THE COLLEGE OF FAMILY PHYSICIANS OF CANADA

LE COLLÈGE DES MÉDECINS DE FAMILLE DU CANADA

Canada Health Infoway

Inforoute Santé du Canada

CONSEIL PRATIQUE

Utilisation avancée et éclairée des DME

MODULE 4

Protection des renseignements personnels et sécurité

NOVEMBRE 2018

À l'ère numérique, il nous incombe, en tant que médecin de famille, de nous informer des enjeux liés à la protection des renseignements personnels et à la sécurité en ce qui a trait aux dossiers médicaux électroniques (DME), ainsi qu'à toutes les autres technologies utilisées pour communiquer les renseignements personnels sur la santé (RPS). Bien qu'il y ait de nombreux avantages à utiliser les DME, les risques de violation des renseignements personnels ont augmenté de façon exponentielle au cours des dernières années.

Les DME ont plusieurs points d'accès (p. ex., ordinateurs, tablettes et téléphones intelligents, courriels, logiciels tiers, etc.), ce qui entraîne plusieurs failles potentielles. Or, les médecins doivent s'assurer de respecter les exigences en matière de protection des RPS dans l'ère électronique.

La plupart des médecins ont confiance en leur façon de pratiquer la médecine. Cependant, ces nouvelles technologies représentent un domaine dans lequel ils s'y connaissent peut-être beaucoup moins.

Pour aider les médecins à répondre à ces enjeux, plusieurs organismes ont créé des recommandations et des lignes directrices. Malheureusement, la myriade de recommandations — comportant parfois des suggestions contradictoires — peut déconcerter les médecins qui essaient de s'y retrouver dans un monde qu'ils ne connaissent pas très bien. Pour brouiller davantage les cartes, des lignes directrices existent à plusieurs niveaux géographiques et à divers paliers gouvernementaux (voir le Tableau 1), et la plupart des médecins trouveront que plusieurs recommandations s'appliquent à leur situation. Ce guide porte sur le palier national. Cependant, les médecins devraient aussi se familiariser avec les recommandations à l'échelle provinciale et locale, qui les touchent.

Tableau 1 : Exemples d'organismes élaborant des lignes directrices

Nationaux	Collège des médecins de famille du Canada (CMFC) Collège royal des médecins et chirurgiens du Canada (Collège royal) Association canadienne de protection médicale (ACPM) Association médicale canadienne (AMC)
Provinciaux	Collèges des médecins et chirurgiens Commissaires à la protection de la vie privée Associations médicales provinciales
Locaux	Institutions de soins de santé Employeurs

DÉFINITIONS

Protection des renseignements personnels : Le droit de contrôler l'accès à sa personne et à l'information sur soi-même. Le droit à la protection des renseignements personnels signifie que les personnes peuvent décider quels types de renseignements donner, quelle quantité, à qui les donner et à quelles fins[1].

Sécurité : Les mécanismes par lesquels les politiques de confidentialité sont mises en œuvre dans les systèmes informatiques, y compris les dispositifs de contrôle d'accès, d'intégrité et de disponibilité[2].

Confidentialité : L'assurance que l'information identifiable sur les personnes, dont la diffusion pourrait constituer une violation de la protecton des renseignements personnels, ne sera pas divulguée sans son consentement, sauf dans la mesure où ceci est permis par la loi[2].

CAS PRATIQUE

Un médecin travaille dans un bureau avec trois autres médecins, deux infirmières et quatre adjoints administratifs. Tous utilisent un système de DME. Si tout le monde avait accès aux DME uniquement à partir du bureau, si tous les ordinateurs étaient encodés et protégés, et si toutes les sauvegardes étaient sécurisées, il serait relativement facile de sécuriser le système.

Considérons toutefois les situations suivantes, qui représentent une utilisation plus typique de la technologie :

- L'ordinateur personnel à la maison ou l'ordinateur portable est utilisé pour consulter le DME, et les sauvegardes sont effectuées sur le nuage ou un disque dur
- Un téléphone intelligent est utilisé pour consulter le DME ou communiquer avec les patients, et les sauvegardes sont effectuées sur le nuage ou l'ordinateur personnel
- Les courriels sont envoyés aux patients à partir de divers appareils électroniques (ordinateur, tablette, téléphone intelligent) par l'intermédiaire d'un compte de courriel non protégé (p. ex., Yahoo, Gmail, Hotmail, etc.)
- Un autre format de messagerie (p. ex., messagerie texte, médias sociaux, etc.) est utilisé pour communiquer avec les patients ou pour échanger des renseignements à leur sujet
- Un fournisseur de service de TI vous offre un soutien technique pour les problèmes d'ordinateur, installe de nouveaux ordinateurs, etc.
- Un commis s'occupe de la facturation et a accès aux DME
- Un fournisseur de services externe offre des fonctionnalités additionnelles (p. ex., kiosque pour la prise de rendez-vous autonome, tablettes pour les patients qui donnent accès au DME, etc.).

