Guide de SÉCURITÉ DE L'INFORMATION POUR LE SECTEUR DES SOINS DE SANTÉ

Information et ressources à l'intention des

petits cabinets de médecin

Introduction

La *Loi sur la protection des renseignements personnels sur la santé, 2004* (LPRPS) est une loi ontarienne sur la protection de la vie privée propre au secteur de la santé. La LPRPS régit la manière dont les renseignements personnels sur la santé (RPS) peuvent être recueillis, utilisés et divulgués dans le système de soins de santé. Bien que tous les membres du personnel jouent un rôle dans la protection de l'information, la LPRPS rend les professionnels de la santé responsables de la sécurité de l'information dans leur rôle de dépositaires de renseignements sur la santé (DRS) ou d'agents des dépositaires de renseignements sur la santé[1]. Le présent guide est destiné à vous, le médecin et clinicien, pour contribuer à l'élaboration d'un programme de sécurité de l'information destiné aux cabinets de votre collectivité. Il vise à offrir de l'aide pour gérer la sécurité de vos renseignements et créer une pratique de sécurité commune afin de protéger les RPS.

Pour établir un programme de sécurité de l'information au sein de votre cabinet, vous devez créer une politique sur la sécurité; définir les rôles et les responsabilités à l'égard de la protection de l'information; s'assurer que tout le personnel est formé et surveiller la conformité à la politique; être préparé à composer avec des incidents imprévus. Le guide comporte une description des rôles liés à la protection des RPS ainsi que des responsabilités individuelles pour chacun des rôles définis. Il comprend des documents types tels qu'une politique sur la sécurité, une entente de confidentialité et une brochure des pratiques exemplaires courantes en matière de sécurité.

RÔLES

Les pratiques exemplaires sur la sécurité de l'information incluent la désignation de personnes à des rôles et à des responsabilités afin de veiller à ce que les fonds de renseignements qui leur sont confiés soient protégés adéquatement. Dans les cabinets communautaires, il peut y avoir plusieurs rôles liés à la protection des RPS et, dans certains cas, la même personne peut jouer de nombreux rôles.

Dépositaire de renseignements sur la santé (DRS)

Le professionnel de la santé ou la personne qui offre une médecine de groupe avec des professionnels de la santé est considéré comme un DRS en vertu de la LPRPS[2]. Dans la plupart des circonstances, les médecins de pratiques communautaires sont des DRS. Le DRS doit mettre en œuvre des mesures physiques, techniques et administratives raisonnables pour protéger les RPS.

Entre autres obligations, le DRS doit prendre des mesures raisonnables pour s'assurer que les RPS sous leur contrôle ou à leur charge sont :

- exacts et à jour pour les besoins à l'égard desquels l'information est utilisée;
- protégés contre le vol, la perte et l'utilisation ou la divulgation non autorisées;
- protégés contre la copie, la modification ou la destruction non autorisées;
- retenus, transférés et éliminés de manière sécuritaire.

Le DRS doit aviser les patients dès que possible si leurs RPS ont été volés, perdus ou consultés par des personnes non autorisées.

Agent de sécurité

Le membre du personnel nommé par le médecin ayant la responsabilité générale de gérer le programme de sécurité quotidiennement. Dans un environnement de bureau, un agent de sécurité peut être l'infirmière, l'adjoint du cabinet médical ou un autre professionnel de la santé.

Fournisseur de service de TI

Une personne ou une entreprise qui offre des services de TI au cabinet de médecin, comme l'installation et l'entretien d'ordinateurs, l'installation de nouveaux logiciels et la prestation d'une connectivité de réseau.

Tout le personnel

Bien qu'il y ait des rôles désignés aux responsabilités précises quant à la protection des RPS, tout le personnel qui a accès aux RPS a également des obligations.

[1] Si vous n'êtes pas certain de votre rôle en tant que dépositaire de renseignements sur la santé (DRS) ou qu'agent en vertu de la LPRPS, veuillez consulter la loi qui se trouve à l'adresse : http://www.e-laws.gov.on.ca/html/statutes/french/elaws_statutes_04p03_f.htm. Le site Web du Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario, http://www.ipc.on.ca/french/home-page/default.aspx, offre également des ressources aux fournisseurs de soins de santé.

[2] LPRPS 3.(1)2.

Parcours du Guide

Voici des volets du guide conçus pour être créés ou utilisés par des personnes occupant différents rôles.

