Mai 2025

Guide de gestion de la protection de la vie privée à l'intention des petits organismes de soins de santé

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

Nous vous présentons le *Guide de gestion de la protection de la vie privée à l'intention des petits organismes de soins de santé* du CIPVP

Que vous soyez un professionnel de la santé exerçant à titre individuel ou que vous dirigiez une clinique ou un petit cabinet, le présent guide vous aidera à élaborer un programme de gestion de la protection de la vie privée et à respecter vos obligations en vertu de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS).

Table des matières

Objet

Le présent guide est un document de référence destiné aux praticiens de la santé exerçant à titre individuel et aux autres petits organismes de soins de santé aux fins de l'élaboration d'un programme efficace de gestion de la protection de la vie privée.

Il peut les aider à relever les lacunes ou faiblesses éventuelles de leurs pratiques relatives aux renseignements à combler pour mieux protéger les renseignements personnels sur la santé de leurs patients.

Le présent guide (et ses annexes) résume des exigences de base et des pratiques exemplaires en vertu de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* à titre informatif seulement. Il ne saurait se substituer à la loi et ne constitue pas un avis juridique. Il ne lie pas le tribunal du CIPVP, qui peut être appelé à enquêter et à rendre une décision sur une plainte ou un appel en se fondant sur les circonstances et les faits pertinents. Pour consulter la version la plus récente de ces lignes directrices, veuillez visiter le site **www.ipc.on.ca/fr**.

Le CIPVP a consulté des praticiens de la santé, des experts en protection des renseignements personnels sur la santé, des associations du secteur de la santé et des membres du Conseil consultatif stratégique du CIPVP lors de la rédaction d'une version antérieure du présent document. Le CIPVP les remercie de leurs commentaires.

1.0 Introduction

Dans le monde numérique d'aujourd'hui, la protection des renseignements personnels sur la santé est plus importante que jamais. C'est pourquoi il est essentiel d'adopter de bonnes pratiques relatives aux renseignements dans le cadre d'un programme rigoureux de gestion de la protection de la vie privée. Il s'agit non seulement de respecter les lois sur la protection de la vie privée, mais aussi de protéger les renseignements personnels sur la santé de vos patients et de leur donner confiance en vous.

1.1 À propos du présent guide

La protection de la vie privée est primordiale

Il est essentiel d'observer la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) de l'Ontario pour assurer la protection des particuliers et respecter leurs droits, mais cela peut sembler une tâche complexe, voire insurmontable pour les praticiens qui exercent seuls et les petits organismes de soins de santé. Le présent guide vise à clarifier vos obligations en matière de protection des renseignements personnels sur la santé et à vous aider à mettre en place un cadre de gestion de la protection de la vie privée pour votre cabinet.

Conseils et outils pour réussir

Dans le présent guide, nous vous proposons :

- des renseignements sur la marche à suivre pour satisfaire aux exigences de la LPRPS;
- des conseils et des directives pour vous aider à élaborer un programme de gestion de la protection de la vie privée adapté à votre cabinet;
- des ressources supplémentaires à consulter pour obtenir de plus amples renseignements.

En fin de compte, pour réussir, il est essentiel d'établir de bonnes pratiques de gestion de la protection de la vie privée qui montrent que vous respectez la LPRPS et que vous vous souciez de vos patients. Les praticiens de la santé sont très occupés; notre objectif n'est pas de faire de vous des experts en protection de la vie privée, mais plutôt de vous fournir des renseignements de base sur les mesures concrètes que vous devez prendre pour respecter vos obligations en la matière. Ce document est rédigé en langage simple et facile à lire, pour les praticiens de la santé qui ne sont pas des spécialistes de la protection de la vie privée. Nous espérons que vous le trouverez utile pour élaborer ou renforcer votre programme de gestion de la protection de la vie privée.

À qui s'adresse le guide?

Le guide est destiné surtout aux dépositaires qui sont :

- des praticiens exerçant à titre individuel qui possèdent et exploitent indépendamment leur propre cabinet de soins de santé;
- de petites cliniques qui fournissent des services de santé semblables ou interdisciplinaires;
- des exploitants de petits établissements de santé.

Parmi les exemples de dépositaires, mentionnons les médecins, les infirmières, les audiologistes et les orthophonistes, les chiropraticiens, les podologues, les professionnels des soins dentaires, les diététistes, les massothérapeutes, les sages-femmes, les optométristes, les ergothérapeutes, les opticiens, les pharmaciens, les physiothérapeutes, les psychologues et les inhalothérapeutes.

Que vous exerciez à titre individuel ou en tant que membre d'un petit établissement de soins de santé, comme un cabinet de médecine familiale, une clinique spécialisée, une clinique sans rendez-vous ou un centre de santé communautaire, le présent guide pourrait vous être utile.

Quoi qu'il en soit, si vous fournissez des soins de santé, il est important de déterminer si vous êtes dépositaire ou mandataire en vertu de la loi. Le présent guide vous renseignera à ce sujet.

Le CIPVP est à votre service

En plus du présent guide, le CIPVP a créé diverses ressources pour aider les organismes et les praticiens de la santé à mieux comprendre leurs obligations en matière de protection de la vie privée et la façon de protéger les renseignements personnels sur la santé. Ces ressources comprennent tout un éventail de lignes directrices, de feuilles-info, de balados et de présentations vidéo. Elles sont accessibles dans le site Web du CIPVP à **www.ipc.on.ca/fr**.

Pour consulter une liste de ressources suggérées, voir l'annexe 4.

Termes clés

Pour comprendre le présent guide, il est important de préciser dès le départ certains termes clés.

Qu'est-ce qu'un dépositaire de renseignements sur la santé?

En vertu de la LPRPS, un dépositaire de renseignements sur la santé (dépositaire) est généralement une personne ou une organisation qui fournit des soins de santé à des particuliers et a la garde ou le contrôle de leurs renseignements personnels sur la santé. Il est important de déterminer d'abord si vous êtes considéré comme un dépositaire, car à ce titre, c'est à vous qu'il incombe de respecter la LPRPS.

Les dépositaires comprennent les praticiens de la santé qui sont membres d'une profession de la santé réglementée ou de l'Ordre des travailleurs sociaux et des techniciens en travail social de l'Ontario qui fournissent des soins de santé, ou toute autre personne dont la fonction principale consiste à fournir des soins de santé contre rémunération.

Les dépositaires comprennent également les exploitants des installations, programmes ou services suivants :

- les hôpitaux, les établissements psychiatriques ou les centres de services de santé communautaires intégrés;
- les foyers de soins de longue durée, les maisons de retraite ou les foyers de soins;
- les pharmacies;
- les laboratoires ou les centres de prélèvement;
- les services d'ambulance;
- les foyers de soins spéciaux;
- les centres, programmes ou services de santé communautaire ou de santé mentale dont le but premier est d'offrir des soins de santé.

Dans certains cas, des organismes qui ne sont pas eux-mêmes des dépositaires en vertu de la LPRPS peuvent retenir les services de dépositaires qui fournissent des soins de santé en leur nom. Mentionnons, par exemple, une infirmière employée par un conseil scolaire; un médecin employé par une équipe sportive professionnelle; un massothérapeute autorisé qui fournit des soins de santé aux clients d'un centre de relaxation privé; ou une infirmière employée en interne dans une entreprise manufacturière.

Qu'est-ce qu'un mandataire?

Un dépositaire peut autoriser un mandataire à recueillir, à utiliser, à conserver, à divulguer ou à éliminer des renseignements personnels sur la santé pour lui-même ou en son nom. Les mandataires ont certaines responsabilités qui leur sont propres en vertu de la LPRPS. Il est toutefois important de noter que le dépositaire demeure responsable des actes de son mandataire, que celui-ci ait ou non l'autorité de le lier, qu'il soit ou non employé par lui et qu'il soit ou non rémunéré. Les mandataires sont souvent des employés, mais ils peuvent aussi être des bénévoles ou des entrepreneurs.

À l'inverse, les employés dont les fonctions et attributions ne comprennent pas le traitement de renseignements personnels sur la santé pour le compte du dépositaire ne sont pas des mandataires. Tout au long du présent guide, nous utilisons le terme « employés » pour désigner les employés à temps plein ou partiel, les entrepreneurs ou les bénévoles. Le terme « mandataires » désigne spécifiquement les membres de l'équipe qui traitent des renseignements personnels sur la santé au nom du dépositaire.

Si vous ne savez pas si vous êtes dépositaire ou mandataire en vertu de la LPRPS, consultez votre association ou ordre professionnel. Vous pouvez également consulter d'autres documents d'orientation publiés par le Commissaire à l'information et à la protection de la vie privée de l'Ontario sur son **site Web** pour mieux comprendre votre rôle et vos obligations.

Que sont les renseignements personnels sur la santé?

Il est important de comprendre ce que sont les renseignements personnels sur la santé au sens de la LPRPS, car celle-ci ne s'applique pas à tous les renseignements.

Aux termes de la LPRPS, les « renseignements personnels sur la santé » sont des renseignements identificatoires concernant un particulier qui se présente sous forme verbale ou autre forme consignée si, selon le cas :

- ils ont trait à la santé physique ou mentale du particulier, y compris aux antécédents de sa famille en matière de santé;
- ils ont trait à la fourniture de soins de santé;
- ils constituent un programme de services pour les particuliers ayant besoin de services de soins à domicile et en milieu communautaire;
- ils ont trait aux paiements relatifs aux soins de santé ou à l'admissibilité à ces soins;
- ils ont trait au don d'une partie de son corps ou d'une de ses substances corporelles ou découlent de l'analyse ou de l'examen d'une telle partie ou substance;
- ils sont le numéro de la carte Santé du particulier;
- ils permettent d'identifier le fournisseur de soins de santé ou le mandataire spécial d'un particulier.

Les renseignements identificatoires comprennent les renseignements qui permettent d'identifier un particulier ou à l'égard desquels il est raisonnable de prévoir qu'ils pourraient servir, seuls ou avec d'autres, à en identifier un. La définition de l'expression « renseignements personnels sur la santé » comprend également d'autres renseignements identificatoires figurant dans un dossier contenant des renseignements personnels sur la santé.

1.2 L'importance de la protection de la vie privée pour votre cabinet et vos patients

Les soins de santé évoluent rapidement en Ontario. Par exemple :

- les fournisseurs offrent de plus en plus des services virtuels en plus des consultations en personne;
- les modèles multidisciplinaires et communautaires offrent des soins plus intégrés et axés sur le patient;
- de nouvelles applications et technologies numériques sont en vente libre, et plus encore.

Dans le contexte de ces changements transformateurs, l'utilisation et la communication des données sur la santé à l'appui de la prestation de soins de santé modernes et efficaces sont plus courantes que jamais.

De plus, nous vivons dans un tout nouveau monde numérique. Même si chaque clic de souris promet quelque chose de nouveau et de passionnant, de dangereuses menaces peuvent se cacher en ligne. La cybercriminalité continue de connaître une croissance exponentielle dans tous les secteurs, y compris celui de la santé, où un volume croissant de renseignements sur la santé existe maintenant en ligne, dans le nuage et dans les systèmes tiers. Les cyberattaques peuvent causer de graves préjudices, notamment la fuite de dossiers confidentiels, la perte d'accès aux dossiers et la perturbation de systèmes et de services. Pour les petits organismes de soins de santé, les cyberattaques peuvent être particulièrement dévastatrices.

Découvrez ce qui est arrivé à une clinique d'imagerie médicale qui a été la cible d'une attaque par rançongiciel, et voyez les leçons pratiques tirées de la réalité des rançongiciels : Décision 249 en vertu de la LPRPS.

Face à ces changements et menaces, il est essentiel que les praticiens de la santé comprennent leurs obligations en matière de protection de la vie privée et respectent leurs engagements envers leurs patients. Les praticiens de la santé d'aujourd'hui doivent être plus vigilants que jamais pour respecter la confidentialité des patients et protéger leurs renseignements personnels sur la santé. Ce sont là des conditions fondamentales pour gagner et conserver la confiance des patients. Ceux-ci fournissent leurs renseignements personnels sur la santé lorsqu'ils demandent des soins médicaux parce qu'ils comptent sur leur fournisseur de soins de santé pour protéger leur vie privée.

Sans cette confiance, les patients peuvent s'abstenir de fournir ces renseignements. Ils peuvent également être moins ouverts au sujet de leurs symptômes ou moins sincères quant à l'observance des plans de traitement. Ils peuvent aussi hésiter à adopter de nouvelles solutions numériques, à participer à la recherche ou à permettre que leurs renseignements personnels sur la santé soient communiqués à des fins générales de santé publique. Pire encore, ils peuvent éviter de demander de l'aide. Comme le dit le vieil adage : « La confiance prend des années à établir, quelques secondes à perdre et une éternité à rétablir. »

1.3 La LPRPS de l'Ontario et son incidence sur votre situation

Tous les Ontariens et Ontariennes jouissent du droit fondamental à la vie privée. Pour respecter ce droit, les dépositaires de renseignements sur la santé sont tenus par la loi de protéger les renseignements personnels sur la santé et de suivre les règles établies en vertu de la LPRPS lorsqu'ils recueillent, utilisent et divulguent ces renseignements.

La LPRPS régit la collecte, l'utilisation et la divulgation des renseignements personnels sur la santé dans le secteur de la santé. Les professionnels de la santé réglementés et les autres dépositaires de renseignements sur la santé en Ontario doivent se conformer à la LPRPS. Le Commissaire à l'information et à la protection de la vie privée (CIPVP) de l'Ontario a pour rôle de surveiller la conformité à la LPRPS afin de s'assurer que les dépositaires de l'Ontario, ainsi que d'autres personnes, organisations et entités assujetties à la LPRPS, respectent les principes et exigences en matière de protection de la vie privée énoncés dans la loi.

Dans le présent guide, nous traitons des aspects auxquels les petits dépositaires de renseignements sur la santé doivent s'attarder et aux mesures qu'ils doivent prendre pour élaborer ou renforcer un programme de protection de la vie privée conforme aux exigences de la LPRPS.

La LPRPS concilie le droit à la vie privée des particuliers avec le besoin légitime des dépositaires de recueillir, d'utiliser et de divulguer des renseignements personnels sur la santé afin de fournir des soins de santé efficaces et en temps opportun.

Vos patients ont les droits suivants :

- **Être informés au sujet de...**
  - la raison pour laquelle vous devez recueillir, utiliser ou divulguer leurs renseignements personnels sur la santé;
  - tout vol, toute perte ou toute utilisation ou divulgation non autorisées de leurs renseignements personnels sur la santé;
  - leur droit de refuser ou de retirer leur consentement à la collecte, à l'utilisation ou à la divulgation de leurs renseignements personnels sur la santé, sauf dans certaines circonstances.
- **Demander...**
  - d'accéder à une copie de leurs dossiers de renseignements personnels sur la santé, sous réserve de certaines exceptions;
  - de faire rectifier leurs dossiers de renseignements personnels sur la santé, sous réserve de certaines exceptions.
- **Porter plainte auprès du CIPVP...**
  - si le dépositaire refuse ou est réputé avoir refusé l'accès à leurs renseignements personnels sur la santé;
  - si le dépositaire a rejeté ou est réputé avoir rejeté une demande de rectification;
  - s'ils s'inquiètent d'une atteinte réelle ou éventuelle à la vie privée.

En tant que dépositaire de renseignements sur la santé, vous pouvez, sous certaines conditions :

- **recueillir les renseignements personnels sur la santé...**
  - qui sont nécessaires pour fournir des soins de santé à votre patient.
- **utiliser des renseignements personnels sur la santé...**
  - pour la gestion des risques ou des erreurs, afin d'améliorer la qualité des soins que vous fournissez à vos patients;
  - en vue d'obtenir un paiement pour la prestation de soins de santé (facturation);
  - pour former vos mandataires sur la prestation de soins de santé.
- **communiquer des renseignements personnels sur la santé...**
  - à des fins de recherche;
  - à un vérificateur ou à une personne qui examine une demande d'agrément ou un agrément;

    - pour appuyer l'évaluation, la planification et la gestion du système de santé;
    - pour contribuer à améliorer la prestation des soins de santé.
- Pour en savoir plus, regardez nos courtes **vidéos sur la protection de la vie privée dans le domaine de la santé de la série *Info CIPVP***, qui expliquent ces concepts en termes simples.

Communication des renseignements personnels sur la santé à des fins de santé générales

En tant que fournisseur de soins de santé, vous recueillez, utilisez ou divulguez des renseignements personnels sur la santé dans le but premier de fournir des soins de santé à vos patients. Toutefois, il est important de savoir que, tant que certaines exigences sont satisfaites, la LPRPS permet également d'utiliser ou de divulguer des renseignements personnels sur la santé en dehors de la relation directe entre le patient et le fournisseur, même sans consentement, afin de contribuer à améliorer le système de soins de santé et la santé du grand public. Ces utilisations et divulgations sont permises, parce que la LPRPS reconnaît que la communication responsable des renseignements personnels sur la santé pour des raisons valables peut se révéler avantageuse pour le public et améliorer les soins de santé pour tous.

La LPRPS permet l'utilisation et la divulgation des renseignements personnels sur la santé aux fins suivantes, sous réserve du respect des exigences précisées :

- mener des recherches;
- planifier, évaluer et gérer le système de santé;
- tenir un registre de renseignements personnels sur la santé afin d'améliorer les soins de santé;
- protéger et promouvoir la santé publique.

Pour en savoir plus sur les diverses utilisations et divulgations des renseignements personnels sur la santé à ces fins et sur les conditions à respecter, veuillez consulter les lignes directrices du CIPVP intitulées **Utilisation et divulgation de renseignements personnels sur la santé à des fins générales de santé publique**.

1.4 Qu'est-ce qu'un programme de gestion de la protection de la vie privée?

Faites de la protection de la vie privée un réflexe!

Lorsque les gens vous confient leurs renseignements personnels sur la santé, ils s'attendent à ce que vous les traitiez en toute sécurité et de façon responsable.