De quoi devriez-vous tenir compte en ce qui concerne la protection des renseignements personnels et la sécurité ?

QUESTIONS DE PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE SÉCURITÉ

LA BASE

- Assurez-vous que tous les utilisateurs comprennent la sécurité comme elle s'applique dans leurs rôles et obligations
- Choisissez des mots de passe complexes et protégez-les contre la divulgation
- N'utilisez jamais l'identifiant ou le mot de passe d'une autre personne
- Verrouillez toujours votre ordinateur quand vous vous en éloignez
- Installez un écran de confidentialité sur votre moniteur afin qu'il soit difficile pour les visiteurs de lire le contenu affiché
- Portez des insignes d'identité au travail quand elles sont fournies et interrogez toutes les personnes qui n'en portent pas pour vous assurer qu'il s'agit de personnel autorisé

MATÉRIEL ET LOGICIEL

- Assurez-vous que l'ordinateur et les disques durs sont encodés
- Stockez les RPS sur un réseau partagé sécurisé seulement, et non sur des ordinateurs personnels
- Assurez-vous que les connexions aux données sont sécurisées
- Installez un pare-feu et un logiciel antivirus
- Installez les mises à jour et correctifs logiciels automatiquement, ou en temps opportun
- N'installez pas de logiciel non autorisé
- Ne visitez pas de sites Web de loterie ou de jeux en ligne, ou de sites destinés à un auditoire adulte
- Balayez les ordinateurs chaque semaine pour vous assurer qu'aucun logiciel espion ou non autorisé n'y est installé

APPAREILS MOBILES

Il s'agit notamment des portables, des tablettes et des téléphones intelligents.

- Ne stockez pas de RPS sur ces appareils ; y compris les courriels avec les patients, les notes personnelles ou les images qui peuvent permettre d'identifier des patients
- Assurez-vous que les appareils mobiles sont encodés et peuvent être nettoyés à distance
- Sécurisez les portables avec un verrou câblé quand ils sont utilisés dans des lieux publics
- Assurez-vous que les appareils mobiles sont sauvegardés (p. ex., sur iCloud, Google Cloud, etc.) et que les sauvegardes sont encodées et sécurisées
- Utilisez des mots de passe complexes (p. ex., une combinaison de majuscules et de minuscules, de chiffres et de symboles) et changez-les régulièrement
- Assurez-vous que les pare-feu et les programmes anti-logiciel malveillants sont installés et activés

STOCKAGE PHYSIQUE OU STOCKAGE SUR LE NUAGE POUR LES DONNÉES DES DME

- Serveur physique local
  - Assurez-vous que la connexion au DME est sécurisée
  - Assurez-vous que le serveur est hébergé dans un endroit sécurisé, avec une sauvegarde hors site
  - Assurez-vous qu'une entente est en place pour régir la protection des renseignements personnels et la confidentialité dans le cas du recours à des tiers pour la gestion des serveurs
- Stockage sur le nuage (modèle de fournisseur de services applicatifs (ASP))
  - Assurez-vous que des lignes de communication sécurisées sont utilisées pour les données en transit
  - Assurez-vous que les sauvegardes et le stockage sur le nuage sont situés au Canada ; les emplacements internationaux sont soumis à la loi sur la protection des renseignements personnels de ces pays (les fournisseurs devraient en être au courant)
  - Assurez-vous de comprendre comment le stockage sur le nuage est géré, et quels sont vos droits en ce qui concerne vos données stockées :

- Le stockage est-il privé ou partagé ?
- Qui gère l'infrastructure ?
- Quelles sont les pratiques en matière de sécurité et de gestion de l'information du fournisseur de services ?
- Qui a accès aux données ?
- Une évaluation des impacts sur la protection de la vie privée a-t-elle été effectuée ?
- Pouvez-vous détecter des violations à la protection des renseignements personnels ?
- Y a-t-il une entente de protection des renseignements personnels et de confidentialité signée en place ?
- Les données peuvent-elles être effacées de façon permanente, y compris les fichiers de sauvegardes, si vous décidez de changer de modèles ?