Dépositaire de renseignements sur la santé

Politique sur la sécurité
Une politique type simplifiée qui fixe des exigences, assigne des responsabilités et démontre l'engagement du médecin à protéger les RPS.

Responsabilités liées à la sécurité du personnel et entente de confidentialité
Une entente type devant être lue, comprise et signée par tous les membres du personnel, qui reconnaissent ainsi leurs responsabilités individuelles avant d'avoir accès à de l'information confidentielle.

Agent de sécurité

Responsabilités liées à la sécurité du personnel
Une liste des principales responsabilités applicables à tout le personnel médical et administratif du cabinet qui pourrait avoir accès à des RPS.

Guide de référence rapide
Un guide sur des pratiques exemplaires simples en sécurité de l'information qui englobent les principales mesures de protection physiques, techniques et administratives de l'information.

Fournisseur de services de TI

Responsabilités liées à la sécurité des fournisseurs de services de TI
Une liste des responsabilités minimales en matière de sécurité auxquelles un fournisseur de services de TI doit se conformer lorsqu'il offre des services techniques au cabinet.

Entente de reconnaissance de la sécurité et de confidentialité
Une entente type devant être lue, comprise et signée par tout le personnel et les personnes qui gèrent et exploitent des ressources d'information qui comportent de l'information confidentielle, qui reconnaissent ainsi leurs responsabilités individuelles avant d'avoir accès à de l'information confidentielle.

Tout le personnel

Politique sur la sécurité
Lire la politique qui fixe des exigences, assigne des responsabilités et démontre l'engagement du médecin à protéger les RPS.

Entente de reconnaissance de la sécurité et de confidentialité
Faire lire, comprendre et signer par tous les membres du personnel, l'entente par laquelle ils reconnaissent leurs responsabilités individuelles avant d'avoir accès à de l'information confidentielle.

Responsabilités liées à la sécurité du personnel
Une liste des principales responsabilités applicables à tout le personnel médical et administratif du cabinet qui pourrait avoir accès à des RPS.

Guide de référence rapide
Un guide sur des pratiques exemplaires simples en sécurité de l'information qui englobent les principales mesures de protection physiques, techniques et administratives de l'information.

Responsabilités liées à la sécurité du personnel

- ☐ Lire la politique sur la sécurité et s'y conformer.
- ☐ Lire et signer l'Entente de reconnaissance de la sécurité et de confidentialité et s'y conformer.
- ☐ Lire et suivre les pratiques exemplaires pour la sécurité dans le Guide de référence rapide sur les pratiques exemplaires liées à la sécurité de l'information.
- ☐ Suivre les pratiques en matière de rangement du bureau, particulièrement dans les lieux de travail sans surveillance. Se reporter à la section Rangement du bureau et environnement du Guide de référence rapide sur les pratiques exemplaires liées à la sécurité de l'information.
- ☐ Verrouiller les classeurs, lorsqu'ils sont sans surveillance, et protéger les appareils informatiques mobiles, comme les ordinateurs portatifs.
- ☐ Interroger les inconnus qui entrent dans des zones réservées.
- ☐ Protéger l'information et les ordinateurs utilisés à l'extérieur du bureau selon la feuille-info du CIPVP
- ☐ Chiffrer des renseignements personnels liés à la santé sur des appareils mobiles[3].
- ☐ Éviter d'exposer accidentellement de l'information sensible lors de conversations, sur des écrans d'ordinateur exposés et dans des bureaux sans surveillance.
- ☐ Éliminer les copies papiers de renseignements personnels sur la santé et des médias numériques selon les feuilles-infos du CIPVP ***La destruction sécurisée de renseignements personnels et La protection des renseignements personnels sur la santé.***
- ☐ Avant d'envoyer une télécopie, confirmer que le numéro est toujours valide et qu'il a été composé correctement. Consulter les autres pratiques exemplaires du document du CIPVP ***Directives concernant la sécurité des transmissions par télécopieur.***
- ☐ Signaler tous les incidents liés à la sécurité à l'agent de sécurité.