Un programme de gestion de la protection de la vie privée regroupe les politiques, les processus et les mesures que vous pouvez utiliser pour protéger les renseignements personnels sur la santé, respecter les exigences de la LPRPS et gagner la confiance des patients. Mettre sur pied un programme de gestion de la protection de la vie privée vous aidera à respecter les normes de protection de la vie privée que les patients attendent de vous et témoignera de votre engagement à continuer de le faire. En fait, de nos jours, c'est une activité essentielle pour toute organisation moderne.

Établir un programme de gestion de la protection de la vie privée n'est pas une tâche ponctuelle. Vous devez le mettre au point à mesure que votre organisation gagne en maturité et que vous approfondissez vos connaissances et votre compréhension des subtilités de la protection de la vie privée. Ainsi, vos pratiques de gouvernance de l'information deviendront plus rigoureuses au fil du temps, et vous montrerez que vous prenez des mesures raisonnables pour vous conformer à la LPRPS.

Respecter la vie privée des patients, c'est gérer efficacement et protéger les renseignements personnels sur la santé que vous détenez. Vous devez assurer une gestion rigoureuse de l'information et montrer aux patients et à tous vos intervenants que vous avez mis en place de bonnes pratiques.

Déterminez les besoins de votre cabinet

Il n'existe pas de solution universelle pour élaborer un programme de protection de la vie privée. En tant que praticien, vous devez déterminer, en tenant compte de la taille et de la situation de votre organisation, ce qui revêt de l'importance pour votre cabinet, et la meilleure façon d'appliquer les directives du présent guide.

Les avantages d'un programme de gestion de la protection de la vie privée	
	**Améliorer la gestion et la protection de l'information** Un programme bien géré de gestion de la protection de la vie privée vous permet d'établir des pratiques rigoureuses de confidentialité et de sécurité qui rehaussent la protection de vos données sur la santé.
	**Répondre aux attentes des patients et accroître leur confiance** De nos jours, les gens sont plus sensibles que jamais à la façon dont leurs renseignements personnels sur la santé sont traités. La mise en place d'un programme solide de gestion de la protection de la vie privée indiquera à vos clients que la protection de leur vie privée représente pour vous une priorité absolue.
	**Réduire vos risques** La mise en œuvre d'un programme solide de gestion de la protection de la vie privée réduit le risque de cyberattaques et d'atteintes à la vie privée, ainsi que l'atteinte à la réputation, les coûts financiers et les pertes de temps et de clients qui en résultent.

Les avantages d'un programme de gestion de la protection de la vie privée	
	**Se démarquer en tant que chef de file dans votre communauté** Ne considérez pas la protection de la vie privée comme une obligation; traitez-la comme un facteur de différenciation! Un bon programme de protection de la vie privée indique que vous avez les intérêts des patients à cœur, et vous distingue en tant que chef de file dans votre communauté. De plus, les partenaires et fournisseurs préfèrent les professionnels et des organisations qui se soucient de la protection de la vie privée.
	**Assurer la conformité réglementaire** Comme les règlements sur la protection de la vie privée sont devenus plus stricts, la création d'un programme de gestion de la protection de la vie privée qui englobe les politiques et pratiques nécessaires peut vous aider à respecter vos obligations en vertu de la LPRPS et à éviter les conséquences de la non-conformité.

1.5 Premiers pas

Contrairement à ce que l'on pourrait croire, l'élaboration d'un programme de gestion de la protection de la vie privée n'est pas nécessairement une tâche ardue. Le présent guide décrit le processus de création, de tenue à jour et d'application d'un programme qui vous conviendra, à vous et à votre cabinet. Vous trouverez ci-après des conseils et des renseignements qui simplifieront votre cheminement dans toute la mesure du possible.

Ne vous attendez pas à créer un programme de protection de la vie privée en une journée, ou même en une semaine! Le processus dépendra bien sûr de la taille de votre cabinet et du temps que vous pouvez y consacrer. C'est un parcours; abordez-le par étapes, en consultant le présent guide.

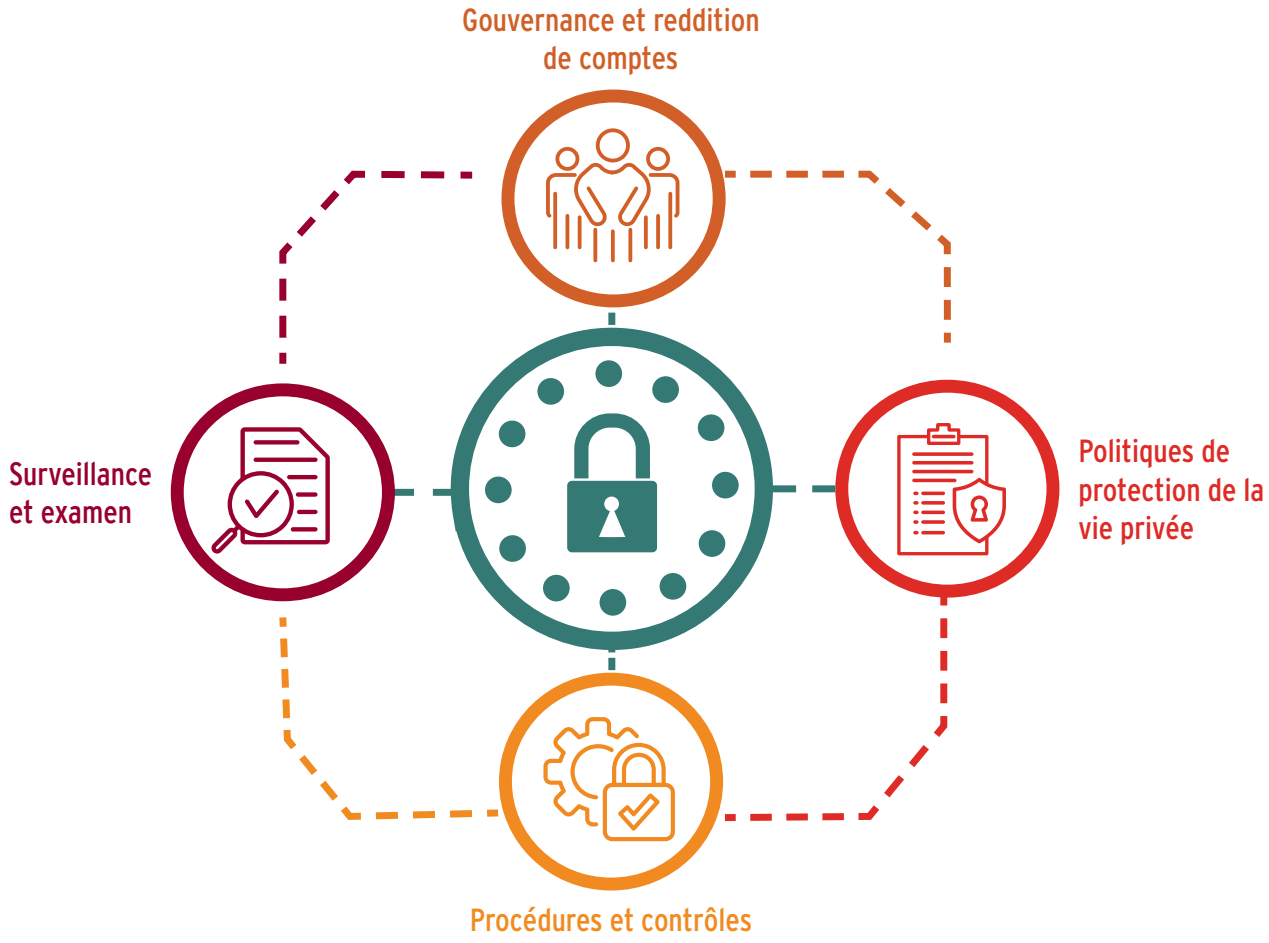
Composantes initiales d'un programme de gestion de la protection de la vie privée pour les petits organismes de soins de santé

La mise en place d'un programme rigoureux de gestion de la protection de la vie privée nécessite une planification et une réflexion minutieuses. Bien qu'un tel programme comporte de nombreux éléments, quatre principales composantes sont à prendre en compte :

1. **Gouvernance et reddition de comptes :** elles créent un fondement solide pour votre programme en attribuant clairement les rôles et les responsabilités afin que rien ne soit laissé au hasard;
2. **Politiques de protection de la vie privée :** il s'agit de règles écrites que vous et vos employés vous engagez à suivre afin que chacun comprenne clairement ce qu'il est censé faire;
3. **Procédures et contrôles :** ils vous aident à opérationnaliser vos politiques dans la pratique;
4. **Surveillance et examen :** ce sont les moyens grâce auxquels vous évaluez continuellement l'efficacité de votre programme et y apportez des améliorations au fil du temps.

Le présent guide décrit chacune de ces composantes en détail.

Programme de gestion de la protection de la vie privée : les petits organismes de soins de santé



2.0 Gouvernance et reddition de comptes : jeter les bases du programme

Un programme rigoureux de gestion de la protection de la vie privée commence par la gouvernance et la reddition de comptes. Il s'agit d'adopter une approche globale et structurée pour attribuer les rôles et les responsabilités et intégrer une culture de protection de la vie privée au cœur de vos activités.

2.1 Ton donné par la direction

Intégrez la protection des données dans votre culture organisationnelle

Pour protéger efficacement les renseignements personnels sur la santé, la démarche de votre organisation en la matière ne doit pas se limiter à de belles paroles. Pour favoriser une culture qui privilégie la protection de la vie privée et la sécurité, il faut d'abord un leadership et un engagement des échelons supérieurs de l'organisation, quelle que soit sa structure hiérarchique, afin que les pratiques quotidiennes reflètent toujours les principes clés de la protection de la vie privée.

Voici trois principes fondamentaux de la protection de la vie privée qui devraient prévaloir dans l'ensemble de votre organisation :

1. Vous devez recueillir, utiliser ou divulguer des renseignements personnels sur la santé uniquement avec le consentement du particulier concerné, à moins que la LPRPS ne vous autorise à le faire sans consentement.
2. Vous ne devez pas recueillir, utiliser ou divulguer des renseignements personnels sur la santé si les renseignements que vous possédez déjà répondent à vos besoins.
3. Vous devez recueillir, utiliser ou divulguer uniquement les renseignements personnels sur la santé qui sont raisonnablement nécessaires aux fins visées.

Intégrez ces principes fondamentaux dans vos politiques. Mettez-les en application à l'aide de procédures et de pratiques mûrement réfléchies. Veillez à leur respect grâce à une formation efficace et à un suivi et à un examen continus. Tous ces éléments constitutifs se renforceront mutuellement pour former une culture solide de protection de la vie privée et contribueront à assurer la protection des renseignements personnels sur la santé de vos patients.

2.2 La reddition de comptes est essentielle!

Définissez les responsabilités : qui est responsable de la protection des données?

Que ce soit pour un cabinet individuel, une clinique de santé multidisciplinaire ou un petit hôpital, la reddition de comptes est essentielle pour jeter des bases solides pour votre programme de gestion de la protection de la vie privée. Accepter de rendre des comptes, c'est assumer la responsabilité de protéger les renseignements personnels sur la santé.

La première étape consiste à déterminer qui est responsable de votre programme de gestion de la protection de la vie privée. Tous les membres de l'organisation jouent un rôle important dans la mise en œuvre du programme, mais il faut une personne haut placée pour le superviser au quotidien. Clarifier les rôles et responsabilités des membres de votre équipe vous aidera à assurer le succès de vos mesures de protection de la vie privée.

La personne chargée de superviser la mise en œuvre du programme de gestion de la protection de la vie privée reposera sur la taille de votre organisation. Dans le cas des praticiens exerçant à titre individuel ou des petites équipes de soins de santé, le propriétaire du cabinet pourrait assumer le rôle de superviseur direct du programme. Dans les grandes cliniques médicales, vous pouvez désigner une personne en particulier qui jouera ce rôle à temps plein ou à temps partiel. Habituellement, on lui donne le titre de responsable de la protection de la vie privée.

Qu'est-ce qu'un responsable de la protection de la vie privée?

Le responsable de la protection de la vie privée d'une organisation est essentiellement chargé d'élaborer et de mettre en œuvre le programme de gestion de la protection de la vie privée au quotidien et d'assurer le respect de la LPRPS. On peut utiliser un autre titre, par exemple, directeur de la protection de la vie privée ou délégué à la protection de la vie privée, mais les fonctions sont essentiellement les mêmes.

En tant que dépositaire, vous devez désigner une personne (soit vous-même, soit un membre de votre équipe) pour agir à titre de responsable de la protection de la vie privée pour votre organisation.

Le responsable de la protection de la vie privée exerce diverses fonctions, notamment :

- Déterminer les enjeux, les risques et les possibilités liés à la protection de la vie privée qui sont les plus pertinents pour votre organisation.
- Communiquer avec la direction sur les questions liées à la protection de la vie privée.
- Faciliter la conformité de votre organisation à la LPRPS.
- Tenir un inventaire de tous les renseignements personnels sur la santé qui sont recueillis, utilisés et communiqués à autrui.

- Élaborer des politiques et des procédures de protection de la vie privée et de sécurité et veiller à les tenir à jour.
- Former les employés afin qu'ils connaissent et respectent leurs obligations en matière de protection de la vie privée.
- Faire office de personne-ressource principale pour les questions liées à la protection de la vie privée.
- Traiter les questions et les plaintes liées à la protection de la vie privée.
- Répondre aux demandes individuelles d'accès aux renseignements personnels sur la santé et de rectification de ces renseignements.
- Rendre les politiques et pratiques de votre organisation en matière de protection de la vie privée accessibles au public.
- Élaborer un protocole d'intervention en cas d'atteinte à la vie privée et veiller à ce que chacun comprenne son rôle en cas d'incident.
- Évaluer et réviser en permanence votre programme de protection de la vie privée.

Donc, que vous soyez un praticien de la santé exerçant à titre individuel qui assumez ce rôle vous-même ou que vous fassiez partie d'un grand cabinet dans lequel un employé désigné (ou une équipe) se concentre à temps plein ou à temps partiel sur cette tâche, il est crucial d'attribuer à quelqu'un ces responsabilités essentielles pour protéger les renseignements personnels sur la santé.

Le rôle et les responsabilités du responsable de la protection de la vie privée et de toute autre personne qui exerce des fonctions en la matière devraient être clairement définis dans leur description de poste. Veuillez consulter l'annexe 1 pour un exemple de description de poste de responsable de la protection de la vie privée.

2.3 Inventaire des données

Pour disposer d'un bon programme de gestion de la protection de la vie privée, il faut d'abord déterminer l'étendue des renseignements personnels sur la santé dont vous avez la garde ou le contrôle. Il est essentiel de dresser un inventaire de tous les renseignements personnels que vous détenez. Quelle que soit la taille de votre organisation, vous devez connaître les types de renseignements personnels sur la santé dont votre cabinet est responsable et savoir où ils se trouvent. À quel point ces renseignements sont-ils délicats? Sous quelle autorité les avez-vous recueillis, comment les utilisez-vous ou les divulguez-vous, et pendant combien de temps devriez-vous les conserver?

Après avoir dressé la liste des données que vous détenez, vous devriez vous poser les questions suivantes :

- De quels renseignements personnels sur la santé ai-je besoin pour exploiter mon cabinet?
- Pourquoi en ai-je besoin? À quoi servent-ils?

- Ai-je besoin de tous ces renseignements, ou puis-je me contenter de moins?
- Dois-je les conserver? Dans l'affirmative, pendant combien de temps?

Réfléchissez bien aux raisons pour lesquelles vous avez besoin de ces différents types de renseignements et à ce dont vous avez besoin pour servir vos patients. Les dépositaires devraient demander un avis juridique et se référer aux lois, règlements et lignes directrices régissant les membres de leur profession (le cas échéant) ainsi qu'à toute autre loi applicable pour obtenir des renseignements supplémentaires sur les exigences de tenue de dossiers. En général, vous ne devriez pas conserver les renseignements personnels sur la santé plus longtemps que la durée de conservation exigée par la loi, après quoi vous devez les éliminer de façon sécuritaire conformément aux pratiques exemplaires de destruction (voir le chapitre 5).

Vous devriez également déterminer si des renseignements dépersonnalisés plutôt que des renseignements personnels sur la santé peuvent répondre à vos besoins.

La **dépersonnalisation** est le processus consistant à supprimer d'un dossier ou d'un ensemble de données tout renseignement qui permet d'identifier une personne ou qui pourrait raisonnablement servir, seul ou avec d'autres renseignements, à l'identifier. Ce processus peut être complexe et poser des difficultés techniques. S'il n'est pas réalisé correctement, il y a un risque important que certaines personnes puissent être réidentifiées. Si vous envisagez de dépersonnaliser certains de vos fonds de données, vous devriez demander conseil à des experts dans le domaine. Vous, ou l'expert dont vous demandez l'avis, devriez consulter les **lignes directrices détaillées sur la dépersonnalisation des données structurées** du CIPVP (en anglais seulement).

N'oubliez pas que plus vous recueillez de renseignements, plus le risque que vous assumez pour les protéger augmente! Vous devez toujours réduire au minimum la quantité de renseignements personnels sur la santé que vous recueillez, utilisez, conservez et communiquez à autrui.

Mettez-vous toujours à la place de vos patients et utilisez leurs renseignements uniquement aux fins auxquelles ils peuvent raisonnablement s'attendre, pour éviter les mauvaises surprises.

2.4 Déterminez et atténuez à l'avance les risques pour la vie privée

La mise en œuvre de nouveaux systèmes, technologies, programmes ou processus d'information ou leur modification importante peut donner lieu à des risques pour la vie privée de vos patients et la sécurité de leurs renseignements personnels sur la santé. En tant que dépositaire de renseignements sur la santé, vous avez l'obligation de déterminer et de gérer à l'avance ces risques pour la vie privée et à la sécurité.