SAUVEGARDES

- Effectuez des sauvegardes régulières de vos données au moins une fois par semaine (idéalement tous les jours) et conservez-les hors site
- Vérifiez au moins deux fois par année que les données peuvent être restaurées des fichiers de sauvegardes
- Conservez tous les documents papier et les supports de sauvegarde dans un contenant à l'épreuve du feu
- Effectuez une sauvegarde du serveur physique
  - Assurez-vous que le serveur de sauvegarde est situé dans un lieu sécurisé loin de votre serveur principal
  - Assurez-vous que la connexion est sécurisée
  - Établissez des sauvegardes automatiques
- Sauvegarde du stockage dans le nuage
  - Assurez-vous de comprendre comment fonctionne le stockage dans le nuage :

- Les sauvegardes sont-elles effectuées ?
- Combien de copies sont créées ?
- À qui appartiennent les fichiers de sauvegarde ?
- Les sauvegardes se font-elles automatiquement ?
- La sauvegarde est-elle testée périodiquement ?

COURRIELS ET MESSAGERIE SÉCURISÉE

- Les échanges par courriel avec les patients
  - Tenez compte des avantages d'obtenir le consentement des patients pour les communications électroniques, préférablement par écrit
  - Utilisez un compte de courriel sécurisé sur un appareil encodé, ou envoyez des messages sécurisés par l'intermédiaire d'un portail pour les patients
  - Où sont conservés ces courriels ? Sont-ils sur divers appareils portables et ordinateurs, ou y a-t-il un processus pour les effacer du serveur de courriels ?
  - Incluez les renseignements suivants dans les signatures ou les notes en bas de page des courriels :
    - Un énoncé selon lequel le contenu du courriel est confidentiel
    - Des instructions sur la façon dont les courriels reçus par erreur seront gérés
    - La recommandation que les personnes qui reçoivent des courriels utilisent seulement des adresses courriel sécurisées qui sont protégées par un mot de passe
  - Assurez-vous qu'il existe un processus pour confirmer que les adresses de courriel sont à jour
  - Assurez-vous qu'il existe un processus pour inclure les courriels dans le dossier médical du patient
  - Ayez en place des politiques et procédures documentées concernant les communications électroniques, et assurez-vous que les membres du personnel et les patients les connaissent
- Échanges de courriels avec d'autres professionnels de la santé
  - Si les courriels contiennent des RPS, assurez-vous que les expéditeurs et les destinataires utilisent des comptes de courriels sécurisés

Les autres formes de communication électronique (p. ex., la messagerie texte, les médias sociaux, etc.) ne sont pas incluses ici car elles ne sont pas considérées comme sécurisées pour la communication des RPS. De plus, il est difficile d'incorporer les communications avec ces outils dans le DME.

FOURNISSEURS TIERS INTERAGISSANT AVEC LES DME

Plusieurs cabinets embauchent des fournisseurs externes pour les aider à gérer leurs logiciels, matériel informatique, accès à Internet, serveurs et infrastructure de bureau liés aux DME. Les fournisseurs qui ont accès à des RPS devraient connaître les procédures de traitement des données, ainsi que les exigences concernant le respect de la protection des renseignements personnels et de sécurité.

- Tierces personnes potentielles
  - Personnel de soutien aux TI
  - Personnel responsable de la facturation

- Fonctionnalités additionnelles (p. ex., logiciel de prise de rendez-vous autonome)
- Laboratoires

- Questions à se poser
  - Une entente de partages de données est-elle requise et en place ?
  - Une entente de protection des renseignements personnels et de confidentialité a-t-elle été signée ?
  - Les tierces parties ont-elles accès aux données de façon sécurisée ?
  - Y a-t-il des RPS stockés ailleurs ?

