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

Feuille-info

La communication de renseignements personnels sur la santé par courriel

Septembre 2016

De nos jours, le courriel est l'un des principaux moyens de communication. Particuliers et organismes l'apprécient parce qu'il est pratique, rapide et économique, qu'il soit utilisé à des fins personnelles ou professionnelles. Les dépositaires de renseignements sur la santé (les « dépositaires ») ne font pas exception. Malgré les nombreux avantages que présente le courriel, il comporte également des risques pour la protection de la vie privée des particuliers et la sécurité des renseignements personnels sur la santé. Il est important que les dépositaires comprennent ces risques et prennent des mesures pour les atténuer avant d'utiliser le courriel pour leurs communications professionnelles.

OBLIGATIONS PRÉVUES DANS LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ*

La *Loi sur la protection des renseignements personnels sur la santé* établit les règles qui régissent la protection de la vie privée des particuliers et la confidentialité des renseignements personnels sur la santé qui les concernent et facilitent la prestation de services de santé efficaces et appropriés. Les dépositaires ont l'obligation de s'assurer que les dossiers de santé dont ils ont la garde ou le contrôle sont conservés, transférés et éliminés de manière sécuritaire. Ils doivent également prendre des mesures raisonnables pour protéger les renseignements personnels sur la santé contre le vol, la perte et une utilisation ou une divulgation non autorisée.

COMPRENDRE LES RISQUES

Comme toutes les formes de communication, le courriel comporte un élément de risque. Une personne peut envoyer un courriel au mauvais destinataire, par exemple, en tapant mal l'adresse de courriel ou en utilisant la fonction de saisie semi-automatique. Les courriels sont souvent consultés sur des appareils portatifs comme des téléphones intelligents, des tablettes et des ordinateurs portables, qui peuvent être volés ou perdus. Un courriel peut également être transféré ou modifié à l'insu de l'expéditeur initial ou sans son autorisation. Les courriels peuvent aussi être interceptés ou faire l'objet de piratage électronique par des tiers non autorisés.

Les renseignements personnels sur la santé sont confidentiels de nature. Leur collecte, utilisation ou divulgation non autorisée peut avoir de graves conséquences pour les particuliers, notamment la stigmatisation, la discrimination et les préjudices psychologiques. Pour les dépositaires et leurs mandataires, les atteintes à la vie privée peuvent entraîner des mesures disciplinaires et des poursuites, sans compter la perte de confiance envers l'ensemble du secteur de la santé, chargé de protéger ces renseignements délicats.

S'ATTAQUER AUX RISQUES

Mesures de protection techniques, matérielles et administratives

Les dépositaires doivent implanter des mesures techniques, matérielles et administratives pour protéger les renseignements personnels sur la santé. Cette exigence s'applique à toutes les communications par courriel qui comprennent ce genre de renseignements.

Mesures de protection techniques :

- Chiffrement pour les appareils portatifs
- Mots de passe forts
- Pare-feux et antiprogrammes malveillants

Mesures de protection matérielles :

- Limiter l'accès au bureau, utiliser des systèmes d'alarme et verrouiller les portes des salles où se trouve du matériel pour l'envoi ou la réception par courriel de renseignements sur la santé
- Garder les appareils portatifs en lieu sűr, comme un tiroir ou un classeur verrouillé, lorsqu'ils ne sont pas utilisés; ne jamais les laisser sans surveillance

Exemples de mesures de protection administratives :

- Inclure un avis dans les courriels indiquant que les renseignements contenus dans le courriel sont confidentiels
- Expliquer la marche à suivre si un courriel est reçu par erreur
- Communiquer par courriel en utilisant un compte d'affaires plutôt qu'un compte personnel (les comptes personnels peuvent avoir des niveaux de sécurité plus faibles et risquent plus d'être compromis)
- Vérifier si une adresse de courriel est toujours valable
- S'assurer que l'adresse de courriel du destinataire correspond à l'adresse proposée pour l'envoi du courriel
- Vérifier régulièrement les adresses de courriel préprogrammées pour s'assurer qu'elles sont toujours valables
- Limiter l'accès au système de courriel et aux courriels aux personnes qui ont absolument besoin d'en connaître le contenu
- Informer les particuliers de tout changement d'adresse de courriel

- Accuser réception des courriels
- Recommander que les particuliers mettent en śuvre ces mesures et qu'ils envoient leur courriel à une adresse de courriel protégée par mot de passe à laquelle eux seuls ont accès

Les dépositaires devraient également veiller à ce que soient respectées les mesures de protection prévues dans d'autres politiques et procédures, comme celles portant sur l'utilisation de son propre appareil au travail.

Pour de plus amples renseignements, sur la protection des renseignements personnels sur la santé, veuillez consulter notre feuille-info ***La protection des renseignements personnels sur la santé***.

