CONSEILS SUR LA PRATIQUE

COMMENT EXERCER DE FAÇON SÉCURITAIRE DANS UN MONDE QUI N'EST PAS TOUJOURS SÉCURITAIRE

DATE: 2012

Par Alexandra Rowland-Carling, Ph.D. Directrice de Pratique professionnelle et d'assurance de la qualité

Il ne fait aucun doute que les changements technologiques et Internet ont fourni aux professionnels de la santé des moyens plus efficaces de communiquer, de rédiger des rapports, de consigner des notes, de transférer des dossiers et de conserver des documents. Nous avons accès à notre calendrier sur nos téléphones intelligents et nous pouvons rédiger un rapport sur notre portable et l'envoyer au bureau par courriel. Les patients, clients et familles nous demandent de communiquer avec eux par courriel et nous lisons ces courriels sur nos téléphones, nos tablettes électroniques et nos portables.

Dans notre pratique, toutefois, il ne faut jamais perdre de vue les facteurs entourant la confidentialité du patient/client, le droit à la vie privée et notre obligation d'exercer dans le respect des principes juridiques de la *Loi sur la protection des renseignements personnels sur la santé* (LPRPS). Hélas, ici à l'OAOO, nous recevons parfois des appels de membres affolés qui viennent de se faire voler leur téléphone, leur porte-documents, leur portable ou leur sac à main. De plus, à mesure que les clés USB se font plus petites, elles sont plus faciles à perdre. Voici quelques conseils de l'Ordre et du Bureau du commissaire à l'information et à la vie privée de l'Ontario pour vous aider à exercer votre profession de façon sécuritaire dans un monde qui n'est pas toujours sécuritaire.

TÉLÉPHONES

TÉLÉPHONES DE RÉSIDENCE**:** Si vous avez un bureau à la maison et que vous travaillez en pratique privée à partir de la maison, assurez-vous d'avoir une ligne téléphonique séparée, une boîte vocale séparée ou une boîte TéléRéponse (Call Answer) séparée pour permettre à vos clients de vous laisser un message.

« Vous avez joint la résidence des Rowland ainsi que le cabinet privé de services d'orthophonie Rowland. Pour laisser un message aux Rowland, appuyez sur le un. Pour le cabinet privé de services d'orthophonie Rowland, appuyez sur le deux. »

Cela permet de protéger la confidentialité de vos clients privés lorsqu'ils laissent un message et d'éliminer le risque que quelqu'un d'autre dans votre maison entende les détails.

TÉLÉPHONES INTELLIGENTS**:** Si vous avez un téléphone intelligent qui vous donne accès à une boîte vocale et à vos courriels du bureau, assurez-vous d'utiliser tous les paramètres de sécurité. Tous les téléphones doivent être protégés au minimum par un mot de passe de

quatre chiffres. Plusieurs téléphones permettent maintenant d'utiliser un mot de passe comptant jusqu'à sept chiffres. On n'est jamais assez prudent!

Pour ajouter un mot de passe à votre compte de courrier électronique, essayez ce qui suit :

Allez à PARAMÈTRES (SETTINGS).

- Allez à GÉNÉRAL (GENERAL).
- Allez à RESTRICTIONS.
- Sélectionnez ACTIVER RESTRICTIONS (ENABLE RESTRICTIONS).
- Entrez votre mot de passe de quatre chiffres.
- Sélectionnez le compte de courrier électronique que vous voulez verrouiller.
- Désélectionnez tout le reste.

Si votre téléphone intelligent ne vous permet pas d'ajouter un mot de passe en suivant cette procédure, essayez de télécharger une application de votre magasin d'applications. L'application qu'il vous faut est une application de verrouillage.

TECHNOLOGIE BLUETOOTH: Il existe plusieurs systèmes qui vous permettent d'utiliser votre téléphone en mode « mains libres » pendant que vous conduisez votre auto. Assurez-vous de ne pas accepter d'appel lié au travail s'il y a quelqu'un d'autre dans la voiture qui pourra entendre la conversation. Dites à la personne que vous allez la rappeler. Vous pouvez toujours vous arrêter et passer au mode téléphone pour votre conversation.

CLÉS USB : Les clés USB sont de petits dispositifs portables de stockage de données que l'on appelle aussi clés à mémoire flash. L'Ordre recommande que vous utilisiez des clés USB **cryptées** ou **encodées**. Le cryptage est un processus qui transforme de l'information ou des données en symboles indéchiffrables les rendant donc inintelligibles. Pour déchiffrer l'information et la ramener à sa forme initiale de texte, vous devez entrer votre mot de passe.

Il est important pour vous ou votre employeur d'élaborer une politique écrite qui explique que vous utilisez des clés USB cryptées. De cette façon, si la clé est volée ou perdue, vous aurez la preuve que vous avez utilisé une méthode de transfert de données sécuritaire lorsque vous présenterez votre rapport au responsable de la protection des renseignements personnels de votre organisme ou au Bureau du commissaire à l'information et à la vie privée.