L'évaluation de l'impact sur la vie privée (EIVP, parfois appelée « évaluation de l'incidence sur la vie privée ») est un outil de gestion des risques que vous pouvez utiliser pour déterminer les risques associés aux changements apportés aux pratiques d'information de votre organisation et

les moyens nécessaires pour y remédier de façon proactive. Les EIVP sont largement reconnues comme une pratique exemplaire en Ontario, dans l'ensemble du Canada et à l'échelle mondiale. Elles sont devenues des outils essentiels pour anticiper et atténuer les répercussions sur la vie privée associées aux systèmes, technologies, programmes et processus de gestion de l'information nouveaux ou différents.

La réalisation d'une EIVP n'a pas besoin d'être complexe ou de prendre beaucoup de temps, mais il faut faire preuve de rigueur pour veiller à bien cerner les risques pour la vie privée, à les évaluer et à les atténuer raisonnablement. La complexité de l'EIVP dépendra de celle de la nouvelle pratique relative aux renseignements que vous instaurez ou du changement que vous envisagez.

Le CIPVP a publié un **guide des EIVP** qui vise à aider les organisations à réaliser des évaluations efficaces, ainsi que des **Lignes directrices concernant l'évaluation de l'incidence sur la vie privée sous le régime de la *Loi sur la protection des renseignements personnels sur la santé***, qui contiennent des directives plus précises pour le secteur de santé. Les petits organismes pourraient envisager de faire appel à des experts externes pour les aider à réaliser une EIVP et profiter de leurs conseils et de leur soutien.

2.5 Collaborez avec des fournisseurs de services

La plupart des petits organismes de soins de santé n'ont pas les ressources nécessaires pour tout faire à l'interne. Ils comptent plutôt sur des fournisseurs de services pour assurer diverses fonctions, comme la livraison et la tenue d'un système de dossiers médicaux électroniques (DME). Ils peuvent faire appel à des fournisseurs externes pour les services de facturation ou de transcription. Ils peuvent s'abonner à des applications, plateformes et outils numériques qui offrent des services numériques, comme les soins virtuels ou des transcripteurs utilisant l'intelligence artificielle (IA). Cependant, il ne faut pas oublier que même lorsque de telles fonctions sont externalisées, c'est le dépositaire de renseignements sur la santé qui reste responsable en dernier ressort de protéger la vie privée des patients et de leur donner accès à leurs renseignements personnels sur la santé.

La LPRPS énonce des exigences particulières pour certains types de fournisseurs de services qui procurent aux dépositaires des moyens électroniques pour recueillir, utiliser, modifier, divulguer, conserver ou éliminer des renseignements personnels sur la santé. Par exemple, ces fournisseurs de services électroniques ne doivent pas utiliser les renseignements personnels sur la santé à une fin autre que celle qui est nécessaire pour fournir le service, et ne peuvent en aucun cas les divulguer. Ils doivent également veiller à ce que leurs employés ou toute autre personne agissant en leur nom respectent également ces restrictions légales.

De plus, un fournisseur de réseau d'information sur la santé qui fournit une technologie de l'information permettant à deux dépositaires ou plus d'échanger des renseignements personnels sur la santé par voie électronique doit satisfaire à d'autres exigences légales. Par exemple, il doit informer le dépositaire de toute violation de la confidentialité des renseignements personnels sur la santé et lui fournir une évaluation de la menace et des risques et une évaluation de l'impact sur la vie privée des services fournis.

Qu'ils utilisent les services d'un fournisseur de services électroniques, d'un fournisseur de réseau d'information sur la santé ou de tout autre fournisseur de services, les dépositaires devraient conclure des ententes écrites énonçant les rôles et responsabilités de toutes les parties concernées. Ces ententes devraient établir des attentes claires décrivant les mesures de protection de la vie privée que chaque partie doit prendre conformément à la LPRPS et comment la conformité sera vérifiée. En fait, la LPRPS exige expressément la conclusion d'ententes écrites entre les fournisseurs de réseau d'information sur la santé et les dépositaires; ces ententes décrivent les services que le fournisseur est tenu de procurer au dépositaire ainsi que les mesures de précaution d'ordre administratif, technique et matériel qui seront prises pour assurer la confidentialité et la sécurité des renseignements, et elles prévoient que le fournisseur de réseau d'information sur la santé doit se conformer à la LPRPS et à ses règlements. De plus, un fournisseur de services électroniques ou un fournisseur de réseau d'information sur la santé qui joue également le rôle de mandataire du dépositaire doit aussi respecter les exigences imposées aux mandataires.

Travailler avec des fournisseurs externes, c'est confier à quelqu'un d'autre le rôle de protéger la vie privée de vos patients; il est donc important de choisir ces fournisseurs judicieusement. En tant que dépositaire, vous devriez évaluer attentivement tout fournisseur de services envisagé pour vous assurer qu'il a la capacité nécessaire pour se conformer à toutes les exigences applicables de la LPRPS et qu'il a de bons antécédents de conformité. Dans certains cas, vous pouvez rechercher des programmes fournis par des intervenants fiables du secteur de la santé pour évaluer les fournisseurs de solutions, comme le programme de certification des **dossiers médicaux électroniques (DME)** d'OntarioMD (en anglais seulement) ou la liste de solutions vérifiées pour les **visites virtuelles** de Santé Ontario accessible à **www.ontariohealth.ca/fr.**

Vous pouvez également consulter le guide du CIPVP intitulé **La protection de la vie privée et l'accès à l'information dans les contrats du secteur public avec des fournisseurs externes**, qui comprend des conseils pratiques et des pratiques exemplaires pour assurer une reddition de comptes appropriée lorsqu'on envisage de travailler avec des fournisseurs de services externes et d'intégrer les facteurs liés à la protection de la vie privée et à la sécurité tout au long du processus d'approvisionnement, du début à la fin.

Petits conseils!

- Évaluez les fournisseurs de services éventuels afin de déterminer s'ils comprennent les exigences établies en matière de protection de la vie privée et de sécurité et toutes les autres exigences, et peuvent y répondre.
- Veillez à ce que les ententes conclues avec les fournisseurs de services tiennent compte des exigences de protection de la vie privée, de sécurité et de conformité et qu'elles soient assorties de modalités claires.
- Établissez clairement les rôles et responsabilités de toutes les parties à un contrat ou à une entente, du début à la fin.

2.6 Donnez à votre équipe les moyens de réussir

Une collaboration efficace avec votre équipe pour assurer la conformité à la LPRPS est un aspect important de votre pratique clinique. C'est aussi un élément essentiel de votre programme de gestion de la protection de la vie privée. Une bonne communication et une formation appropriée appuieront les personnes qui travaillent pour vous et contribueront à promouvoir et à favoriser une culture de protection de la vie privée dans toute votre organisation.

Le saviez-vous?

C'est l'erreur humaine ou la négligence des employés qui constitue la principale cause des atteintes à la vie privée.

Il faut inculquer de bonnes habitudes dès le départ, à commencer par vos pratiques d'intégration du personnel. Tous les membres du personnel qui travaillent avec des renseignements personnels sur la santé, y compris les médecins, doivent bien comprendre leur rôle en tant que mandataires au sens de la LPRPS et leurs responsabilités particulières à l'égard de ces renseignements. Le matériel de formation doit être mis à jour en fonction des nouvelles exigences légales, des leçons retenues ou de toute modification importante apportée aux pratiques relatives aux renseignements. La formation est une responsabilité permanente : elle devrait être donnée régulièrement et faire l'objet d'un suivi pour s'assurer que tout le personnel l'a suivie avec succès.

Pour bien comprendre l'importance de cet aspect, consultez les leçons apprises et les autres points clés dans l'affaire marquante du CIPVP intitulée Prévention des atteintes à la vie privée dans le secteur de la santé : l'importance de la formation, des politiques et des ententes de confidentialité.

Tout le personnel devrait recevoir une formation sur vos politiques, procédures et contrôles afin de savoir comment préserver la confidentialité et la sécurité des renseignements personnels sur la santé et comment repérer et signaler les atteintes éventuelles à la vie privée. Cela vaut même pour les employés qui ne travaillent pas directement avec des renseignements personnels sur la santé. Par exemple, même si un employé n'interagit normalement pas avec de tels renseignements dans le cadre de son travail, il peut en recevoir par erreur, faire l'objet d'une tentative d'hameçonnage ou soupçonner un incident de cybersécurité. Tous les employés, qu'ils soient mandataires ou non, doivent donc savoir quoi faire dans de tels cas. La formation devrait être renforcée par une communication continue afin de maintenir un niveau élevé de sensibilisation à la protection de la vie privée au sein du personnel.

Petits conseils!

- Tout le personnel doit recevoir une formation sur la protection de la vie privée avant l'entrée en fonction ou le début de la relation contractuelle et avant d'avoir accès aux renseignements personnels sur la santé.
- Une formation d'appoint sur la protection de la vie privée devrait être donnée régulièrement ou lorsque des changements sont apportés aux politiques, règlements ou lois.
- Dans le cadre de la formation, vous devez déterminer si votre personnel comprend les exigences de l'Ontario en matière de protection de la vie privée.

- La formation sur la protection de la vie privée axée sur les rôles est une méthode utile pour s'assurer que les gens comprennent comment appliquer les politiques et procédures de protection de la vie privée dans leur travail quotidien.
- Les scénarios fictifs, comme les simulations d'atteinte à la vie privée, pourraient aider tout le monde à s'exercer à réagir lorsqu'une véritable atteinte à la vie privée se produit.
- Les documents de formation sur la protection de la vie privée devraient faire l'objet d'un examen et d'une mise à jour périodiques.
- L'achèvement réussi de la formation requise par chaque employé devrait faire l'objet d'un suivi, dans le respect des bonnes pratiques de tenue des dossiers.

2.7 Obtenez l'engagement de chacun

Pour vous assurer que les membres de votre équipe reconnaissent leurs obligations et engagements en matière de protection de la vie privée, vous devriez conclure avec chacun d'eux une entente de confidentialité écrite qui énonce ces obligations et engagements et explique les conséquences d'une atteinte à la vie privée. La protection de la vie privée devrait être au cœur des préoccupations de tous les employés, qu'ils agissent ou non comme mandataires dans leurs tâches quotidiennes.

Les ententes de confidentialité devraient être signées à l'entrée en fonction (ou à un autre moment convenu) et de nouveau chaque année. Assurez-vous de tenir un registre des personnes qui ont signé l'entente et d'en faire le suivi afin qu'il reste à jour.

Les ententes de confidentialité avec les employés doivent :

- exiger que tous les employés reconnaissent qu'ils ont lu vos politiques et procédures en matière de protection de la vie privée, les comprennent et conviennent de les respecter, et attestent qu'ils comprennent les conséquences possibles d'une non-conformité;
- dans le cas des mandataires, plus précisément, définir les fins pour lesquelles les mandataires sont autorisés à recueillir, utiliser et divulguer des renseignements personnels sur la santé, y compris toute limitation, condition ou restriction, et confirmer qu'ils comprennent leur rôle et leur responsabilité de se conformer à la LPRPS et à son règlement d'application;
- exiger de tous les employés qu'ils restituent en toute sécurité tous les biens à la fin de leur contrat ou de leur emploi, et des mandataires qu'ils rendent tout renseignement personnel sur la santé qu'ils possèdent, le cas échéant;
- préciser que vous pouvez effectuer des audits aléatoires de la protection de la vie privée et de la sécurité pour contrôler périodiquement la conformité aux politiques et procédures en matière de protection de la vie privée et de sécurité;
- exiger des employés qu'ils vous informent de toute atteinte à la vie privée ou à la sécurité à la première occasion raisonnable.

2.8 Expliquez clairement les conséquences de la non-conformité

Un cadre solide de gouvernance et de reddition de comptes permet de préciser ce qui se passera en cas de non-conformité. Les dépositaires devraient décrire les conséquences auxquelles un employé ou un mandataire s'expose en cas de manquement aux politiques, procédures ou obligations en matière de protection de la vie privée.

Adopter une approche fondée sur une culture d'équité consiste à réagir de façon proportionnée aux atteintes à la vie privée. Les erreurs commises de bonne foi peuvent servir d'occasion d'apprentissage pour rappeler les politiques et procédures au personnel, et le former de nouveau sur la façon de les éviter à l'avenir. Selon leur fréquence et leur gravité, certaines erreurs peuvent justifier des mesures correctives ou disciplinaires plus sérieuses pouvant aller jusqu'à la suspension ou même au congédiement. Dans les cas encore plus graves, les atteintes à la vie privée peuvent donner lieu à des pénalités administratives pécuniaires imposées par le CIPVP ou à des poursuites de la part du ministère du Procureur général pour infraction à la LPRPS. Ces conséquences peuvent être imposées au dépositaire responsable, ainsi qu'à la ou aux personnes responsables de l'infraction à la LPRPS.

Il importe d'expliquer clairement les aspects suivants aux employés :

- décrivez les types d'atteintes à la vie privée qui peuvent entraîner des mesures correctives ou disciplinaires;
- décrivez les conséquences possibles d'une atteinte à la vie privée et les facteurs qui seront pris en compte pour déterminer les mesures correctives ou disciplinaires appropriées à prendre, y compris les mesures progressives et l'intervention éventuelle d'ordres professionnels compétents;
- expliquez que certains cas de non-conformité peuvent faire l'objet d'une enquête et indiquez qui sera responsable de mener cette enquête et d'en communiquer les résultats;
- décrivez tous les documents qui seront remplis, fournis ou signés dans le contexte d'une enquête et la période de conservation des résultats;
- expliquez que, dans certains cas, le CIPVP peut enquêter sur des cas de non-conformité, ce qui pourrait donner lieu à la publication de rapports, à une ordonnance judiciaire de mettre fin à certaines pratiques relatives aux renseignements ou de les modifier, et éventuellement à des pénalités administratives pécuniaires;
- dans les cas les plus graves, la non-conformité peut même faire l'objet de poursuites de la part du ministère du Procureur général pour infraction à la LPRPS, et entraîner de lourdes amendes, voire une peine d'emprisonnement.

Omettre de protéger la vie privée peut avoir de graves conséquences. Une personne reconnue coupable d'une infraction en vertu de la LPRPS est passible d'une amende d'au plus 200 000 $ et d'une peine d'emprisonnement d'au plus un an, ou d'une seule de ces peines, s'il s'agit d'une personne physique, ou d'une amende d'au plus 1 000 000 $ dans le cas des organisations. Depuis 2024, le CIPVP a également le pouvoir d'imposer des pénalités administratives pécuniaires (PAP)

dans le cadre de ses pouvoirs d'application élargis en cas d'infraction à la LPRPS ou à son règlement d'application. Ces pénalités peuvent atteindre un maximum de 50 000 $ s'il s'agit d'une personne physique et de 500 000 $ dans le cas des organisations. Le CIPVP peut majorer la pénalité d'un montant égal au bénéfice pécuniaire qu'a acquis la personne ayant contrevenu à la LPRPS. Pour en savoir plus sur les PAP et sur l'approche du CIPVP en matière d'exécution de la loi, veuillez consulter le document d'orientation **Pénalités administratives pécuniaires : Orientations à l'intention du secteur des soins de santé**. Vous pouvez également regarder une courte vidéo d'information *Info CIPVP*, accessible sur la chaîne YouTube du CIPVP, intitulée **Guide sur les pénalités administratives pécuniaires**, qui les explique en termes plus brefs et simples.

2.9 Dressez un plan de sauvegarde des données

Garder le contrôle des renseignements dont vous êtes responsable est un aspect important de la reddition de comptes. Les systèmes informatiques peuvent subir des pannes de courant ou être visés par des voleurs ou des cyberattaques, ce qui peut entraîner le vol, la perte et l'utilisation ou la divulgation non autorisées de renseignements personnels sur la santé. Il est conseillé de mettre en place un plan de continuité des activités et un plan de reprise après sinistre pour assurer la disponibilité continue de votre environnement d'information en cas d'interruption des activités à court et à long terme. Au minimum, ce plan doit comprendre :

- une description de vos méthodes de sauvegarde et de la façon dont vous utiliserez les copies de sauvegarde en cas d'interruption des activités à court ou à long terme;
- les procédures à suivre pour la restauration sécurisée et rapide des fichiers et des systèmes à partir des copies de sauvegarde et des images système, ainsi que la mise à l'essai régulière de ces procédures;
- les politiques concernant la fréquence de sauvegarde des dossiers de renseignements personnels sur la santé (p. ex., quotidienne, hebdomadaire) et l'endroit où les copies de sauvegarde sont stockées en toute sécurité.

Les dépositaires devraient demander conseil à leur fournisseur de services pour obtenir de plus amples renseignements sur les capacités de sauvegarde et de récupération de leur système et les options de sauvegarde hors site disponibles. Votre entente avec le fournisseur de services devrait traiter de la sécurité des copies de sauvegarde et établir des politiques de conservation claires.

Une copie de sauvegarde hors ligne est un bon moyen de protéger votre organisation et les renseignements personnels sur la santé de vos patients contre les effets paralysants d'une cyberattaque. Renseignez-vous à ce sujet et découvrez d'autres points clés tirés de l'affaire marquante du CIPVP Décision 249 en vertu de la LPRPS.