[3] http://www.ipc.on.ca

Responsabilités de l'agent de sécurité

- ☐ S'assurer que la Politique sur la sécurité est affichée bien en vue dans le bureau afin qu'elle soit accessible au personnel et aux patients.
- ☐ S'assurer que le personnel et les entrepreneurs sont au courant de la Politique sur la sécurité et qu'ils sont informés de la façon dont elle devrait être interprétée et mise en action avec l'aide du Guide de référence rapide sur les pratiques exemplaires liées à la sécurité de l'information.
- ☐ S'assurer que tout le personnel est formé à ses responsabilités liées à la sécurité. Consulter les Responsabilités liées à la sécurité du personnel et le Guide de référence rapide sur les pratiques exemplaires liées à la sécurité de l'information.
- ☐ Recueillir et classer les Ententes de reconnaissance de la sécurité et de confidentialité signées et datées de tout le personnel et des fournisseurs de service de TI.
- ☐ S'assurer que l'élimination des renseignements personnels et personnels sur la santé respecte les normes de sécurité prévues à la feuille-info du CIPVP ***La destruction sécurisée de renseignements personnels et La protection des renseignements personnels sur la santé***[4]**.**
- ☐ S'assurer que le personnel a accès à une déchiqueteuse pour éliminer de manière sécuritaire les renseignements personnels sur la santé qui ne sont plus nécessaires.
- ☐ Informer le personnel de la façon de créer des mots de passe forts, faciles à mémoriser, mais difficiles à deviner, et ne jamais communiquer ses mots de passe. Consulter la section des lignes directrices sur les mots de passe du Guide de référence rapide sur les pratiques exemplaires liées à la sécurité de l'information.
- ☐ S'assurer que les membres du personnel savent qu'ils ne doivent pas installer de logiciels non autorisés, brancher des appareils non autorisés à leurs ordinateurs ni utiliser leurs ordinateurs à des fins non autorisées.
- ☐ S'assurer que tous les membres du personnel font des sauvegardes hebdomadaires de leurs données. Si possible, conserver les copies de sauvegarde hors site.
- ☐ Révoquer ou modifier judicieusement l'accès (physique, réseau, système et application) et modifier les mots de passe communs dès que les employés quittent le service ou changent de responsabilités.
- ☐ Demander au fournisseur de service en TI de configurer les mesures de sécurité sur tous les ordinateurs de bureau, notamment un chiffrement fort[5] , des correctifs de sécurité et des solutions antivirus.
- ☐ S'assurer que le fournisseur de service de TI fournit une description écrite du service offert.
- ☐ Signaler tous les incidents liés à la sécurité au dépositaire de renseignements sur la santé. Organiser l'aide dans la réalisation de l'investigation, au besoin, et s'assurer que les mesures correctives nécessaires sont mises en place.
- ☐ Surveiller et effectuer des vérifications ponctuelles régulières pour s'assurer que tous les membres du personnel suivent la Politique sur la sécurité. Prendre des mesures appropriées si elle n'est pas suivie.

[4] http://www.ipc.on.ca

[5] Consulter la feuille-info du CIPVP Le chiffrement fort dans les soins de santé à *http://www.ipc.on.ca.*

Responsabilités du fournisseur de service de TI

- ☐ Signer l'Entente avec le cabinet avant d'avoir accès à de l'information confidentielle, s'il y a lieu.
- ☐ Lire la Politique sur la sécurité et signer l'Entente de reconnaissance de la sécurité et de confidentialité avant de commencer un travail.
- ☐ Placer le ou les ordinateurs dans un endroit sûr pour minimiser les risques de modification, de perte, d'accès, de vol, de consultation et de divulgation par des personnes non autorisées.
- ☐ S'assurer que chaque utilisateur d'un ordinateur reçoit un identificateur d'utilisateur unique et qu'il choisit son propre mot de passe.
- ☐ Former les membres du personnel à l'utilisation de mots de passe forts comportant de 8 à 10 caractères et constituant une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.
- ☐ Faciliter des caractéristiques de sécurité comme des mots de passe et un économiseur d'écran verrouillé.
- ☐ Installer et gérer le chiffrement des disques durs, s'il y a lieu. Consulter la feuille-info du CIPVP ***Le chiffrement fort dans les soins de santé***[6]**.**
- ☐ Installer des logiciels de sécurité, comme un anti-virus, un anti-pourriel, un logiciel anti espion et un pare feu personnel d'un fournisseur digne de confiance et les mettre à jour.
- ☐ Utiliser régulièrement des correctifs de sécurité et des mises à jour sur des ordinateurs.
- ☐ Brancher les ordinateurs à un système d'alimentation sans coupure (UPS).
- ☐ S'assurer que l'agent de sécurité responsable de la sécurité générale du bureau comprend les caractéristiques de sécurité installées et les mesures à prendre dans le cas d'un incident.