ÉDUCATION ET SENSIBILISATION POUR LE PERSONNEL CLINIQUE ET NON CLINIQUE

- Assurez-vous qu'une politique sur la protection des renseignements personnels (et les procédures connexes) soit en place pour tous les membres du personnel
- Assurez-vous que tous les membres du personnel suivent une formation sur la protection des renseignements personnels et la sécurité, au moment de l'embauche et sur une base continue
- Désignez un agent de la protection des renseigments personnels
- Assurez-vous que les ententes de confidentialité et d'utilisateurs finaux sont signées par tous les membres du personnel
- Assurez-vous qu'un processus est en place pour gérer l'accès seulement aux données pertinentes au rôle de chaque membre du personnel
- Assurez-vous qu'un processus est en place pour supprimer l'accès quand un employé quitte son poste
- Assurez-vous qu'un processus de vérification est en place pour les données du DME

GESTION DES VIOLATIONS DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

GESTION

- Existe-t-il une politique pour gérer une violation des RPS ?
- Avez-vous une politique pour gérer la perte d'un appareil électronique (p. ex., téléphone intelligent ou ordinateur portable) ?
  - La politique devrait inclure la possibilité de désactiver à distance et de nettoyer l'appareil immédiatement, et de le signaler au fournisseur de télécommunication

CYBER-ASSURANCE

Incontestablement, la mise en place de ces moyens de protection n'est pas une mince tâche pour des médecins occupés. Bien que rien ne remplace la diligence raisonnable, le besoin d'une garantie en cas de problème se fait sentir de plus en plus. Même les politiques et procédures les plus strictes ne peuvent garantir que les pirates informatiques n'accéderont pas au DME ou à un appareil connexe. La cyberassurance, un produit relativement nouveau, peut aider à gérer ces risques et est considérée comme un investissement judicieux par plusieurs personnes.

PERSPECTIVE GÉNÉRALE

Manifestement, les DME sont là pour de bon. Il est aussi évident que les exigences complexes en matière de protection des renseignements personnels et de la sécurité de ces systèmes peuvent être source de stress et d'angoisse pour les médecins de famille.

Les médecins ne sont généralement pas bien formés sur les technologies de l'information et les enjeux associés. Cependant, nous sommes obligés de faire preuve de diligence raisonnable afin de respecter nos obligations professionnelles et de respecter la confidentialité. Ce module donne un aperçu des questions liées à la protection des renseignements personnels et à la sécurité dont il faut tenir compte, surtout dans un contexte de soins offerts en équipe, basés sur le modèle du Centre de médecine de famille. Le potentiel de violation de la protection des renseignements personnels dans les nombreux points d'accès aux DME pour le partage des données sur les patients ne peut être négligé. Pour de plus amples renseignements, consultez les ressources nationales suivantes, en plus des lignes directrices des organismes provinciaux/locaux.

RESSOURCES POUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LA SÉCURITÉ

L'ASSOCIATION CANADIENNE DE PROTECTION MÉDICALE (ACPM)

- Piratage par rançongiciel : savez-vous comment y faire face ?
- Les communications électroniques et les renseignements personnels
- Protection des renseignements sur la santé des patients dans les dossiers électroniques
- Modèle de formulaire : Consentement à l'utilisation de moyen de communication électronique
- Guide sur les dossiers électroniques

INFOROUTE SANTÉ DU CANADA (ISC)

- Enjeux et exigences de protection des renseignements personnels et de sécurité des solutions de santé numériques
- Document de travail – Les ententes de partage de données et le dossier de santé numérique interopérable

ASSOCIATION MÉDICALE CANADIENNE (AMC)

- Principes directeurs de l'adoption par les médecins du dossier médical électronique (DME) en pratique clinique ambulatoire
- Accords d'échange de données : Principes pour les dossiers médicaux/électroniques/dossiers de santé électroniques
- Principes directeurs pour l'utilisation optimale de l'analyse des mégadonnées par les médecins en situation clinique

REMERCIEMENTS

Je tiens à remercier Madame Abigail Carter-Langford (Chef de la protection des renseignements personnels, Inforoute) et Madame Nancy Cahill (Directrice des initiatives sur la protection des renseignements personnels, Inforoute) pour leurs commentaires et leurs contributions à ce document.

Références

1. Cavoukian A. *Privacy by Design: From Rhetoric to Reality*. Toronto, ON: Commissaire à l'information et à la protection de la vie privée de l'Ontario ; 2012.
2. O'Carroll P, Yasnoff W, Ward M, Ripp L, Martin E, eds. *Public Health Informatics and Information Systems*. New York, NY: Springer Science & Business Media; 2006.