RÉCAPITULATIF! Gouvernance et reddition de comptes : principales mesures à prendre

- **Donnez l'exemple du respect de la vie privée :** favorisez une culture qui incarne les principes fondamentaux de la protection de la vie privée.
- **Attribuez des rôles et des responsabilités clairs :** désignez un responsable de la protection de la vie privée chargé d'élaborer et d'exécuter votre programme de protection de la vie privée.
- **Dressez un inventaire de vos données :** déterminez l'étendue des renseignements dont vous avez la garde ou le contrôle et limitez la collecte à ce dont vous avez besoin.
- **Déterminez s'il faut effectuer une EIVP :** une approche systématique pour évaluer les nouveaux systèmes, programmes ou technologies de gestion de l'information ou les changements qui y sont apportés peut aider à cerner et à atténuer les risques liés à la protection de la vie privée.
- **Choisissez les fournisseurs avec soin :** tenez compte des facteurs liés à la protection de la vie privée et à la sécurité lorsque vous envisagez de travailler avec des fournisseurs de services externes, comme des fournisseurs de DME, et intégrez ces facteurs dans vos ententes contractuelles.
- **Donnez une formation et communiquez :** assurez-vous en permanence que vous et votre personnel possédez les connaissances et les compétences appropriées en matière de protection de la vie privée, et veillez à mettre régulièrement à jour vos documents de formation, au besoin.
- **Obtenez des engagements :** le personnel devrait signer chaque année une entente de confidentialité attestant qu'il comprend et s'engage à respecter les politiques de protection de la vie privée.
- **Expliquez clairement les conséquences :** assurez-vous que le personnel comprend les conséquences de ne pas respecter les politiques, qui peuvent aller d'un apprentissage ou d'une formation d'appoint à d'éventuelles mesures disciplinaires et conséquences judiciaires.
- **Préparez-vous aux catastrophes :** élaborez un plan de reprise après sinistre et préparez la façon dont vous reprendrez vos activités à la suite de perturbations importantes.

3.0 Élaboration et documentation des politiques de protection de la vie privée

Votre programme de gestion de la protection de la vie privée repose sur les engagements et les valeurs qui sous-tendent vos pratiques de gestion des renseignements. Certains de ces engagements et valeurs seront déterminés par les exigences énoncées dans la LPRPS, tandis que d'autres peuvent aller au-delà des exigences légales strictes et refléter une culture axée sur la protection de la vie privée.

3.1 Définissez vos engagements envers la protection de la vie privée

Dans le cadre de votre programme de gestion de la protection de la vie privée, vous devez élaborer des politiques et des procédures écrites qui incarnent ces valeurs et ces engagements.

Politiques ou procédures?

Il est important de connaître la différence entre une politique et une procédure. Il est facile de les confondre, mais elles ont des objectifs et des usages très distincts.

- **Une politique** décrit le quoi et le pourquoi. Son application est générale.
- **Une procédure** décrit la façon dont vous mettez la politique en œuvre.

Les politiques sont destinées à un usage interne et externe, tandis que les procédures sont généralement réservées aux employés.

Dans ce chapitre, nous allons discuter de ce que vous devez inclure dans vos politiques. Dans le chapitre 5, nous discuterons des types de procédures que vous devez mettre en place pour rendre vos politiques opérationnelles.

3.2 Documentez vos politiques de protection de la vie privée

Les politiques constituent l'épine dorsale de tout programme de gestion de la protection de la vie privée. Elles forment un fondement essentiel pour gérer efficacement les renseignements personnels sur la santé et indiquer explicitement, tant à l'interne qu'à l'externe, votre engagement à le faire.

Qu'est-ce qu'une politique?

Une politique est un document écrit qui énonce vos engagements envers la protection de la vie privée et les normes selon lesquelles vous gérez les renseignements. Les politiques se présentent sous diverses formes; elles définissent les règles que doivent suivre toutes les personnes, comme les mandataires et les entrepreneurs, qui interagissent avec des renseignements personnels sur la santé dont votre cabinet a la garde ou le contrôle.

Avez-vous besoin de politiques de protection de la vie privée?

Absolument! Il est judicieux sur le plan juridique et commercial d'adopter des politiques officielles par écrit. Des politiques claires et bien rédigées vous guideront, vous, votre équipe et toute autre personne susceptible de traiter des renseignements personnels sur la santé sous votre direction, afin que chacun sache ce qu'il lui est permis ou interdit de faire de ces renseignements et comment les protéger. Les politiques de protection de la vie privée contribuent également à renforcer la confiance de vos patients et les font se sentir plus en sécurité. Elles témoignent de votre engagement à traiter leurs renseignements personnels sur la santé avec le plus grand soin.

Par où commencer?

Vos politiques doivent être adaptées à la taille et au modèle de gestion de votre cabinet et au type de données que vous recueillez. Certains fournisseurs de soins de santé ont des documents distincts qui comprennent différentes politiques relatives à la protection de la vie privée, tandis que d'autres disposent d'une politique générale sur la protection de la vie privée qui intègre plusieurs politiques dans un seul document.

Si vous exploitez un petit organisme de soins de santé, il pourrait être plus facile de réunir dans un seul document toutes vos politiques relatives à la protection de la vie privée.

Le tableau suivant résume les renseignements de base que vous devez inclure dans votre ou vos politiques de protection de la vie privée. N'oubliez pas que certains éléments ne s'appliquent peut-être pas à tous les praticiens de la santé; votre politique reposera sur la taille et l'envergure de votre cabinet. Vous trouverez en annexe un exemple de modèle à utiliser pour les composantes plus détaillées du programme à inclure dans vos politiques de protection de la vie privée.

Votre politique de protection de la vie privée : que doit-elle couvrir?	
Objet : **Pourquoi avez-vous besoin des renseignements personnels sur la santé du patient?**	• Décrivez votre engagement à respecter la vie privée des patients. • Cet engagement peut inclure votre obligation en tant que dépositaire de vous conformer à la LPRPS et à son règlement d'application. • Expliquez pourquoi vous avez besoin des renseignements personnels sur la santé du patient et ce que vous comptez en faire.
Collecte : **Comment allez-vous recueillir les renseignements?**	• Indiquez tous les modes de collecte de renseignements personnels sur la santé des patients (p. ex., formulaires imprimés, applications numériques, autres fournisseurs de soins de santé). • Décrivez les sources à partir desquelles vous recueillez des renseignements sur les patients (p. ex., laboratoires médicaux, cliniques d'imagerie médicale, pharmacies, autres fournisseurs de soins de santé et, dans certains cas, mandataires spéciaux).
Utilisation : **Comment allez-vous utiliser les renseignements?**	• Indiquez les différentes fins auxquelles vous pouvez utiliser les renseignements. Vous les utiliserez surtout pour fournir des soins de santé. • Toutefois, les renseignements peuvent aussi servir à d'autres fins, comme la gestion des erreurs ou des risques, ou l'amélioration ou le maintien de la qualité des services de soins de santé. Ils peuvent également servir à la facturation, au traitement des demandes et aux paiements relatifs aux soins de santé que vous fournissez à vos patients.
Communication : **Comment allez-vous communiquer les renseignements à autrui, le cas échéant?**	• Décrivez comment et quand vous pouvez communiquer (divulguer) les renseignements, et à qui, si vous remplissez les conditions de la LPRPS. • Par exemple, les destinataires peuvent inclure d'autres fournisseurs de soins de santé ou des spécialistes, pour les besoins de la prestation de soins, le ministère de la Santé à des fins de facturation, des chercheurs externes pour une recherche, ou les responsables de la santé publique pour améliorer la santé au niveau de la population.
Protection : **Comment allez-vous protéger les renseignements?**	• Indiquez comment et où les renseignements seront conservés. • Énumérez les mesures de précaution d'ordre matériel, technique et administratif que vous prendrez pour protéger les renseignements personnels sur la santé. • Précisez pendant combien de temps vous conserverez les renseignements et comment ils seront détruits de façon permanente et sécuritaire lorsqu'ils ne seront plus nécessaires.

Votre politique de protection de la vie privée : que doit-elle couvrir?	
Réponse : **Comment allez-vous répondre aux demandes de renseignements sur la protection de la vie privée des patients, ainsi qu'aux atteintes éventuelles à la vie privée?**	• Décrivez le processus que vous suivrez pour traiter les préoccupations, les plaintes et les demandes relatives à la protection de la vie privée des patients. N'oubliez pas que les patients ont le droit de demander une copie de leur dossier de santé ainsi que la rectification et la mise à jour de leurs renseignements personnels sur la santé. • Indiquez la personne ou le poste à qui les demandes de renseignements ou les plaintes des patients peuvent être adressées, avec leurs coordonnées. • Décrivez comment vous allez gérer un incident ou une atteinte à la vie privée (p. ex., en cas de vol, de perte ou d'utilisation ou de divulgation non autorisées de renseignements personnels sur la santé), y compris en avisant les personnes concernées et, au besoin, le CIPVP. • Précisez clairement le droit d'une personne de porter plainte auprès du CIPVP et indiquez la procédure à suivre pour ce faire.
Consentement : **Quelle forme de permission avez-vous obtenue pour recueillir, utiliser et communiquer des renseignements personnels sur la santé?**	• Précisez les circonstances dans lesquelles votre cabinet s'appuie sur le consentement exprès ou implicite pour la collecte, l'utilisation et la divulgation de renseignements personnels sur la santé. • Par exemple, il faut obtenir le consentement exprès du patient pour divulguer à un dépositaire des renseignements personnels sur la santé à des fins autres que la fourniture de soins de santé ou à une personne qui n'est pas dépositaire. Ces cas de figure pourraient inclure les divulgations à l'avocat ou à l'assureur d'un patient, par exemple. • Le consentement exprès est également requis pour toute collecte, utilisation ou divulgation de renseignements personnels sur la santé à des fins de commercialisation ou d'étude de marché. Toutefois, le règlement pris en application de la LPRPS exclut de la définition de commercialisation les communications entre les patients et les praticiens qui fournissent des services assurés, dans lesquelles ils leur proposent des services accessoires non assurés moyennant le paiement d'honoraires forfaitaires ou le paiement à l'acte.

Votre politique de protection de la vie privée : que doit-elle couvrir?	
Consentement : **Quelle forme de permission avez-vous obtenue pour recueillir, utiliser et communiquer des renseignements personnels sur la santé? (suite)**	• Les dépositaires peuvent se fonder sur le consentement implicite pour recueillir, utiliser et divulguer l'adresse postale d'un patient ou le nom et l'adresse postale d'un mandataire spécial dans le cadre d'activités de financement. Toutefois, toute collecte, utilisation ou divulgation d'autres formes de renseignements (comme un numéro de téléphone ou une adresse courriel) ou d'autres renseignements sur l'état de santé du patient ou la réception de soins de santé pour les besoins d'activités de financement nécessite le consentement exprès du patient. Veuillez noter que le règlement pris en application de la LPRPS prescrit d'autres exigences et restrictions importantes qui s'appliquent à toutes les collectes, utilisations et divulgations de renseignements personnels sur la santé pour les besoins des activités de financement. Veuillez consulter la feuille-info du CIPVP intitulée **Les activités de financement en vertu de la LPRPS** pour en savoir plus. • Dans les autres cas, la plupart des fournisseurs de soins de santé peuvent s'appuyer sur le consentement implicite d'un patient pour recueillir, utiliser ou divulguer leurs renseignements personnels sur la santé en vue de leur fournir des soins de santé ou de les diriger vers d'autres professionnels de la santé pour des examens diagnostiques ou un traitement spécialisé, lorsque certaines conditions sont remplies. Pour en savoir plus sur la communication des renseignements à des fins de soins de santé, consultez les lignes directrices du CIPVP : **Le cercle de soins : Communication de renseignements personnels sur la santé pour la fourniture de soins de santé**. • Les patients ont le droit de refuser leur consentement ou de restreindre l'accès à leur dossier. Sachez que les directives sur le consentement des patients sont assujetties à des exceptions, par exemple lorsque la divulgation vise à éliminer ou à réduire un risque considérable de blessure grave. Pour des précisions, consultez la **feuille-info sur le verrouillage** du CIPVP. • Précisez les circonstances dans lesquelles la collecte, l'utilisation ou la divulgation des renseignements personnels sur la santé d'un patient peuvent être permises ou exigées par la loi sans son consentement, notamment à des fins de facturation, de planification de la santé, d'évaluation ou de recherche, sous réserve des conditions applicables.

Votre politique de protection de la vie privée : que doit-elle couvrir?	
Consentement : **Quelle forme de permission avez-vous obtenue pour recueillir, utiliser et communiquer des renseignements personnels sur la santé? (suite)**	• Expliquez les situations dans lesquelles des patients peuvent faire appel à un mandataire spécial pour prendre des décisions en leur nom, par exemple, les mineurs ou les adultes qui n'ont pas la capacité de donner leur consentement eux-mêmes. Des exigences particulières s'appliquent aux personnes qui peuvent agir à titre de mandataire spécial et dans quelles circonstances. Veuillez consulter le **Guide de la Loi de 2004 sur la protection des renseignements personnels sur la santé** du CIPVP pour obtenir de plus amples renseignements sur la capacité et la prise de décisions au nom d'autrui.
Surveillance : **Comment allez-vous surveiller la conformité à la politique et la faire respecter?**	• Décrivez les mesures que vous prendrez pour veiller à ce que les employés et les autres personnes respectent la politique. • Expliquez comment vous surveillerez la conformité et effectuerez périodiquement des audits de la protection de la vie privée et de la sécurité. • Expliquez clairement les conséquences de la non-conformité. • Mentionnez que la politique sera mise à jour périodiquement pour refléter les changements nécessaires découlant des recommandations issues des évaluations de l'impact sur la vie privée ou des audits de la protection de la vie privée et de la sécurité, des modifications apportées aux exigences légales ou réglementaires ou de l'évolution des pratiques exemplaires.

3.3 Informez les patients et les autres intervenants

Après avoir élaboré et documenté vos politiques internes sur la protection de la vie privée, vous êtes prêt à informer les patients et les autres personnes de vos pratiques relatives aux renseignements. En vertu de la LPRPS, les praticiens sont tenus de mettre à disposition une déclaration publique écrite qui fournit une description générale de la façon dont ils protègent et gèrent les renseignements personnels sur la santé.

Vos politiques de protection de la vie privée internes pourraient être communiquées à l'externe en l'état, ou bien devoir être modifiées pour en faciliter la lecture par des personnes qui ne font pas partie de votre cabinet. Quoi qu'il en soit, vous devez disposer de renseignements écrits facilement accessibles au public qui :

- résument vos pratiques relatives aux renseignements;
- fournissent les coordonnées de la personne-ressource désignée dans votre organisation;
- décrivent comment présenter une demande d'accès aux renseignements personnels sur la santé ou de rectification de ces renseignements;
- expliquent comment déposer une plainte auprès de vous ou du CIPVP en cas de préoccupations au sujet de votre conformité à la LPRPS.

Vous pouvez choisir un nom approprié pour votre déclaration publique écrite, par exemple, avis de confidentialité, protection de la vie privée externe ou énoncé des pratiques relatives aux renseignements. Par souci de simplicité, nous l'appellerons ici avis de confidentialité.

Petits conseils!

Préparation de votre avis de confidentialité : petits conseils pour réussir

Avez-vous déjà lu l'avis de confidentialité d'une application ou d'un site Web avant de cliquer pour en accepter les modalités? Probablement pas. Vous n'êtes pas le seul. Des recherches ont montré que bien des gens ne lisent jamais l'avis de confidentialité avant d'y consentir. Pourquoi? Parce que les avis de confidentialité ont tendance à être trop longs et compliqués, rédigés pour satisfaire aux exigences de conformité aux lois et aux organismes de réglementation au lieu d'être vraiment utiles pour informer les gens.

Voici quelques conseils à suivre pour que votre avis de confidentialité explique bien vos pratiques relatives aux renseignements et que les patients et autres personnes le comprennent :

- **Utilisez un langage clair :** rédigez un avis convivial que les patients n'auront aucune peine à comprendre. Évitez le jargon technique ou juridique.
- **Soyez transparent :** décrivez ouvertement la façon dont vous utilisez ou comptez utiliser les renseignements personnels sur la santé des gens. Ils ont le droit de le savoir. Vous devriez donner un exemplaire de votre avis de confidentialité aux patients la première fois que vous recueillez leurs renseignements personnels.
- **Donnez vos coordonnées :** dites aux gens à qui ils peuvent s'adresser au sein de votre cabinet s'ils ont des questions ou des préoccupations concernant vos pratiques de protection de la vie privée. En vertu de la LPRPS, vous devez également fournir des renseignements sur la façon de communiquer avec le Commissaire à l'information et à la protection de la vie privée de l'Ontario s'ils souhaitent déposer une plainte.
- **Soyez concis :** si l'avis est court et simple, les gens sont plus susceptibles de le lire. Vous n'avez pas besoin de tout dire en détail. Résumez les points essentiels.
- **Adoptez une approche à plusieurs volets :** fournissez les renseignements à petites doses, en rédigeant des paragraphes courts, des titres clairs et des listes à puces, et offrez de fournir de plus amples renseignements sur demande.
- **Soignez la présentation visuelle :** envisagez d'utiliser des graphiques, des images, des icônes et d'autres aides visuelles pour rendre les renseignements plus attrayants et plus faciles à comprendre pour divers publics.
- **Assurez l'accessibilité :** assurez-vous que votre avis de confidentialité est facilement accessible si les gens veulent le lire maintenant ou plus tard. Par exemple, il peut figurer sur une affiche ou dans un dépliant à votre clinique, et comporter un lien ou un code QR qui renvoie les patients vers votre site Web pour plus de détails.

RÉCAPITULATIF! Engagements et politiques : principales mesures à prendre

- Définissez vos engagements envers la protection de la vie privée.
- Rédigez vos politiques internes de protection de la vie privée, qui documentent :
  - les fins de la collecte, de l'utilisation et de la divulgation des renseignements personnels sur la santé;
  - comment vous recueillerez les renseignements;
  - l'utilisation que fait votre cabinet des renseignements personnels sur la santé;
  - comment vous pouvez communiquer les renseignements personnels sur la santé;
  - comment vous protégez en général les renseignements personnels sur la santé;
  - comment vous répondrez aux demandes de renseignements sur la protection de la vie privée des patients, ainsi qu'aux atteintes éventuelles à la vie privée;
  - les exigences relatives au consentement pour la collecte, l'utilisation et la divulgation des renseignements personnels sur la santé;
  - comment vous surveillerez la conformité à la politique et la ferez respecter.
- Créez une déclaration publique externe pour les patients et d'autres intervenants qui :
  - est rédigée en langage clair;
  - est transparente;
  - fournit vos coordonnées;
  - est claire et concise;
  - adopte une approche à plusieurs volets;
  - est visuellement attrayante et utile;
  - est facilement accessible.