PORTABLES:

Tous les portables utilisés pour le travail doivent être protégés par mot de passe. Ne divulguez votre mot de passe à personne et changez-le après quelques mois. Si vous avez un portable à la maison et qu'il est utilisé par d'autres personnes, assurez-vous que ces personnes n'ont PAS accès à vos fichiers du bureau ou à votre compte de courrier électronique du bureau.

Il est également possible de crypter les portables et les ordinateurs personnels pour protéger encore davantage les renseignements personnels sur la santé. Si vous utilisez le cryptage et les mots de passe et que le pire scénario se produit et que l'ordinateur est volé ou perdu, les renseignements de votre patient et client seront protégés et vous le serez

aussi. Encore une fois, nous recommandons que l'utilisation du cryptage soit documentée à votre lieu de travail comme preuve de diligence raisonnable dans le rapport d'atteinte à la vie privée.

COURRIELS:

Les systèmes de courriels peuvent maintenant utiliser le cryptage. Dans un système qui utilise la cryptographie symétrique, le destinataire et l'expéditeur partagent la même clé ou le même mot de passe pour décrypter et crypter le message. C'est une bonne méthode à utiliser avec les familles; vous leur donnez le mot de passe pour décrypter le message. La plupart des logiciels de cryptage de courrier électronique utilisent ce système parce qu'il est facile, rapide et peu coûteux. Certains systèmes permettent à l'expéditeur de décider ce qui est crypté et ce qui ne l'est pas, mais nous ne recommandons pas cette approche. Il est beaucoup plus sûr de savoir que tout est crypté.

CRYPTAGE DES PIÈCES JOINTES EN WORD:

Lorsque vous avez terminé la rédaction de votre document en format Word, cliquez sur l'onglet **Fichier (File).** Cliquez sur **Informations (Info).** Sous **Autorisations (Permissions)**, cliquez sur **Protéger le document (Protect Document),** puis sélectionnez **Chiffrer avec mot de passe (Encrypt with Password).** On vous demandera alors d'entrer un mot de passe et de l'entrer une deuxième fois. Envoyez le document par courriel. Dans un courriel séparé, envoyez le mot de passe.

Le Bureau de la Commissaire à l'information et à la protection de la vie privée (CIPVP) a élaboré sept principes pour l'utilisation des courriels avec les patients/clients.

PRINCIPES DE LA CIPVP POUR L'UTILISATION DU COURRIER ÉLECTRONIQUE

1. Il faut respecter et protéger la vie privée des utilisateurs du courrier électronique.
2. Chaque organisme devrait élaborer une politique explicite sur la protection de la vie privée des utilisateurs du courrier électronique.
3. Chaque organisme devrait communiquer sa politique sur l'utilisation du courrier électronique aux utilisateurs et informer ceux-ci de leurs droits et responsabilités liés à la confidentialité des messages dans le système.
4. Les utilisateurs devraient recevoir une formation appropriée sur le courrier électronique et sur les questions de sécurité et de protection de la vie privée liées à son utilisation.
5. Les systèmes de courrier électronique ne devraient pas être utilisés pour recueillir, utiliser et divulguer des renseignements personnels sans que des mesures de sécurité adéquates soient en place pour protéger la vie privée.
6. Les fournisseurs de systèmes de courrier électronique devraient se pencher sur les moyens techniques disponibles pour protéger la vie privée.
7. Les organismes devraient mettre en place des mesures de sécurité appropriées pour protéger les courriels.

DIX CONSEILS POUR UNE PRATIQUE SÉCURITAIRE

1. Faites l'inventaire de tous les appareils et dispositifs électroniques que vous utilisez et qui contiennent des renseignements personnels sur la santé.
2. Pour chaque appareil ou dispositif, déterminez de quelles façons la confidentialité des

patients/clients pourrait être à risque et ce que vous pouvez faire pour vous protéger contre toute atteinte de ce genre.

3. Supposez le pire!
4. Lorsque vous voyagez, conservez tous les dossiers de vos clients dans un cartable verrouillé et rangez votre portable dans le coffre verrouillé de votre auto. Apportez-les avec vous à la maison ou au bureau à la fin de la journée.
5. Lorsque vous utilisez le téléphone, tenez compte des personnes qui pourraient entendre la conversation ou les messages laissés dans la boîte vocale.
6. Familiarisez-vous avec le cryptage et utilisez-le.
7. Documentez TOUTES les mesures que vous utilisez pour assurer la confidentialité et pour veiller à la protection des renseignements personnels.
8. Tenez-vous à jour sur les lois en matière de protection des renseignements personnels et sur les recommandations du Bureau de la Commissaire à l'information et à la protection de la vie privée et de l'OAOO dans les sites Web www.caslpo.com et www.ipc.on.ca.
9. Sachez quoi faire en cas d'atteinte à la vie privée.
10. Appelez-nous au bureau de l'OAOO si vous avez une question au sujet de la protection des renseignements personnels.

Envoyez un courriel à acarlingrowland@caslpo.com ou composez le 416- 975-5347, 1 800 993-9459, poste 226.