée « Le signalement d'une atteinte à la vie privée au commissaire : Lignes directrices pour le secteur de la santé ». Les Dt.P. qui agissent à titre de DRS devraient s'y reporter pour se renseigner davantage sur leurs obligations de signalement concernant toute atteinte à la vie privée. Une telle atteinte peut s'appliquer dans plus d'une catégorie. Si au moins une des situations indiquées ci-dessous s'applique, les Dt.P. agissant à titre de DRS doivent la signaler au commissaire.

## LES SEPT CATÉGORIES D'ATTEINTE À LA VIE PRIVÉE SONT LES SUIVANTES.

### 1. Utilisation ou divulgation sans autorisation

Il faut signaler tout « fouinage » par le personnel d'une organisation, un fournisseur de soins de santé ou un tiers (p. ex. un fournisseur de services externe à contrat).

Si l'atteinte à la vie privée est de nature accidentelle, par exemple si l'information a été envoyée par inadvertance (soit par courriel ou par messagerie) au mauvais destinataire ou si une personne autorisée accède par mégarde au dossier du mauvais patient, il n'est généralement pas nécessaire de faire un signalement. Cette exception concernant l'utilisation ou la divulgation accidentelle ne s'applique pas aux autres types d'atteinte indiqués dans les six catégories ci-dessous.

### 2. Renseignements volés

Signalez les vols de documents papier, d'ordinateurs portatifs et d'autres appareils électroniques comprenant des renseignements personnels sur la santé. Faites de même pour ce qui est des attaques par rançongiciel ou autre programme malveillant ayant permis de voler des renseignements personnels sur la santé.

Il n'est pas nécessaire d'aviser le commissaire si les renseignements volés avaient été anonymisés ou correctement chiffrés. On encourage les DRS à adopter de telles mesures afin de prévenir des atteintes à la vie privée. Pour plus de renseignements, veuillez vous reporter au document intitulé « Le chiffrement fort dans les soins de santé » (Ann Cavoukian, Ph. D., commissaire à l'information et à la protection de la vie privée de l'Ontario, 2010).

### 3. Autre utilisation ou divulgation sans autorisation après une atteinte à la vie privée

L'atteinte à la vie privée doit être signalée si elle est aggravée par d'autres atteintes. Prenons l'exemple d'un accès non autorisé à des renseignements personnels pouvant mener à une exploitation à des fins commerciales ou criminelles de ces informations, ou l'ayant déjà fait, ou la menace de publier ces renseignements.

### 4. Contexte d'atteintes à la vie privée similaires

Les DRS doivent faire preuve de jugement pour décider si une atteinte à la vie privée constitue un cas isolé ou une constante.

Une série d'atteintes accidentelles ou peu importantes peut indiquer des problèmes systémiques, par exemple le mauvais fonctionnement d'une pièce d'équipement ou de systèmes, des lacunes concernant les dispositifs de protection ou la formation. Le fait de conserver les atteintes à la vie privée dans un format normalisé aidera les DRS à identifier des constantes.

**5. Mesure disciplinaire contre un membre d'un ordre**

ISi un membre d'un ordre est congédié, suspendu ou se voit infliger des mesures disciplinaires ou s'il démissionne par suite d'une atteinte à la vie privée, ou ses privilèges sont révoqués, suspendus ou assortis de restrictions, ou s'il y renonce ou s'ils sont volontairement assortis de restrictions en raison d'une atteinte à la vie privée, l'incident doit être signalé au commissaire.

**6. Mesure disciplinaire contre une personne qui n'est pas membre d'un ordre de réglementation des professions de la santé**

Cette situation est similaire à la catégorie 5 ci-dessus, mais elle s'applique aux employés ou aux agents d'un DRS qui ne sont pas membres d'un ordre de réglementation des professions de la santé. Les lignes directrices du commissaire prévoient le scénario suivant : « L'un de vos commis à l'inscription fait une rencontre désagréable avec un patient et affiche l'information au sujet de ce dernier dans les médias sociaux. Vous suspendez le commis durant un mois. » Bien que le commis ne soit pas membre d'un ordre de réglementation des professions de la santé, les DRS doivent signaler cette atteinte à la vie privée au commissaire.

**7. Atteinte importante à la vie privée**

Toutes les atteintes importantes à la vie privée doivent être signalées au commissaire, qu'elles fassent partie ou non des six catégories ci-dessus. Pour établir si une atteinte à la vie privée est « importante », il faut examiner attentivement la situation, en consultation avec l'avocat du DRS, pour que les atteintes à la vie privée soient signalées dans les cas appropriés. En menant cette évaluation, les DRS peuvent poser les questions suivantes.

- L'information est-elle de nature délicate?
- L'atteinte à la vie privée concerne-t-elle un volume considérable de renseignements?
- Bien des personnes sont-elles touchées par cette atteinte à la vie privée?
- Y avait-il plus d'un DRS ou d'un agent responsable de l'atteinte à la vie privée?

Même si une atteinte à la vie privée ne cause pas de préjudice particulier, elle peut être jugée considérable et nécessiter un rapport au commissaire. Par exemple, la divulgation accidentelle de l'évaluation de la santé mentale d'un patient à d'autres fournisseurs de soins de santé qui sont sur une liste d'envoi par courriel et non seulement au médecin de ce patient est une situation qui, selon le commissaire, constitue une atteinte importante à la vie privée. On trouvera d'autres exemples dans les lignes directrices du commissaire.

## RAPPORT ANNUEL

Dès le 1er janvier 2018, les DRS devront commencer à compiler des statistiques sur l'atteinte à la vie privée et, à compter de janvier 2019, ils devront fournir un rapport annuel au commissaire sur les statistiques de l'année civile précédente sur les atteintes à la vie privée. Le rapport devra également indiquer le nombre de fois où des renseignements personnels ont été volés, perdus, utilisés sans autorisation ou divulgués sans autorisation (le rapport devant préciser le nombre exact de cas pour chaque type d'atteinte à la vie privée). Plus tard en 2017, le commissaire publiera des indications supplémentaires sur les rapports statistiques.

## POLITIQUES ET PROCÉDURES

Ces nouvelles exigences en matière d'information à fournir au sujet des atteintes à la vie privée présenteront de nouveaux défis pour les fournisseurs de soins de santé. Il est souhaitable que les Dt.P. qui agissent à titre de DRS conçoivent des politiques et procédures internes pour détecter et gérer adéquatement de telles atteintes et donner suite convenablement à ces atteintes et aux obligations en matière de présentation de rapports.

*L'Ordre remercie Fasken Martineau DuMoulin LLP pour son bulletin électronique (Commissioner Issues Important Privacy Breach Reporting Guideline for Health Sector) qui a servi à la rédaction du présent article.*