4.0 Protection des renseignements personnels sur la santé

La relation entre le patient et son fournisseur de soins de santé est fondée sur la confiance. Le premier fournit au second des détails intimes sur sa santé et son bien-être pour recevoir les meilleurs soins et traitements et s'attend à ce que ses renseignements personnels sur la santé soient protégés.

Si l'on ne répond pas aux attentes des patients en matière de protection de la vie privée et de confidentialité, le lien de confiance avec eux pourrait être rompu. Cela peut avoir de graves répercussions sur eux, les fournisseurs de soins de santé et l'ensemble du secteur de la santé.

Malheureusement, il arrive que des atteintes à la vie privée se produisent. Il peut s'agir, par exemple, de situations où les dépositaires ou leurs mandataires accèdent à des dossiers sans autorisation, ou utilisent ou divulguent des renseignements personnels sur la santé à des fins non autorisées. L'accès, l'utilisation ou la divulgation non autorisés peuvent avoir lieu par négligence ou inadvertance, ou ils peuvent être motivés par l'intention de fouiller dans les dossiers de membres de la famille, de voisins ou de personnalités connues. Parfois, il s'agit d'une simple curiosité ou d'une inquiétude mal placée pour la santé et le bien-être du patient, alors qu'en réalité, il n'est pas vraiment nécessaire de consulter ces renseignements. L'atteinte à la vie privée peut aussi avoir pour but d'embarrasser une personne ou de lui causer du tort, ou d'en tirer un avantage financier.

Dans d'autres circonstances, les atteintes à la vie privée sont le fait d'auteurs de menace externes, comme des cybercriminels, qui accèdent sans autorisation à vos systèmes d'information. Ils pourraient menacer de divulguer les renseignements personnels sur la santé de vos patients sur le Web caché, ou de verrouiller votre système pour paralyser la prestation de vos services à moins que vous ne leur payiez une rançon. Quoi qu'il en soit, une telle cyberattaque peut être dévastatrice pour vous, votre cabinet et la confiance de vos patients.

La LPRPS vous oblige, en tant que dépositaire de renseignements sur la santé, à prendre des mesures raisonnables dans les circonstances pour vous assurer que les renseignements personnels sur la santé dont vous avez la garde ou le contrôle sont protégés contre le vol, la perte et toute utilisation, divulgation, copie, modification ou élimination non autorisées.

Le présent chapitre décrit des mesures de précaution et considérations importantes pour protéger les renseignements personnels sur la santé qui vous sont confiés. Comme les pratiques exemplaires de sécurité de l'information sont en constante évolution, nous vous recommandons de consulter des ressources supplémentaires et de demander l'avis d'un expert lorsque vous élaborez vos politiques et procédures de sécurité.

30

Élaborez de solides contrôles de sécurité

En tant que dépositaire, vous êtes responsable des renseignements personnels sur la santé dont vous avez la garde ou le contrôle et des actions de vos mandataires à l'égard de ces renseignements. Vous devez protéger les renseignements personnels sur la santé sans égard à leur forme (fournis de vive voix, sur papier ou par voie numérique), à leur lieu de conservation (au bureau, à domicile, en ligne, auprès d'un tiers, etc.) et à leur mode de communication (par courriel, messagerie vocale, poste, etc.).

En vertu de la LPRPS, vous devez prendre des mesures de précaution d'ordre technique, matériel et administratif raisonnables pour protéger les renseignements personnels sur la santé contre le vol, la perte et toute utilisation, copie, modification ou élimination non autorisées.

Par conséquent, pour remplir cette obligation, vous devez prendre des mesures raisonnables dans les circonstances afin de protéger les renseignements personnels sur la santé contre les risques pour la vie privée et la sécurité. Il est important d'adopter une approche à plusieurs volets pour détecter, prévenir et réduire ces risques, notamment en prenant les mesures suivantes :

Mesures de précaution d'ordre technique

- utilisez uniquement des comptes de courriel, de messagerie ou de vidéoconférence, des logiciels et du matériel connexe qui sont approuvés par l'organisation;
- utilisez des pare-feu et des mesures de protection contre les menaces logicielles;
- mettez régulièrement à jour les applications logicielles avec les derniers logiciels de sécurité et antivirus;
- chiffrez les données sur tous les dispositifs de stockage mobiles et portables, tant en transit qu'au repos;
- tenez à jour les journaux d'audit, surveillez-les et passez-les en revue;
- utilisez et conservez des mots de passe forts;
- examinez les paramètres et choisissez ceux qui sont les plus stricts pour la protection de la vie privée;
- vérifiez et authentifiez l'identité d'un patient avant de participer à un échange de courriels, à un clavardage ou à une vidéoconférence;
- effectuez des évaluations régulières des menaces et des risques.

Mesures de précaution d'ordre matériel

- conservez toute la technologie contenant des renseignements personnels sur la santé, comme les ordinateurs de bureau, dans un endroit sûr;
- lorsqu'ils sont sans surveillance, gardez les appareils portables contenant des renseignements personnels sur la santé, comme les téléphones intelligents, les tablettes et les ordinateurs portatifs, dans un endroit sûr, comme une pièce, un tiroir ou une armoire fermés à clé;
- limitez l'accès aux bureaux, utilisez des systèmes d'alarme et verrouillez les salles pour protéger le matériel utilisé pour envoyer, recevoir ou stocker des renseignements personnels sur la santé;

- ne prêtez de technologie contenant des renseignements personnels sur la santé à personne sans autorisation;
- assurez-vous qu'il n'y a pas de personnes non autorisées présentes ou à portée de voix ou de vue lorsque vous parlez aux patients;
- isolez les serveurs physiquement et limitez-en l'accès aux seules personnes autorisées.

Mesures de précaution d'ordre administratif

- rappelez aux employés qu'il est interdit de recueillir, d'utiliser ou de divulguer des renseignements personnels sur la santé sans autorisation;
- donnez aux employés une formation suffisante pour utiliser les plateformes sécurisées de courriel, de messagerie et de vidéoconférence, et assurez une formation continue sur la sécurité pour favoriser la détection des tentatives d'hameçonnage;
- adoptez un système fiable de contrôles d'accès et réservez l'accès aux personnes qui en ont besoin;
- veillez à ce que les ententes de confidentialité contiennent des dispositions expresses sur les obligations des employés concernant l'utilisation du courrier électronique, de la messagerie ou de la vidéoconférence sécurisés, et renouvelez-les chaque année.

La protection contre les risques pour la sécurité liés à la vie privée est une obligation permanente. Vous devez prendre des mesures raisonnables pour surveiller de façon proactive les nouvelles menaces à la cybersécurité et y faire face, et adapter continuellement en conséquence vos mesures de précaution d'ordre technique, matériel et administratif.

N'utilisez pas de télécopieurs

Les professionnels de la santé ont fait appel au télécopieur comme moyen de communication pendant longtemps, mais il est dépassé et peu sécuritaire. En fait, une grande partie des atteintes à la vie privée signalées au CIPVP sont le résultat de télécopies mal acheminées, c'est-à-dire envoyées au mauvais numéro ou à la mauvaise personne, ce qui viole la confidentialité des patients.

Le CIPVP préconise depuis longtemps de réduire, voire d'éliminer, l'utilisation des télécopieurs dans le secteur de la santé en Ontario. Dans le cadre de son engagement à « **aider les médecins de famille à faire passer les patients avant la paperasse** », le gouvernement a promis d'« éliminer le télécopieur » en le remplaçant par d'autres dispositifs de communication numérique d'ici 2028 « pour accélérer les diagnostics, les aiguillages et les traitements tout en améliorant la confidentialité des renseignements sur la santé des patients ». Nous vous encourageons fortement, en tant que fournisseurs de soins de santé, à passer à des formes plus sécurisées de communication numérique.

Pour un exemple d'institution qui a subi les conséquences d'un grand nombre de télécopies mal acheminées et qui a mis en place des mesures efficaces pour réduire sa dépendance aux télécopies et atténuer le risque d'atteintes à la vie privée, lisez le rapport du CIPVP sur le Centre de soins de santé St-Joseph de Hamilton.

Mesures de protection supplémentaires pour les applications de courriel et de messagerie sécurisée

Bien que les communications par courriel et autres applications de messagerie numérique comportent de nombreux avantages dans un cabinet moderne, elles présentent également des risques pour la vie privée et la confidentialité des patients. En tant que dépositaire, il est important que vous compreniez ces risques et preniez des mesures raisonnables pour les atténuer avant d'utiliser ces outils à des fins professionnelles. La feuille-info du CIPVP intitulée **La communication de renseignements personnels sur la santé par courriel** décrit plusieurs facteurs dont vous devriez tenir compte pour déterminer si vous devez utiliser ces outils et comment vous acquitter de vos obligations en vertu de la LPRPS.

Si vous décidez d'utiliser le courrier électronique et d'autres applications de messagerie numérique, vous devriez le mentionner dans votre politique de protection de la vie privée. Plus précisément, cette politique devrait préciser quand, comment et à quelles fins des renseignements personnels sur la santé peuvent être envoyés et reçus par l'intermédiaire d'applications de messagerie, ainsi que les modalités ou restrictions qui s'y rattachent. La politique devrait également préciser les types de renseignements dont l'envoi et la réception ne peuvent se faire qu'en utilisant le chiffrement, ainsi que les circonstances dans lesquelles les communications non chiffrées sont acceptables.

L'une des difficultés particulières que pose l'utilisation d'outils numériques pour communiquer directement avec un patient, en particulier lorsque vous ne pouvez pas le voir ou l'entendre, consiste à veiller à ce que l'échange se fasse avec la bonne personne. Il est important de vérifier l'identité du destinataire et d'adresser correctement les messages afin d'éviter toute erreur d'acheminement. Vous pouvez par exemple envoyer un message de test à l'avance et demander un accusé de réception pour vous assurer que le message est parvenu au destinataire visé. Voici d'autres mesures de précaution pour la communication de renseignements personnels sur la santé par courriel :

- fournir dans le courriel un avis indiquant que les renseignements reçus sont confidentiels;
- vérifier (et revérifier!) si les personnes appropriées sont incluses dans les cases « à » et « cc »;
- fournir des instructions à suivre en cas d'erreur de destinataire;
- communiquer par courriel uniquement à partir d'un compte professionnel approuvé;
- confirmer que l'adresse courriel est à jour;
- s'assurer que l'adresse courriel du destinataire correspond à l'adresse souhaitée;
- vérifier régulièrement les adresses courriel préprogrammées pour s'assurer qu'elles sont toujours exactes;
- limiter l'accès au système de courriel et au contenu des courriels aux personnes qui en ont besoin;
- accuser réception des courriels;
- réduire au minimum la divulgation de renseignements personnels sur la santé dans la ligne d'objet et le corps du courriel;

- mettre en place des contrôles d'accès rigoureux aux comptes de courriel;
- recommander aux patients d'utiliser une adresse courriel protégée par mot de passe à laquelle ils sont les seuls à pouvoir accéder.

Chiffrement

Les communications par courriel entre dépositaires qui contiennent des renseignements personnels sur la santé devraient être chiffrées pour éviter tout accès non autorisé. Lorsque vous communiquez avec les patients, vous devriez également utiliser le chiffrement, surtout lorsque vous transmettez des renseignements personnels sur la santé. Vous devez aussi chiffrer les pièces jointes ou les protéger par mot de passe que vous communiquez d'une autre manière (p. ex., si vous envoyez les documents chiffrés par courriel, vous pouvez transmettre le mot de passe par texto). Si le chiffrement est impossible, vous devez déterminer s'il est raisonnable dans les circonstances d'envoyer un courriel non chiffré en tenant compte de tous les facteurs pertinents, y compris le caractère délicat des renseignements, le but de la communication et l'urgence de la situation.

Stockage

De plus, les renseignements personnels sur la santé ne devraient être stockés sur des serveurs de courriel que pendant le temps nécessaire pour servir aux fins visées. Par exemple, si la communication par courriel est consignée dans les dossiers de renseignements personnels sur la santé du patient, il n'est peut-être pas nécessaire d'en conserver une copie sur un serveur de messagerie. De même, vous devez vous assurer que toutes les copies des courriels contenant des renseignements personnels sur la santé se trouvant sur des appareils portatifs sont supprimées en toute sécurité dès qu'elles ont été consignées dans le dossier du patient et qu'elles ne sont plus nécessaires.

Pour connaître les pratiques exemplaires relatives à l'utilisation du courrier électronique et d'autres applications de messagerie numérique, veuillez consulter la feuille-info du CIPVP intitulée **La communication de renseignements personnels sur la santé par courriel**.

Hameçonnage

L'hameçonnage est une attaque en ligne où un pirate, qui utilise des tactiques à la fois technologiques et psychologiques, envoie un message conçu pour inciter le destinataire à révéler des renseignements confidentiels ou à télécharger un logiciel malveillant. Les attaques d'hameçonnage imitent souvent des sources légitimes et fonctionnent en exploitant la confiance, la curiosité, la peur ou le désir d'être utile et efficace. Vous devez donner à vos employés une formation régulière afin qu'ils puissent déceler, éviter et signaler les tentatives d'hameçonnage. Vous devriez également montrer à vos patients comment reconnaître les risques associés à l'hameçonnage pour éviter d'être victimes de logiciels malveillants ou espions ou d'autres formes de piratage psychologique.

Les destinataires qui reçoivent des messages inattendus ou contenant des pièces jointes ou des liens suspects doivent faire preuve de prudence. Par exemple, il faut se méfier des courriels d'hameçonnage envoyés à des heures inhabituelles, contenant des fautes de frappe ou des noms d'utilisateur et de domaine étranges ou qui demandent d'agir immédiatement en raison d'une situation urgente. Demandez à vos employés et à vos patients de vous alerter immédiatement dans

de tels cas, et d'éviter de répondre à ces courriels, de cliquer sur les liens suspects ou d'ouvrir les pièces jointes.

Pour découvrir des pratiques exemplaires et des conseils pratiques, veuillez consulter la feuille-info du CIPVP Se protéger contre l'hameçonnage. Vous pouvez également écouter l'épisode du balado *L'info, ça compte* intitulé Ne vous faites pas prendre! Protégez-vous contre l'hameçonnage.

Mesures de précaution supplémentaires pour les vidéoconférences

Les services de soins de santé virtuels se sont révélés très commodes et utiles pour servir des populations éloignées ou pendant des périodes d'urgence de santé publique, comme la pandémie de COVID-19. Ils soulèvent toutefois des préoccupations particulières en matière de protection de la vie privée et de sécurité, en raison des nouvelles technologies et infrastructures de communication qu'ils utilisent, ainsi que des environnements en ligne dans lesquels ils fonctionnent. Comme pour les autres outils numériques, il est important que les dépositaires comprennent ces risques et prennent des mesures pour les atténuer avant d'adopter des technologies de soins virtuels.

Lorsque vous utilisez des plateformes de vidéoconférence pour prodiguer des soins, il est important de prendre des mesures supplémentaires pour protéger la vie privée des patients :

- Il est préférable que vous et votre patient teniez la vidéoconférence à partir d'un endroit privé en utilisant une connexion Internet sécurisée, par exemple, dans une pièce fermée et insonorisée ou à un endroit par ailleurs calme et privé, avec des couvre-fenêtres au besoin. Utilisez des écouteurs plutôt que le haut-parleur de l'appareil pour éviter que d'autres personnes vous entendent, et faites attention à l'emplacement des écrans.
- Une fois connecté à la vidéoconférence, vous devez vérifier les paramètres pour vous assurer que l'entretien est inaccessible aux participants non autorisés. Si le logiciel ou l'application peut enregistrer l'entretien, vous ne devriez utiliser cette fonction que lorsque c'est nécessaire et si le patient y consent expressément.
- Au début d'une première consultation, il est important de vérifier l'identité du patient. Si vous rencontrez un nouveau patient, vous devez comparer l'image du patient à une photo enregistrée ou demander au patient de présenter sa carte Santé à la caméra pour confirmation.
- N'oubliez pas de vous présenter et de présenter toute autre personne présente du côté du dépositaire, et assurez-vous que le patient consent à la présence d'autres personnes. Vous devez également vérifier si quelqu'un accompagne le patient et confirmer son consentement.
- Il est important que le son et la définition du moniteur soient de qualité suffisante pour être en mesure de recueillir des renseignements (y compris des indications verbales et non verbales) aussi exacts et complets que nécessaire pour fournir les soins de santé.

Pour des précisions sur la gestion des risques liés à la protection de la vie privée et à la sécurité associés aux outils et aux technologies de soins virtuels, veuillez consulter le document d'orientation du CIPVP intitulé Considérations relatives à la protection de la vie privée et à la sécurité dans le contexte des visites de soins de santé virtuelles.

Mesures de précaution supplémentaires pour l'utilisation de l'intelligence artificielle

Dans le secteur de la santé de l'Ontario, on constate dernièrement un recours croissant aux technologies de l'intelligence artificielle (IA), qui visent à aider les fournisseurs de soins de santé à s'acquitter de leurs tâches administratives. Les plus populaires d'entre elles sont les transcripteurs par IA. Selon ses fonctionnalités particulières, un tel transcripteur pourrait transcrire ou de résumer des consultations de santé, verser des renseignements personnels sur la santé dans un DME ou un DSE et produire des notes ou des rapports médicaux. De nombreux transcripteurs par IA évoluent pour offrir des fonctionnalités supplémentaires, comme diriger les patients vers d'autres praticiens, commander des tests médicaux et même recommander des diagnostics et traitements.

Bien que les transcripteurs par IA soient susceptibles d'alléger le fardeau administratif des fournisseurs de soins de santé en Ontario, il est important de tenir compte des difficultés que peuvent présenter les technologies de l'IA. Voici quelques exemples de mesures supplémentaires que vous devriez envisager pour protéger la vie privée des patients lorsque vous achetez, implantez et utilisez des transcripteurs par IA.