Chiffrement des courriels

Le chiffrement est un moyen important et efficace de réduire les risques associés à l'envoi par courriel de renseignements personnels sur la santé. Le chiffrement consiste à brouiller le contenu d'un courriel de manière que seules les personnes ayant accès à une clé ou à un mot de passe secret puissent le déchiffrer et le lire. Le chiffrement réduit les risques de collecte, d'utilisation ou de divulgation non autorisée des renseignements. L'utilisation du chiffrement dans le contexte de la communication par courriel entre dépositaires et entre ceux-ci et leurs patients est analysée ci-après.

Pour de plus amples renseignements sur le chiffrement, veuillez consulter nos feuilles-info ***Le chiffrement des renseignements personnels sur la santé dans les appareils mobiles*** et ***Le chiffrement fort dans les soins de santé***.

Communication par courriel entre dépositaires

Le CIPVP s'attend à ce que les communications par courriel entre dépositaires soient protégées contre les accès non autorisés grâce au chiffrement, sauf dans des circonstances exceptionnelles. Le chiffrement de bout en bout représente la solution la plus sűre pour les courriels, l'expéditeur ayant l'assurance que seul le destinataire prévu lira le courriel. Le destinataire peut également être rassuré que le message est authentique et qu'il a bel et bien été envoyé par l'expéditeur. Par exemple, le service ONE Mail de cyberSanté Ontario permet aux professionnels de la santé inscrits d'envoyer et de recevoir des renseignements personnels sur la santé chiffrés.

Cependant, dans certaines circonstances exceptionnelles, la transmission de renseignements personnels sur la santé entre dépositaires par courriel chiffré n'est pas pratique. Par exemple, dans une situation d'urgence, les dépositaires peuvent déterminer que l'envoi d'un courriel non chiffré est le moyen le plus rapide et le plus pratique de transmettre l'information. Les dépositaires devraient également consulter les lignes directrices, normes ou règlements de leur ordre professionnel sur l'utilisation des courriels non chiffrés pour la transmission de renseignements personnels sur la santé.

Communication par courriel entre les dépositaires et leurs patients

Lorsque c'est possible, les dépositaires devraient chiffrer les courriels qu'ils envoient aux patients. Le chiffrement est de plus en plus répandu et facile à utiliser. Les portails de patients et les systèmes de dossiers médicaux électroniques comprennent de plus en plus des applications d'envoi chiffré.

S'il est impossible de chiffrer un envoi, les dépositaires devraient déterminer s'il est souhaitable de communiquer avec leurs patients sans chiffrer leur message. Pour ce faire, ils doivent tenir compte des facteurs suivants :

Caractéristiques des renseignements

Quel genre de renseignements le dépositaire enverra-t-il à son patient? Bien que tous les renseignements personnels sur la santé soient confidentiels, le degré de confidentialité peut varier. Par exemple, l'heure et la date d'un rendez-vous ne sont peut-être pas aussi confidentiels que les renseignements diagnostiques contenus dans le dossier de santé d'une personne.

Volume de renseignements et fréquence des courriels

À mesure que le volume et la fréquence des courriels augmentent, les risques augmentent également. Le courriel contiendra-t-il beaucoup de renseignements personnels sur la santé? Le dépositaire envoie-t-il les renseignements une seule fois ou le fait-il souvent ou régulièrement?

Objet de la transmission

Le dépositaire envisage-t-il d'utiliser le courriel à des fins administratives, comme pour envoyer des rappels de rendez-vous, pour l'éducation et la promotion de la santé, par exemple pour envoyer des ressources générales sur la santé, ou pour des soins individualisés, par exemple, pour répondre à des questions de suivi?

Attentes des patients

Comment les patients souhaitent-ils que les dépositaires communiquent avec eux?

Autres modes de communication et risques connexes

Quels autres modes de communication sont disponibles? Les dépositaires devraient évaluer les risques que pose chacun pour la vie privée et la confidentialité, et choisir celui dont le niveau de risque est proportionnel aux préjudices qui pourraient résulter d'une atteinte à la vie privée.

Situations d'urgence

Le dépositaire se trouve-t-il dans une situation d'urgence? Un courriel non chiffré représente-t-il le moyen le plus rapide et le plus pratique de transmettre les renseignements nécessaires à la prestation des soins à la personne ou pour prévenir les préjudices?

Après avoir examiné chacun de ces facteurs, le dépositaire doit être convaincu que l'envoi d'un courriel non chiffré est raisonnable. Dans le cas contraire, il ne devrait pas utiliser ce mode de communication pour communiquer avec ses patients.