Remarques : Les responsabilités du fournisseur de service de TI, servent aussi à orienter l'agent de sécurité dans la surveillance d'un tiers avec lequel le professionnel de la santé ou les professionnels de la médecine de groupe souhaitent signer un contrat pour offrir un soutien en TI.

6 http://www.ipc.on.ca

Modèle

Notre Politique sur la sécurité

Notre bureau s'engage à protéger les renseignements personnels et les renseignements personnels sur la santé de tous nos patients conformément aux obligations juridiques énoncées dans la *Loi sur la protection des renseignements personnels sur la santé* (LPRPS) et conformément à de bonnes pratiques d'affaires et à des pratiques exemplaires en matière de vie privée et de sécurité.

En particulier, nous assumons les responsabilités suivantes :

1. Protéger les renseignements personnels des patients ou des clients et les renseignements personnels sur la santé contre le vol, la perte ainsi que la collecte, l'utilisation ou la divulgation non autorisées et s'assurer que les dossiers contenant l'information sont protégés contre la reproduction, la modification ou l'élimination non autorisées.
2. Nous conformer aux exigences législatives et réglementaires.
3. Nommer un agent de sécurité désigné.
4. Voir à ce que les membres du personnel comprennent leurs responsabilités et s'assurer qu'ils reçoivent la formation appropriée pour s'acquitter de ces responsabilités.
5. Fournir du matériel de référence au personnel avec des pratiques de sécurité utiles dans des secteurs clés ayant une incidence sur les activités de notre cabinet.
6. Effectuer des examens périodiques des pratiques de sécurité.
7. Afficher bien en vue la politique sur la sécurité pour un accès rapide par le personnel et nos patients.
8. Conclure des ententes contractuelles comportant des engagements en matière de sécurité avec un tiers qui pourrait traiter des renseignements personnels et des renseignements personnels sur la santé.

Signature du clinicien : _____

Nom en caractères d'imprimerie : _____

Date : _____

Modèle

Entente de reconnaissance de la sécurité et de confidentialité

En envisageant de travailler à ce cabinet, je reconnais l'importance de protéger la confidentialité et l'intégrité des renseignements personnels ou des renseignements personnels sur la santé auxquels j'ai accès. J'accepte de ne pas recueillir, utiliser ni divulguer ces renseignements à toute personne ou organisation, sauf si cela est nécessaire dans la prestation de mes services.

D'autre part, j'assume les responsabilités suivantes :

i. je reconnais que j'ai reçu, lu et compris la Politique sur la sécurité du cabinet

ii. je reconnais que j'ai reçu, lu et compris le Guide de référence rapide sur la sécurité, ainsi qu'un énoncé de mes responsabilités en ce qui a trait à la protection de la confidentialité de l'information

iii. j'accepte que la politique de ce cabinet et les directives justificatives font partie de mes conditions d'emploi ou de mon contrat, et que toute infraction à cette Entente de reconnaissance de la sécurité et de confidentialité peut entraîner des mesures disciplinaires, même la résiliation de mon emploi ou de mon contrat

iv. j'accepte que j'aviserai immédiatement la personne ayant la responsabilité générale de la sécurité dans le cabinet si je deviens au fait de toute infraction à la Politique sur la sécurité du cabinet, ou aux directives justificatives, notamment toute collecte, utilisation, divulgation ou élimination non autorisées de renseignements personnels sur la santé, autres que conformément à la Politique sur la sécurité de ce cabinet, telle qu'elle est modifiée de temps à autre.

Signature de l'employé : _____

Nom en caractères d'imprimerie : _____

Date : _____

[7] Pour les besoins de cette Entente de reconnaissance de la sécurité et de confidentialité, les renseignements personnels sur la santé ont le même sens que les renseignements personnels sur la santé définis à la section 4 de la *Loi sur la protection des renseignements personnels sur la santé,* 2004 (LPRPS).

cyberSanté Ontario

C.P. 148, 777, rue Bay
Bur. 701, Toronto, (Ontario) M5G 2C8
Tél. : 416 - 586 - 6500
Téléc. : 416 - 586 - 4363

Sans frais. : 1 888 441 - 7742
Courriel : info@ehealthontario.on.ca
Web : www.cybersanteontario.on.ca