- Premièrement, vous devez vous assurer que la loi vous autorise à recueillir, à utiliser et à divulguer des renseignements personnels sur la santé. Dans le contexte des transcripteurs par IA, cela signifie que vous devez faire preuve de la diligence requise pour vous assurer que les données sous-jacentes utilisées pour élaborer et entraîner le modèle du transcripteur ont été obtenues légalement et continuent de l'être.
- De plus, vous devez obtenir le consentement du patient avant d'utiliser un transcripteur, et faire preuve d'une grande transparence à son égard au sujet des objectifs, des risques et des conséquences d'une telle utilisation.
- Vous devez prendre des mesures raisonnables pour veiller à ce que le transcripteur par IA ait été développé et soit maintenu d'une manière qui protège la sécurité et la vie privée. Pour ce faire, vous pouvez notamment effectuer une évaluation de l'impact sur la vie privée (EIVP), une évaluation de la menace et des risques (EMR), s'il y a lieu, ainsi qu'une évaluation propre à l'IA appelée évaluation de l'incidence algorithmique (EIA). Ces évaluations ne sont pas un exercice ponctuel; il faut les mettre régulièrement à jour, surtout avant de déployer toute nouvelle utilisation ou fonctionnalité ajoutée d'un transcripteur.
- Un transcripteur par IA est une technologie d'IA générative qui change au fil du temps à mesure qu'elle apprend en s'appuyant sur de nouvelles données. Vous devez donc vous assurer que le modèle du logiciel est continuellement surveillé et évalué pour en déterminer la validité, la fiabilité et l'exactitude tout au long de son utilisation, afin de toujours assurer la sécurité de vos patients.

- Vous devez disposer de solides garanties contractuelles auprès du fournisseur d'IA pour protéger la vie privée des patients. Pour ce faire, vous devez procéder à un examen minutieux des modalités de service du fournisseur pour vous assurer que ce dernier n'utilise pas les renseignements sur les patients à des fins autres que la prestation du service, et qu'il s'engage à respecter ses obligations en vertu de la LPRPS.

En tant que petit fournisseur de soins de santé, vous n'avez peut-être pas la capacité ou les ressources nécessaires pour faire tout cela vous-même. Vous voudrez peut-être faire appel à des experts externes pour ces aspects.

Pour des précisions, veuillez consulter les lignes directrices du CIPVP intitulées *Acquisition, mise en œuvre et utilisation de transcripteurs par IA : considérations clés pour le secteur de la santé*. Vous voudrez peut-être aussi écouter l'épisode du balado L'info, ça compte du CIPVP, intitulé L'intelligence artificielle dans les soins de santé : mettre en balance l'innovation et la protection de la vie privée.

Journalisation, audit et surveillance

Il est important d'effectuer la journalisation, l'audit et la surveillance de tous les accès aux dossiers électroniques contenant des renseignements personnels sur la santé pour assurer la protection de la vie privée des particuliers et la confidentialité de ces renseignements. La journalisation de tous les cas où des renseignements personnels sur la santé sont recueillis, utilisés et divulgués vous permettra d'auditer et de surveiller les activités de vos mandataires, de répondre à toute plainte reçue et d'enquêter sur les atteintes réelles ou soupçonnées à la vie privée, y compris les cas d'accès non autorisé.

Termes clés

Journalisation : processus qui consiste à consigner des événements dans les systèmes et réseaux informatiques. La journalisation permet de saisir des données provenant de diverses sources et surveille les activités du système et du réseau afin de détecter les accès, utilisations ou divulgations non autorisés et de s'en protéger.

Audit : examen et vérification des journaux, autres dossiers et activités pour examiner la conformité aux politiques et procédures et déterminer si les mesures de la protection de la vie privée et de sécurité sont suffisantes.

Surveillance : observation continue, souvent automatisée, des données recueillies à partir de systèmes et réseaux informatiques afin de repérer les comportements inhabituels et les anomalies qui peuvent révéler des attaques ou des activités non autorisées.

La journalisation, l'audit et la surveillance peuvent également constituer un moyen de dissuasion efficace contre les accès non autorisés si vos mandataires savent que leur accès aux systèmes numériques et leur utilisation seront journalisés, audités et surveillés en permanence ainsi que

de façon ciblée et aléatoire. En général, vous devriez veiller à ce que les systèmes d'information contenant des renseignements personnels sur la santé puissent journaliser tous les cas où ces renseignements sont recueillis, utilisés ou divulgués, ainsi que tous les cas de dérogation à une directive de consentement du patient ou de contournement d'un indicateur d'avertissement de protection de la vie privée. En consultant les journaux, vous devriez être en mesure de déterminer, au minimum :

- le type de renseignements personnels sur la santé qui ont été recueillis, utilisés ou divulgués;
- la personne à qui les renseignements personnels sur la santé se rapportent;
- le mandataire qui a recueilli, utilisé ou divulgué les renseignements personnels sur la santé;
- la date, l'heure et le lieu de collecte, d'utilisation et de divulgation des renseignements personnels sur la santé.
- la durée d'accès à un dossier, idéalement.

Certains outils d'audit peuvent analyser systématiquement et automatiquement les journaux d'accès et générer des rapports en fonction de critères de recherche définis. En automatisant les processus manuels à l'aide de diverses requêtes, ces outils peuvent rehausser l'efficacité des audits et contribuer à prévenir et à déceler l'accès non autorisé aux renseignements personnels sur la santé. Par exemple, ils peuvent repérer les tendances d'accès des mandataires aux systèmes d'information électroniques qui sont typiques de comportements inappropriés ou d'activités irrégulières. En générant automatiquement des alertes ou des rapports, ils peuvent sonner l'alarme, vous avertir de problèmes éventuels et motiver un audit supplémentaire.

Pour des précisions, veuillez consulter le document d'orientation du CIPVP intitulé L'accès non autorisé aux renseignements personnels sur la santé : détection et dissuasion.

RÉCAPITULATIF! Protection des renseignements personnels sur la santé

- **Mettez en œuvre des mesures de précaution raisonnables d'ordre technique, matériel et administratif et passez-les en revue régulièrement** afin de protéger les renseignements personnels sur la santé dont vous avez la garde ou le contrôle.
- **N'utilisez pas le télécopieur**. Les télécopies mal acheminées sont une cause importante d'atteintes à la vie privée.
- **Si vous utilisez le courrier électronique ou d'autres applications de messagerie** pour communiquer avec d'autres fournisseurs et avec vos patients, assurez-vous d'utiliser le chiffrement, d'acheminer les communications en toute sécurité dans le dossier du patient et de supprimer les messages des serveurs ou des appareils portatifs lorsqu'ils ne sont plus nécessaires.
- Montrez vos employés à détecter, éviter et signaler les **attaques d'hameçonnage**, et informez également vos patients des risques liés à ces attaques.
- Suivez des pratiques exemplaires pour protéger la vie privée et la confidentialité lorsque vous utilisez la **vidéoconférence** pour les visites virtuelles.
- Si vous envisagez d'utiliser des **transcripteurs par IA**, examinez attentivement les risques et les préjudices éventuels et cherchez à les atténuer dès le début.
- **Assurez-vous que la journalisation est activée** pour tous les systèmes numériques utilisés pour recueillir, utiliser ou divulguer des renseignements personnels sur la santé.
- **Examinez et auditez régulièrement les journaux du système** pour détecter les accès non autorisés et prendre des mesures rapides afin d'examiner plus en détail toute irrégularité éventuelle.

5.0 Procédures et contrôles : opérationnalisation

Maintenant que vous avez élaboré et documenté vos politiques, il est temps de les mettre en pratique! Pour opérationnaliser vos politiques de protection de la vie privée, vous devez élaborer des procédures et des contrôles qui expliquent comment vous et votre équipe gérerez, utiliserez, communiquerez et protégerez les renseignements que vous recueillez.

N'oubliez pas qu'une procédure est le processus détaillé de mise en œuvre d'une politique. Bien que la création de politiques soit une étape fondamentale de l'établissement de votre cadre de gestion de la protection de la vie privée, vos procédures reflètent les mesures concrètes que vous prendrez pour respecter vos obligations en matière de protection de la vie privée.

Demandez aux employés de confirmer qu'ils comprennent vos politiques de protection de la vie privée et les respecteront

Il ne suffit pas que vos employés lisent en diagonale vos politiques de protection de la vie privée. Il faut qu'ils prennent (et qu'on leur donne) le temps de les examiner attentivement et attester qu'ils les comprennent. Ils doivent connaître vos engagements, règles et attentes en matière de protection des données, ainsi que leurs obligations. Vos employés doivent confirmer par écrit qu'ils ont lu et compris vos politiques de protection de la vie privée et qu'ils les respecteront.

Veillez à ce que les employés suivent régulièrement une formation sur la protection de la vie privée

De même, il ne suffit pas que les employés suivent machinalement la formation annuelle sur la protection de la vie privée. Vous devez être en mesure de confirmer et de documenter qu'ils ont suivi avec succès la formation requise et qu'ils sont en mesure d'opérationnaliser vos politiques dans la pratique. Pour ce faire, vous pouvez leur demander de passer un test ou de répondre à un questionnaire pour confirmer qu'ils ont assimilé et compris les règles qu'ils sont tenus de suivre. En outre, prévoyez un suivi si un mandataire ne suit pas la formation requise, y compris la suspension de l'accès aux renseignements personnels sur la santé au besoin.

Passez régulièrement en revue les contrôles d'accès

Déterminez les membres de votre équipe qui doivent accéder aux renseignements personnels sur la santé des patients et à quelles fins. Ensuite, établissez les fonctions de chacun et les procédures

nécessaires pour accorder des privilèges d'accès à ceux qui en ont besoin. Un accès basé sur les rôles permet de faire en sorte que vos mandataires qui traitent des renseignements personnels sur la santé peuvent accéder uniquement aux renseignements dont ils ont besoin pour s'acquitter de leur rôle, et à rien de plus. Passez régulièrement en revue les contrôles d'accès de vos mandataires afin de vous assurer qu'ils demeurent pertinents et nécessaires, et révoquez immédiatement les privilèges d'accès de toute personne qui quitte l'organisation, que ce soit temporairement ou définitivement.

Établissez de bonnes pratiques de tenue des dossiers

Les bonnes pratiques de gestion de l'information reposent sur une bonne tenue des dossiers. Cela contribue à une gestion plus harmonieuse de votre cabinet, les renseignements que vous tenez seront bien organisés et vous pourrez trouver plus facilement ceux dont vous avez besoin. Une bonne tenue de dossiers montre également que vous prenez au sérieux la gestion des renseignements personnels sur la santé et que vous veillez à respecter la LPRPS.

Assurez-vous de documenter ou de consigner les renseignements que vous pourriez avoir besoin de suivre et de consulter à l'avenir, par exemple :

- les formulaires de consentement des patients;
- les ententes ou contrats avec les fournisseurs de services;
- les ententes de confidentialité des employés;
- les ententes de partage des données avec des tiers;
- les ententes de recherche avec les chercheurs;
- les attestations des employés confirmant qu'ils ont lu et compris la ou les politiques de protection de la vie privée de votre organisation et qu'ils ont suivi la formation requise sur la protection de la vie privée;
- les droits d'accès basés sur les rôles accordés aux mandataires selon leurs besoins;
- les demandes d'accès aux renseignements personnels sur la santé ou de rectification de ces renseignements et l'issue de chaque demande;
- les résultats des évaluations de l'impact sur la vie privée, des évaluations de la menace et des risques et, le cas échéant, des évaluations de l'incidence algorithmique;
- les demandes de renseignements et les plaintes relatives à la protection de la vie privée;
- les rapports sur les atteintes à la vie privée;
- les certificats de destruction.

Créez des procédures de conservation et de destruction des dossiers

Les dépositaires doivent conserver, transférer et éliminer tous les dossiers de renseignements personnels sur la santé dont ils ont la garde ou le contrôle de façon sécuritaire et conformément à la LPRPS. Conserver des renseignements personnels sur la santé plus longtemps que nécessaire augmente le risque d'atteinte à la vie privée.

Voici quelques éléments clés à prendre en compte :

- **Dressez des calendriers de conservation des dossiers :** élaborez des règles relatives à la conservation des dossiers. La LPRPS exige que les dossiers de renseignements personnels sur la santé soient conservés aussi longtemps que nécessaire pour permettre à une personne d'épuiser tous les recours juridiques concernant une demande d'accès. Comme la LPRPS n'établit pas de période de conservation particulière pour les renseignements personnels sur la santé, les dépositaires doivent se référer à leur loi habilitante, à leurs lignes directrices professionnelles et à toute autre loi applicable pour déterminer les exigences en matière de conservation des dossiers.
- **Établissez une justification et des exceptions :** si vous déterminez qu'il est dans l'intérêt supérieur de votre cabinet ou de vos patients de conserver les dossiers de renseignements personnels sur la santé plus longtemps, assurez-vous de documenter ce qui vous autorise à le faire et une justification.
- **Dressez un plan de destruction sécuritaire :** une fois la période de conservation expirée, il est crucial de détruire les dossiers en toute sécurité afin qu'ils ne puissent pas être reconstitués.
- Par exemple, il faut incinérer, pulvériser ou, à tout le moins, déchiqueter les **documents papier** à l'aide d'une déchiqueteuse à coupe transversale. Il ne suffit pas de déchirer les documents à la main et de les jeter dans une poubelle non sécurisée.

Découvrez les leçons pratiques apprises et les principaux points à retenir dans l'affaire marquante du CIPVP intitulée L'élimination sécuritaire des dossiers de santé!

- Quant aux **documents numériques**, il faut les détruire, les supprimer ou les effacer de façon irréversible. Il ne suffit pas de simplement supprimer les fichiers ou de formater les appareils électroniques pour assurer une destruction sécuritaire. Pour détruire en toute sécurité les renseignements personnels sur la santé sous forme numérique, vous devez effectuer certaines opérations sur le support où ils sont stockés. Ainsi, vous pouvez détruire le support en faisant appel à des outils ou services spéciaux pour pulvériser, déchiqueter, incinérer ou démagnétiser les dispositifs, lecteurs ou disques, ou à des outils logiciels spécialisés et propres à l'appareil pour écraser les données stockées en toute sécurité.
- Consultez les feuilles-infos du CIPVP intitulées **La destruction sécurisée de renseignements personnels** et **Comment se débarrasser des supports électroniques** pour en savoir plus.

Mettez en place un protocole d'intervention clair en cas d'atteinte à la vie privée

Malheureusement, les atteintes à la vie privée sont de plus en plus fréquentes, surtout dans le secteur des soins de santé. Les cyberattaques sont en hausse et en sont une cause majeure, mais elles peuvent aussi résulter de certaines actions : courriel mal acheminé, envoi d'un courriel de masse au sujet de votre cabinet sans masquer les adresses des destinataires, ou envoi d'un résultat médical au mauvais patient, par exemple. Il y a une atteinte à la vie privée chaque fois que des

données personnelles dont vous êtes responsable sont perdues, ou accidentellement détruites, endommagées ou communiquées à quelqu'un qui n'aurait pas dû les recevoir.

La gravité des répercussions d'un pareil incident sur la vie privée est variable. En tant que dépositaire, vous devez agir immédiatement quand vous êtes informé d'une atteinte à la vie privée. Vous devez donc élaborer et mettre en œuvre un protocole d'intervention détaillé qui décrit les étapes de gestion de l'atteinte à la vie privée selon son importance et le risque de préjudice. Vous devrez peut-être suivre les étapes ci-après simultanément et rapidement en cas d'atteinte à la vie privée.

Étape 1 : Avisez le personnel et les autres dépositaires

- Informez tout le personnel concerné de l'atteinte à la vie privée, y compris votre responsable de la protection de la vie privée ou la personne-ressource pour la LPRPS.
- Selon la nature ou la gravité de l'atteinte à la vie privée et la taille et la structure de votre organisation, vous devrez peut-être également communiquer avec la haute direction, les représentants des relations avec les patients et le personnel de la technologie et des communications.
- Si l'atteinte à la vie privée concerne des renseignements personnels sur la santé contenus dans un système électronique que se partagent plusieurs dépositaires, assurez-vous de les informer afin qu'ils puissent mener leur propre enquête.

Étape 2 : Déterminez la portée de l'atteinte à la vie privée et prenez les mesures nécessaires pour la maîtriser

- Déterminez la portée de l'atteinte à la vie privée, et notamment les personnes ou les organisations qui pourraient être impliquées ou en être responsables, ainsi que la nature et la quantité des renseignements personnels sur la santé touchés.
- Récupérez et sécurisez les renseignements personnels sur la santé qui ont été divulgués.
- Assurez-vous qu'aucune copie des renseignements personnels sur la santé n'a été faite ou conservée par une personne non autorisée à les recevoir. Il faut obtenir les coordonnées de tout destinataire non autorisé au cas où un suivi serait nécessaire.
- Déterminez si l'atteinte à la vie privée permettrait un accès non autorisé à d'autres renseignements personnels sur la santé (p. ex., si un système d'information électronique utilisé en commun est touché) et prenez les mesures nécessaires, comme changer le mot de passe ou les numéros d'identification ou mettre le système hors service temporairement.
- En cas d'accès non autorisé par un mandataire, envisagez de suspendre ses droits d'accès.

Étape 3 : Avisez les personnes touchées par l'atteinte à la vie privée, le CIPVP ou les ordres professionnels concernés

- Recensez tous les particuliers concernés et informez-les de l'atteinte à la vie privée à la première occasion raisonnable. La LPRPS ne précise pas le mode de notification; toutefois, dans la plupart des cas, vous devez fournir un avis direct par téléphone, par la poste, par courriel ou en personne aux particuliers concernés. Veuillez consulter l'annexe 3 pour des précisions sur le contenu d'un avis d'atteinte à la vie privée.