Politique concernant les courriels

Les dépositaires devraient élaborer et mettre en śuvre une politique sur l'envoi et la réception par courriel de renseignements personnels sur la santé. La politique devrait prévoir à quel moment, comment et à quelles fins ces renseignements peuvent être envoyés et reçus par courriel, ainsi que les conditions ou les restrictions applicables. Elle devrait également énoncer le genre de renseignements qui peuvent être envoyés et reçus par courriel non chiffré ainsi que les circonstances dans lesquelles le dépositaire enverra un courriel non chiffré.

Avis et consentement

Les dépositaires doivent informer leurs patients de la politique sur le courriel et obtenir leur consentement avant d'envoyer un courriel non chiffré. Le consentement devrait être écrit en langage simple et préciser le genre de renseignements qui peut ou non être transmis dans un courriel non chiffré, les risques associés aux courriels non chiffrés et les circonstances dans lesquelles le dépositaire enverra un courriel non chiffré. Par exemple, les dépositaires peuvent limiter l'utilisation de courriels non chiffrés uniquement pour fixer des rendez-vous et interdire l'envoi ou la réception de renseignements cliniques non chiffrés. Les dépositaires voudront peut-être fournir d'autres options pour le consentement, permettant aux particuliers de choisir les circonstances dans lesquelles ils acceptent l'envoi de courriels non chiffrés.

L'avis et le consentement relatifs aux communications par courriel non chiffré peuvent prendre différentes formes. Par exemple, si les patients fournissent leur adresse de courriel par écrit, notamment en remplissant un formulaire, celui-ci peut comprendre des renseignements sur les risques que comportent les communications par courriel non chiffré et leur demander s'ils consentent à ce genre de communications. Cela peut aussi prendre la forme d'une discussion de vive voix, lorsque le particulier donne son adresse de courriel oralement au dépositaire.

Minimisation des données

Même si le patient accepte de communiquer par courriel, cela ne veut pas dire que tous les renseignements personnels sur la santé devraient être envoyés de cette façon. Le dépositaire a l'obligation de limiter la quantité et le genre de renseignements personnels compris dans un courriel. Les dépositaires devraient également déterminer comment ils répondront aux demandes de particuliers pour limiter l'utilisation du courriel.

Conservation et élimination des renseignements personnels sur la santé

Les dépositaires sont tenus de conserver et d'éliminer les renseignements personnels sur la santé dont ils ont la garde ou le contrôle de façon sécuritaire. Cette exigence s'applique aux renseignements contenus dans les communications par courriel.

Les dépositaires devraient stocker les renseignements personnels sur la santé dans les serveurs de courriel seulement jusqu'à ce que l'objectif visé soit atteint. Par exemple, si un courriel a déjà été versé au dossier du patient, il sera peut-être inutile de conserver les renseignements dans les serveurs de courriel. De même, les dépositaires devraient également s'assurer que tous les doubles des courriels contenant des renseignements personnels sur la santé stockés dans des appareils portatifs sont supprimés lorsqu'ils ne sont plus nécessaires et qu'ils ont déjà été versés dans le dossier du patient.

Le chiffrement des appareils portatifs empêche l'accès non autorisé à des renseignements qui y sont stockés en cas de perte ou de vol. Les renseignements personnels sur la santé peuvent également être protégés par le chiffrement des copies de sécurité, y compris celles qui sont situées hors site.

Pour de plus amples renseignements, veuillez consulter nos feuilles-info ***La protection des renseignements personnels sur la santé*** et ***La destruction sécurisée de renseignements personnels***.

Formation

Une formation complète sur la protection de la vie privée et la sécurité est un moyen essentiel de réduire les risques de collecte, d'utilisation et de divulgation non autorisées de renseignements personnels sur la santé. Les dépositaires doivent s'assurer que leurs employés et mandataires reçoivent une formation initiale sur la protection de la vie privée et la sécurité, et qu'ils sont tenus de suivre une formation continue sur ces sujets, y compris une formation sur la politique et la procédure d'envoi et de réception de renseignements personnels sur la santé par courriel.

Gestion des atteintes à la vie privée

Les dépositaires devraient avoir un protocole de gestion des atteintes à la vie privée. Ce protocole devrait porter sur l'identification, la déclaration et le contrôle des atteintes à la vie privée réelles ou soupçonnées, l'enquête connexe et l'atténuation des conséquences.

Le CIPVP ne considère pas que la perte ou le vol d'un appareil électronique contenant des renseignements personnels sur la santé chiffrés constitue une atteinte à la vie privée. Cependant, que les renseignements soient chiffrés ou non, les dépositaires devraient exiger que leurs mandataires déclarent une telle perte ou un tel vol. Cela permettra aux dépositaires de déterminer, au cas par cas, si les renseignements sont bien protégés.

Pour de plus amples renseignements sur les atteintes à la vie privée, veuillez consulter ***Que faire en cas d'atteinte à la vie privée : Lignes directrices pour le secteur de la santé***.