- Dans certaines circonstances exceptionnelles, le dépositaire peut donner un avis indirect aux particuliers concernés. Si votre organisation envisage de le faire, vous devriez consulter le CIPVP, et expliquer pourquoi vous estimez qu'un avis indirect est raisonnable dans les circonstances, et comment vous comptez le donner. Vous devez notamment présenter le contenu de l'avis que vous proposez et vos stratégies de diffusion.
- Votre organisation peut envisager de donner un avis indirect dans une ou plusieurs des circonstances exceptionnelles suivantes :
    - L'atteinte à la vie privée a touché un grand nombre de personnes qu'il serait difficile d'aviser directement.
    - Il a été établi que le risque de préjudice pour les personnes concernées est faible.
    - Vous n'avez pas pu confirmer l'identité des personnes concernées même après avoir pris des mesures raisonnables pour le faire.
    - La fiabilité ou l'exactitude des coordonnées des personnes concernées est douteuse. Remarque : Toutes les personnes concernées ne devraient pas être avisées indirectement, même si les coordonnées de certaines d'entre elles ne sont plus valables. Lorsque certaines coordonnées sont valables mais que d'autres ne le sont plus, une démarche de notification hybride (directe et indirecte) pourrait être appropriée.
    - La notification directe entraverait abusivement et considérablement les activités de votre organisation. Remarque : Tous les processus de notification en cas d'atteinte à la vie privée nécessitent du temps et des ressources. C'est uniquement lorsque le temps et les ressources requises pour fournir un avis direct entraveraient abusivement et considérablement vos activités qu'il pourrait être justifié de donner un avis indirect.
    - Il serait raisonnable de s'attendre à ce que la notification directe cause un préjudice aux personnes concernées.
- Pour obtenir de plus amples renseignements sur les méthodes de notification indirecte des personnes concernées, voir l'annexe 3.
- En vertu de la LPRPS, le dépositaire doit signaler certaines atteintes à la vie privée au CIPVP dès que possible et coopérer avec le CIPVP. Les circonstances dans lesquelles vous êtes tenu de signaler l'atteinte au CIPVP sont énoncées dans le règlement pris en application de la LPRPS et décrites en détail dans le document du CIPVP intitulé **Le signalement d'une atteinte à la vie privée au commissaire : Lignes directrices pour le secteur de la santé**.
    - Si vous êtes tenu de signaler l'atteinte au CIPVP, faites-le dès que possible en ligne, par courriel ou par la poste.
- Si une atteinte à la vie privée fait intervenir une personne qui est membre d'une profession de la santé réglementée, vous pourriez être tenu de la signaler à son ordre professionnel. Vous devez donner cet avis dans les 30 jours dans l'une ou l'autre des circonstances suivantes :
    - La personne était un employé ou un mandataire du dépositaire et elle a été congédiée ou suspendue ou elle a fait l'objet d'une mesure disciplinaire en raison d'une atteinte à la vie privée.
    - Les privilèges ou l'affiliation de la personne sont révoqués, suspendus ou assortis de restrictions en raison d'une atteinte à la vie privée.

- La personne démissionne et le dépositaire a des motifs de croire que la démission est liée à une enquête ou à une autre mesure qu'il a prise relativement à une prétendue atteinte à la vie privée.
- La personne renonce à ses privilèges ou à son affiliation, ou les restreint volontairement, et le dépositaire a des motifs raisonnables de croire que cette décision est liée à une enquête ou à une autre mesure qu'elle a prise relativement à une prétendue atteinte à la vie privée.

Étape 4 : Enquête et mesures correctives

- Vous devrez mener une enquête interne pour :
  - vous assurer que les mesures immédiates de maîtrise de la situation et de notification ont été prises;
  - passer en revue les circonstances qui ont entouré l'atteinte à la vie privée;
  - déterminer si les politiques et procédures en vigueur sont suffisantes pour protéger les renseignements personnels sur la santé;
- Si vous avez avisé le CIPVP d'une atteinte à la vie privée, vous serez appelé à décrire votre enquête et à collaborer avec lui pour établir les mesures correctives qui s'imposent et vous engager à les prendre. Vous pourriez également être tenu de collaborer à toute enquête du CIPVP sur l'atteinte à la vie privée.
- Les mesures correctives sont d'une importance cruciale pour éviter à l'avenir les circonstances qui ont mené à l'atteinte à la vie privée et éviter ainsi que des incidents semblables se reproduisent. Ce processus commence par l'élimination systématique des conditions ayant mené à l'atteinte à la vie privée; dans certains cas, il pourrait être justifié de réexaminer les procédures à l'échelle du programme.
  - Par exemple, les contrôles administratifs ou les caractéristiques de sécurité d'un système électronique pourraient être insuffisants et devoir être mis à niveau ou améliorés.
  - Déterminez si tous les employés ont reçu une formation appropriée en ce qui concerne la conformité aux dispositions de la LPRPS relatives à la protection de la vie privée.
- La tenue d'un registre des atteintes à la vie privée peut faciliter les enquêtes et aider à cerner les problèmes systémiques qui pourraient nécessiter des mesures correctives. Vous devriez désigner une personne responsable de la tenue de ce registre. Pour chaque atteinte à la vie privée, consignez :
  - le nom de l'employé ou du mandataire qui a causé l'atteinte à la vie privée si vous le jugez pertinent, par exemple dans le cas d'un accès non autorisé;
  - la date de l'atteinte à la vie privée;
  - la nature, la portée et la cause de l'atteinte à la vie privée;
  - le nombre de personnes touchées par l'atteinte à la vie privée;
  - une description des renseignements personnels sur la santé concernés;
  - un résumé des mesures prises en réponse à l'atteinte à la vie privée.

Pour des précisons sur l'élaboration de procédures relatives aux atteintes à la vie privée et les mesures à prendre en cas de pareil incident, veuillez consulter les guides du CIPVP intitulés **Lignes directrices sur les interventions en cas d'atteinte à la vie privée dans le secteur de la santé** et **Le signalement d'une atteinte à la vie privée au commissaire : Lignes directrices pour le secteur de la santé**.

Au cas où une brèche de cybersécurité surviendrait, consultez un cabinet de cybersécurité réputé et des conseillers juridiques chevronnés avant de vous retrouver en situation de crise. Consultez la feuille-info du CIPVP intitulée **Se protéger contre les rançongiciels** pour obtenir d'autres conseils sur ce que doivent comprendre des procédures efficaces de gestion des incidents de cybersécurité.

Soyez prêt à communiquer les statistiques annuelles sur les atteintes à la vie privée au CIPVP

Assurez-vous également de tenir un registre des atteintes à la vie privée qui consigne la date réelle ou estimative des incidents, une description générale des circonstances et le type des renseignements touchés, et qui indique si les atteintes à la vie privée ont été signalées aux personnes concernées et au CIPVP.

En vertu de la LPRPS, les dépositaires doivent déclarer au CIPVP le nombre d'atteintes à la vie privée survenues chaque année. Leur rapport doit inclure toutes les atteintes à la vie privée, y compris celles qui n'ont pas atteint le seuil requis pour être signalées au CIPVP. Une atteinte accidentelle à la vie privée qui est isolée et de portée limitée, par exemple, une correspondance mal acheminée, n'a peut-être pas été signalée au CIPVP lorsqu'elle s'est produite, mais elle doit toujours être comptée dans le rapport statistique annuel.

Pour des précisions sur la présentation des rapports annuels, veuillez consulter la page **Rapport statistique annuel au commissaire sur les atteintes à la vie privée**.

Élaborez des procédures pour répondre aux demandes de renseignements des patients

Demandes d'accès à l'information

En vertu de la loi, les patients ont le droit d'avoir accès aux renseignements personnels sur la santé détenus par les fournisseurs de soins de santé et de les consulter sans frais ou moyennant un montant qui ne dépasse pas les droits de recouvrement des coûts raisonnables. Les patients ont également le droit de demander la rectification de leurs renseignements personnels sur la santé s'ils estiment que les dossiers contiennent des renseignements inexacts ou incomplets. Vous devez donc établir des procédures pour répondre à de telles demandes, sous réserve des exemptions ou des exceptions prévues par la LPRPS. Vos procédures d'accès et de rectification devraient traiter des aspects suivants :

- **La marche à suivre pour accéder aux dossiers.** Par exemple, vous pouvez créer un formulaire de demande normalisé.
- **Les délais de réponse aux demandes.** En vertu de la LPRPS, vous devez répondre le plus tôt possible dans les circonstances, mais au plus tard 30 jours après avoir reçu la demande du patient. Vous pouvez proroger ce délai d'au plus 30 jours dans certaines circonstances, à condition d'en informer par écrit l'auteur de la demande en précisant la durée et les raisons de cette prorogation. Inversement, vous pourriez devoir répondre dans un délai de moins

de 30 jours si l'auteur de la demande vous présente une preuve qu'il a besoin d'accéder d'urgence à ses renseignements personnels sur la santé et si vous pouvez raisonnablement donner la réponse exigée dans ce délai.

- **Les droits exigés pour fournir les copies des dossiers.** En raison des coûts liés à la copie des documents, vous avez le droit d'imposer des droits de recouvrement des coûts raisonnables. Vos procédures devraient décrire clairement comment vous calculez ces droits (voir ci-dessous).
- **Les procédures à suivre pour un caviardage efficace.** Si vous décidez de ne pas divulguer des renseignements qui, selon vous, sont légalement exclus de l'accès ou font l'objet d'une exception en vertu du régime d'accès de la LPRPS, vous devez établir des procédures pour caviarder ou extraire ces renseignements afin que le reste du dossier auquel la personne peut accéder puisse tout de même lui être fourni.

Que sont les droits de recouvrement des coûts raisonnables ?

La LPRPS vous permet d'exiger des droits d'un particulier pour lui accorder l'accès à ses renseignements personnels sur la santé. Comme il n'existe actuellement aucun règlement qui prescrit des droits d'accès, vous pouvez exercer votre pouvoir discrétionnaire pour déterminer le montant à exiger. Toutefois, le CIPVP a le pouvoir d'effectuer un examen pour déterminer si les droits que vous avez exigés dépassent les droits de recouvrement des coûts raisonnables. Le CIPVP a déjà conclu que ce montant ne permet pas nécessairement de recouvrer tous les coûts engagés pour répondre à une demande d'accès[1].

Vous ne devriez pas exiger plus de 30 $ pour les tâches requises afin de répondre à une demande, y compris :

- la réception d'une demande d'accès et toute demande de précisions, si besoin est;
- la fourniture d'une estimation des droits exigibles;
- le repérage et la récupération du dossier;
- l'examen du contenu du dossier par le dépositaire de renseignements sur la santé ou son mandataire, d'une durée maximale de 15 minutes, pour déterminer s'il contient des renseignements personnels sur la santé auxquels l'accès peut être refusé;
- la préparation d'une réponse à l'intention du particulier;
- la préparation du dossier à photocopier, à imprimer ou à transmettre par voie électronique;
- la photocopie du dossier ou son impression, si celui-ci est stocké sur support électronique, jusqu'à concurrence des 20 premières pages, à l'exclusion de l'impression de photographies électroniques;

1 L'**ordonnance HO-009** (en anglais seulement) du CIPVP fournit un raisonnement détaillé des conclusions du CIPVP concernant le recouvrement raisonnable des coûts d'accès.

- le conditionnement de la photocopie ou de la copie imprimée du dossier à expédier ou à envoyer par télécopieur;
- la transmission, par voie électronique, d'une copie du dossier stocké sur support électronique, à la place de l'impression d'une copie du dossier et de son expédition ou de son envoi par télécopieur;
- les frais de télécopie du dossier en Ontario ou les frais de mise à la poste d'une copie du dossier par courrier ordinaire au Canada;
- la surveillance de l'examen de l'original par le particulier, d'une durée maximale de 15 minutes.

En plus des frais maximaux, vous pouvez exiger des frais fixes spécifiques pour certains autres services, comme la photocopie de documents de plus de 20 pages, l'impression de photographies et le coût de la production ou de la préparation de copies d'autres supports, comme les CD ou les clés USB, les cassettes audio ou vidéo, les microfiches, les radiographies, les tomodensitogrammes et les clichés IRM.

Pour obtenir de plus amples renseignements sur ce qui, de l'avis du CIPVP, constitue des droits de recouvrement des coûts raisonnables, veuillez consulter l'**ordonnance HO-009** du CIPVP.

Gestion des rectifications

Les patients peuvent contester l'exactitude ou l'exhaustivité des renseignements contenus dans leurs dossiers. Si la personne est en mesure d'établir, à votre satisfaction, que le dossier est incomplet ou inexact, et qu'elle vous donne les renseignements nécessaires pour vous permettre de rectifier le dossier, vous devez accueillir sa demande de rectification.

Vous devriez établir des procédures de rectification claires conformément aux exigences de la LPRPS. Par exemple, la personne peut vous demander, dans la mesure où il est raisonnablement possible de le faire et sous réserve de certaines exceptions, d'informer de la rectification toute personne à qui les renseignements ont été communiqués; vous devez mettre en place une procédure à suivre si vous n'êtes pas d'accord avec la rectification proposée. Par exemple, en vertu de la LPRPS, la personne peut toujours exiger que vous joigniez une déclaration de désaccord au dossier et que vous fassiez tous les efforts raisonnables pour divulguer la déclaration de désaccord à toute personne qui aurait été avisée si vous aviez accédé à la demande de rectification.

Veuillez consulter le **Guide de la *Loi de 2004 sur la protection des renseignements personnels sur la santé*** du CIPVP pour obtenir des conseils détaillés sur le traitement des demandes de rectification.

Gestion des plaintes et des préoccupations

Les patients peuvent avoir des préoccupations au sujet de vos pratiques relatives aux renseignements. En tant que dépositaire, vous devez établir un processus pour répondre aux préoccupations et aux plaintes. Un processus de gestion des plaintes accessible et efficace est un aspect essentiel de la gestion des risques liés à la vie privée et contribue à promouvoir la reddition de comptes, l'ouverture et la confiance. Il permet également à un cabinet de traiter rapidement les

plaintes, de détecter les problèmes de conformité systémiques ou persistants et de manifester son souci de protéger la vie privée.

Voici quelques étapes à envisager :

1. Consignez la plainte ou la préoccupation, y compris la date à laquelle elle a été présentée.
2. Consignez votre réponse à la plainte et la date de la réponse.
3. Déterminez les échéanciers de suivi et veillez à ce que les mesures appropriées soient prises.
4. Mettez en place un processus d'escalade si la plainte n'est pas facile à résoudre.

Planification de la relève

Parfois, des changements dans la vie personnelle ou professionnelle peuvent se traduire par des changements dans votre cabinet médical, lesquels ne sont pas toujours prévisibles. Cependant, vous devriez prévoir ce qu'il adviendra des dossiers de santé de votre cabinet dans le cas où vous prenez votre retraite, déménagez, déclarez faillite, êtes frappé d'incapacité ou décédez de façon inattendue. La planification de la relève peut vous permettre de protéger vos patients contre une interruption des soins de santé ou une atteinte à leur vie privée en raison de ces changements. Elle peut également protéger vos collègues, partenaires d'affaires ou proches des coûts imprévus liés à la récupération et à la gestion des dossiers que vous aurez abandonnés. N'oubliez pas que vos obligations en tant que dépositaire en vertu de la LPRPS ne prennent fin qu'une fois qu'un successeur autorisé par la loi prend en charge les dossiers de renseignements personnels sur la santé dont vous aviez la garde ou le contrôle.

Suivez les pratiques exemplaires suivantes pour prévenir l'abandon de dossiers :

- Dressez un plan de relève qui identifie clairement un successeur et ses obligations, ainsi que celles des mandataires (comme une entreprise d'entreposage de documents) qui apporteront leur concours pour la conservation, le transfert ou l'élimination des dossiers de santé.
- Assurez-vous que ce plan identifie la personne qui sera responsable de ce qui suit :
  - assurer la sécurité des dossiers;
  - répondre aux demandes d'accès et de rectification des patients;
  - conclure des ententes avec les mandataires (comme une société d'entreposage de dossiers) qui énoncent leurs obligations à l'égard des dossiers;
  - informer les patients du transfert.
- Examinez et mettez à jour le plan régulièrement et lorsqu'un changement se répercuterait sur le transfert des dossiers à un successeur.

Pour découvrir les leçons apprises et les points pratiques à retenir sur ce sujet, consultez l'affaire marquante du CIPVP intitulée Préservation des dossiers médicaux abandonnés.

Pour des précisions à ce sujet, veuillez consulter la publication du CIPVP intitulée **Éviter l'abandon des dossiers médicaux : Conseils pour les dépositaires de renseignements sur la santé en cas de changement de leurs activités**.

RÉCAPITULATIF! Procédures et contrôles : principales mesures à prendre

- **Demandez aux employés de confirmer** qu'ils respecteront les politiques de protection de la vie privée.
- **Assurez-vous que les employés suivent avec succès la formation annuelle sur la protection de la vie privée.**
- **Passez régulièrement les contrôles d'accès en revue** afin de limiter l'accès aux renseignements personnels sur la santé.
- **Établissez de bonnes pratiques de tenue de dossiers** pour faire le suivi des renseignements que vous pourriez avoir besoin de consulter à l'avenir, comme les ententes.
- **Établissez des procédures de conservation et de destruction des dossiers** afin que les dossiers de renseignements personnels sur la santé soient toujours conservés, transférés et éliminés en toute sécurité.
- **Mettez en place un protocole d'intervention en cas d'atteinte à la vie privée** afin que vous puissiez prendre des mesures immédiates en cas d'incident.
- **Tenez un registre des atteintes à la vie privée** aux fins de la déclaration au CIPVP des statistiques annuelles à ce sujet.
- **Élaborez des procédures pour répondre aux patients** qui présentent des demandes d'accès ou de rectification, ou des plaintes ou des demandes de renseignements au sujet de vos pratiques de protection de la vie privée.
- **Établissez un plan de continuité des activités et un plan de relève** pour protéger vos patients contre une interruption de leurs soins de santé ou une atteinte à leur vie privée en raison de changements qui surviennent dans votre vie personnelle ou professionnelle.

ÉLABORATION DE VOTRE PROGRAMME DE PROTECTION DE LA VIE PRIVÉE

6.0 Surveillance et examen : un processus continu

Quand et à quelle fréquence évaluerez-vous votre programme de protection de la vie privée? Comment saurez-vous si vos mandataires et fournisseurs de services respectent vos politiques et procédures? Une surveillance et un examen périodiques sont une étape clé d'un programme fructueux de protection de la vie privée.

Pourquoi la surveillance et l'examen sont-ils importants?

Vous avez déployé beaucoup d'efforts pour mettre en place des politiques, des procédures et des contrôles. Pour respecter vos obligations en matière de protection de la vie privée en vertu de la LPRPS, il est important de vérifier régulièrement s'ils sont toujours efficaces.

La surveillance de votre programme peut vous éviter les surprises, vous informer de nouveaux risques pour la vie privée, vous permettre de respecter la loi et vous aider à rendre des comptes. Voici quelques aspects à envisager :

- Votre programme de protection de la vie privée fonctionne-t-il comme prévu?
- Dans quelle mesure vous et votre équipe et respectez-vous la LPRPS?
- Vos mandataires et fournisseurs de services respectent-ils leurs obligations contractuelles en matière de protection de la vie privée?
- Vos contrôles de sécurité sont-ils à jour?
- Y a-t-il eu des modifications aux lois sur la protection de la vie privée qui revêtent de l'importance pour votre cabinet?

Conseils pour l'élaboration d'un programme de surveillance et d'examen

- Surveillez en permanence vos contrôles de protection de la vie privée et de sécurité. Cela vous permettra, par exemple, de détecter rapidement tout nouveau risque pour la sécurité de vos fonds de données et d'y réagir, par exemple, les personnes qui ne sont pas autorisées à accéder aux renseignements personnels sur la santé. Si vous utilisez des ordinateurs ou des applications en ligne, envisagez d'investir dans des outils ou des services de surveillance de la sécurité.
- Établissez des points de contrôle pour effectuer un examen global de votre programme. Cet examen peut avoir lieu tous les mois, tous les six mois ou une fois par année. Définissez les intervalles qui conviennent le mieux à votre cabinet en fonction des renseignements personnels sur la santé que vous détenez.

- Assurez le suivi des recommandations découlant des évaluations de l'impact sur la vie privée ou des audits de la protection de la vie privée et veillez à leur mise en œuvre au plus tard à leur date d'échéance.
- Vérifiez régulièrement les dates d'expiration ou les exigences de renouvellement des ententes et des attestations et mettez en place un système de notification pour vous rappeler quand il est temps de les renouveler.
- Assurez-vous de révoquer les privilèges d'accès des employés dont l'emploi ou le contrat a pris fin.
- Tenez-vous au courant des développements externes liés à la protection de la vie privée. Les lois peuvent changer. Il en va de même des systèmes électroniques et des logiciels, qui sont fréquemment mis à jour.
- Documentez les résultats de vos activités de surveillance.
- Adaptez vos politiques, procédures et contrôles en fonction des résultats de votre surveillance et de vos évaluations.

RÉCAPITULATIF! Surveillance et examen : principales mesures à prendre

- **Supervision :** examinez régulièrement votre programme de protection de la vie privée (une fois mis en place) pour vous assurer qu'il reste à jour et efficace, et tenez de bons dossiers sur vos activités de surveillance.
- **Surveillance :** Selon votre cabinet, vous devrez peut-être effectuer une surveillance plus soutenue de vos contrôles de protection de la vie privée et de sécurité.
- **Amélioration :** Utilisez les connaissances et les leçons retenues pour renforcer certains éléments de votre programme de protection de la vie privée.

7.0 Annexes

Annexe 1 : Exemple de description de poste (responsable de la protection de la vie privée)

Le responsable de la protection de la vie privée d'une organisation est généralement investi du pouvoir de gérer la plupart ou la totalité des aspects du programme de protection de la vie privée au quotidien. Sa description de poste doit établir le lien hiérarchique entre le poste et la direction et préciser clairement les responsabilités et obligations du titulaire concernant le programme de protection de la vie privée. Dans la plupart des organisations, ces responsabilités et obligations comprendraient les suivantes (sans nécessairement s'y limiter) :

- élaborer, mettre en œuvre, examiner et modifier les politiques, procédures et pratiques de protection de la vie privée;
- assurer la conformité aux politiques, procédures et pratiques de protection de la vie privée mises en œuvre par l'organisation;
- assurer la transparence des politiques, procédures et pratiques de protection de la vie privée;
- faciliter le respect de la LPRPS et de son règlement d'application;
- veiller à ce que les mandataires connaissent la LPRPS et son règlement d'application, ainsi que leur obligation d'assurer la protection de la vie privée et la confidentialité des dossiers de renseignements personnels sur la santé;
- veiller à ce que les mandataires soient dûment informés de leurs fonctions et obligations en ce qui concerne les politiques, procédures et pratiques de protection de la vie privée mises en œuvre par l'organisation;
- veiller à ce que les fournisseurs de services externes respectent leurs obligations contractuelles en matière de protection de la vie privée en évaluant leur conformité aux modalités de l'entente au moins une fois par année;
- diriger ou dispenser la formation initiale et continue sur la protection de la vie privée ou en assurer la prestation, et favoriser une culture de protection de la vie privée;
- effectuer, examiner et approuver les évaluations de l'impact sur la vie privée, au besoin;
- recevoir les demandes de renseignements et les plaintes liées à la protection de la vie privée, les documenter, en faire le suivi, mener une enquête à leur sujet, apporter les corrections nécessaires et y répondre;
- recevoir les demandes d'accès et de rectification, les documenter, en assurer le suivi et y répondre;
- prendre connaissance des atteintes à la vie privée réelles ou soupçonnées, les documenter, en assurer le suivi, mener une enquête à leur sujet et apporter les corrections nécessaires;
- effectuer ou examiner les audits de la protection de la vie privée.

Annexe 2 : Exemple de politique de protection de la vie privée

Chaque politique de protection de la vie privée traite des mêmes éléments communs, mais il faut l'adapter au modèle de soins de votre organisation, notamment les types de renseignements personnels sur la santé que vous recueillez, les modes de collecte et les fins de la collecte, de l'utilisation et de la divulgation de ces renseignements. La politique devrait également témoigner des mesures de précaution générales que vous avez mises en place pour protéger la vie privée des particuliers et la confidentialité des renseignements personnels sur la santé dont vous avez la garde. Vous pouvez vous inspirer des politiques de protection de la vie privée d'organisations semblables à la vôtre.

Énoncé de principes

Commencez par un énoncé qui illustre votre engagement à l'égard des principes de protection de la vie privée, y compris un engagement de faire preuve de transparence quant à la façon dont vous recueillez, utilisez et communiquez les renseignements personnels sur la santé de vos patients.

Définissez l'expression « renseignements personnels sur la santé »

Utilisez un langage clair pour aider les patients et les autres intervenants à comprendre quels types de renseignements sont assujettis à la politique. Par exemple, selon le **Guide de la *Loi de 2004 sur la protection des renseignements personnels sur la santé*** du CIPVP :

Les renseignements personnels sur la santé comprennent les renseignements sous forme verbale ou écrite concernant le particulier si, selon le cas :

- ils ont trait à la santé physique ou mentale du particulier, y compris aux antécédents de sa famille en matière de santé;
- ils ont trait à la fourniture de soins de santé, notamment à l'identification d'une personne comme fournisseur de soins de santé de ce dernier;
- ils constituent un programme de services pour les particuliers ayant besoin de soins de longue durée;
- ils ont trait aux paiements relatifs aux soins de santé ou à l'admissibilité à ces soins;
- ils ont trait au don d'une partie de son corps ou d'une de ses substances corporelles ou découlent de l'analyse ou de l'examen d'une telle partie ou substance;
- ils sont le numéro de la carte Santé du particulier;
- ils permettent d'identifier le mandataire spécial d'un particulier.

Tout autre renseignement sur un particulier qui est compris dans un dossier contenant des renseignements personnels sur la santé est également visé par cette définition.

Décrivez votre organisation

Expliquez la structure de votre organisation, y compris les noms commerciaux concernés et une liste des membres du personnel professionnel et de soutien qui peuvent prodiguer des soins aux patients ou remplir des fonctions administratives connexes. Soyez transparent quant à tout recours à un fournisseur de services externe qui pourrait avoir accès à des renseignements personnels sur la santé dans le cadre de ses fonctions et expliquez comment cette relation est gérée.

Décrivez les fins de la collecte, de l'utilisation et de la divulgation des renseignements personnels sur la santé

Expliquez clairement les différentes fins auxquelles vous recueillez, utilisez et divulguez des renseignements personnels sur la santé. Les organismes de soins de santé recueillent généralement des renseignements personnels sur la santé dans le but premier d'offrir des soins de santé. Vous pouvez faire savoir aux patients que vous recueillez des renseignements sur leur santé et les antécédents médicaux de leur famille, leur état de santé actuel et tout déterminant social de la santé afin d'évaluer leurs besoins en santé, de poser des diagnostics, de suggérer des options, puis de fournir des traitements ou d'autres soins. Vous pouvez également recueillir des renseignements en vue de déterminer l'état de santé actuel de votre patient comme référence pour les consultations futures, afin de faire le suivi de sa santé au fil du temps.

La plupart des organismes de soins de santé recueillent, utilisent et divulguent également des renseignements personnels sur la santé à d'autres fins valables qui peuvent être liées aux fins principales, mais qui ne sont pas directement liées à la prestation de soins. Vous devez préciser que vous demanderez le consentement exprès du patient pour toute fin pour laquelle la LPRPS exige un tel consentement. Voici des exemples courants de fins connexes :

- **Paiements :** vous devrez peut-être recueillir, utiliser ou divulguer des renseignements pour coordonner les paiements de votre patient ou d'assureurs publics ou privés.
- **Santé publique :** certains professionnels de la santé sont tenus par la loi de communiquer à leur médecin hygiéniste local des renseignements importants sur le plan de la santé publique.
- **Amélioration de la qualité et gestion des risques :** vous devrez peut-être recueillir, utiliser ou divulguer des renseignements à des fins de gestion des risques ou des erreurs ou pour l'exercice d'activités visant à améliorer ou à maintenir la qualité des soins ou celle des programmes ou services connexes du dépositaire.
- **Commercialisation :** avec le consentement exprès de vos clients, vous pouvez utiliser leurs renseignements pour les informer des services que vous fournissez ou pour leur annoncer un événement spécial.
- **Conformité :** en tant que fournisseur de soins de santé, vous pourriez être tenu par la loi d'autoriser votre ordre professionnel ou d'autres organismes de réglementation à inspecter vos dossiers. Vous pourriez également être tenu de communiquer des renseignements à des organismes gouvernementaux ou de signaler divers problèmes liés à une faute professionnelle ou à des infractions à la loi.
- **Financement :** les activités de financement peuvent être autorisées avec le consentement exprès ou implicite, conformément à la LPRPS et à son règlement d'application (voir l'**article 32 de la LPRPS** et l'**article 10 du Règlement de l'Ontario 329/04** pris en application de la LPRPS).

Consentement

Expliquez clairement les circonstances dans lesquelles vous vous appuierez sur :

- **un consentement implicite.** Dans de nombreux milieux de soins de santé, le patient donne implicitement son consentement à la collecte ou à l'utilisation de ses renseignements personnels sur la santé par sa présence et son consentement à l'évaluation, au diagnostic

ou au traitement. Les fournisseurs de soins de santé recueillent, utilisent et divulguent souvent des renseignements personnels sur la santé pour consulter d'autres fournisseurs en se fondant sur le consentement implicite aux fins de la fourniture de soins de santé au particulier ou d'une aide à cet égard.

- **un consentement exprès.** Expliquez que, dans certaines circonstances, vous devez obtenir le consentement exprès pour communiquer des renseignements, par exemple, à des personnes qui ne sont pas dépositaires, ou encore à des dépositaires mais à des fins autres que la fourniture de soins de santé, notamment à des fins de commercialisation ou de divulgation à des membres de la famille ou à des amis, ou à une compagnie d'assurance.

Les patients devraient savoir qu'ils peuvent choisir de ne pas donner leur consentement, et qu'ils peuvent retirer leur consentement à tout moment, mais que ce retrait n'aura pas d'effet rétroactif. Vous devriez leur expliquer comment demander le verrouillage d'une partie ou de la totalité de leurs dossiers.

- **Situations dans lesquelles le consentement n'est pas requis :** les patients devraient savoir que, dans certaines circonstances, la collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé sans leur consentement peuvent être permises ou exigées par la loi. Par exemple, sous réserve des exigences et restrictions, le cas échéant, que prescrit la LPRPS, le consentement n'est pas nécessaire pour divulguer des renseignements au ministre de la Santé ou à un autre dépositaire de financement pour qu'il puisse établir ou fournir un financement ou des paiements pour la prestation de soins de santé.

Décrivez vos mesures générales de protection des renseignements personnels sur la santé

Exprimez votre engagement à prendre les mesures nécessaires pour protéger les renseignements personnels sur la santé et expliquez de façon générale les principaux contrôles d'ordre technique, matériel et administratif que vous avez mis en place, notamment :

- veiller à ce que les documents papier et numériques soient sécurisés dans des zones verrouillées ou restreintes lorsqu'ils ne sont pas utilisés;
- utiliser des mots de passe forts et des contrôles d'accès basés sur les rôles pour les systèmes numériques;
- veiller à ce que les appareils mobiles soient verrouillés de façon appropriée;
- utiliser le chiffrement pour protéger les renseignements personnels sur la santé qui sont stockés ou transmis par voie numérique;
- donner une formation aux membres du personnel afin qu'ils limitent leur accès aux renseignements personnels sur la santé et leur utilisation et qu'ils respectent la politique sur la protection de la vie privée;
- veiller à ce que tous les entrepreneurs et fournisseurs de services externes signent des ententes exigeant le respect des politiques de protection de la vie privée.

Décrivez votre politique de conservation

Expliquez clairement combien de temps les documents des patients sont conservés au dossier

et pour quelle raison (p. ex., pour vous permettre de répondre à des questions ou à des préoccupations au sujet de ces documents et pour respecter toute exigence légale).

Vous devez également décrire les méthodes employées pour éliminer les renseignements personnels sur la santé après la période de conservation. Par exemple, vous pouvez utiliser une déchiqueteuse à coupe transversale pour détruire les fichiers papier et rendre les fichiers numériques irrécupérables en les écrasant avec des données aléatoires ou en démagnétisant ou détruisant les disques durs.

Informez les patients de leur droit d'avoir accès à leur dossier et d'en demander la rectification

La politique devrait informer les patients de leur droit d'accéder à leurs dossiers de renseignements personnels sur la santé dont vous avez la garde ou le contrôle (sous réserve de quelques exceptions) et expliquer comment en faire la demande. Précisez qu'il leur faudra confirmer leur identité et présenter leur demande par écrit, et que vous les aiderez à trouver les dossiers pertinents et à en comprendre le contenu (p. ex., en expliquant les acronymes ou en simplifiant le langage technique). Précisez également comment vous déterminerez les droits de recouvrement des coûts raisonnables exigés pour accorder l'accès.

De même, informez les patients de leur droit de demander une rectification lorsque le dossier est inexact ou incomplet (mais précisez qu'ils ne peuvent pas demander la rectification de vos opinions professionnelles faites de bonne foi). Expliquez clairement comment documenter une telle demande, les preuves qui sont requises et comment vous déterminerez si une rectification est appropriée. Si vous êtes d'avis qu'il n'est pas nécessaire d'apporter la rectification, informez les patients que leur point de vue peut être documenté dans leur dossier. Indiquez également que les patients peuvent demander qu'un avis soit donné à toute personne qui a reçu les renseignements, sauf s'il n'y a pas raisonnablement lieu de s'attendre à ce que la rectification puisse avoir des répercussions sur la fourniture continue de soins de santé ou d'autres avantages aux patients.

Décrivez vos procédures de gestion des atteintes à la vie privée

Décrivez les mesures qui seraient prises en cas de perte, de vol ou d'accès non autorisé à des renseignements personnels sur la santé dont vous avez la garde. Ces mesures comprendraient généralement les suivantes, entre autres :

- informer les personnes concernées, fournir vos coordonnées pour toute question, et donner à ces personnes les coordonnées du CIPVP en indiquant qu'elles ont le droit de porter plainte en vertu de la LPRPS;
- prévenir tout autre accès non autorisé en modifiant les mots de passe, en limitant l'accès, en déconnectant les réseaux ou en mettant les systèmes hors service;
- prendre des mesures pour récupérer les copies de renseignements personnels sur la santé qui auraient pu être divulguées ou s'assurer qu'aucune copie n'a été faite;
- mener une enquête;
- prendre des mesures correctives pour prévenir de futures atteintes à la vie privée (p. ex., modifier les politiques, prendre des mesures de précaution supplémentaires);
- informer le CIPVP et collaborer avec lui au besoin;
- signaler les mesures disciplinaires prises aux ordres professionnels.

Coordonnées à fournir en cas de question ou de préoccupation

Fournissez les coordonnées de votre responsable de la protection de la vie privée et faites savoir aux patients qu'il est à leur disposition pour répondre à leurs questions ou préoccupations, ou pour recevoir toute plainte officielle concernant vos pratiques en matière de protection de la vie privée. Expliquez votre procédure de réception et de traitement des plaintes, y compris le droit des patients de porter **plainte** au :

Commissaire à l'information et à la protection de la vie privée de l'Ontario
2, rue Bloor Est, bureau 1400
Toronto (Ontario) M4W 1A8
Téléphone : 416 327-8533
Interurbain : 1 800 387-0073
www.ipc.on.ca/fr

Annexe 3 : Avis d'atteinte à la vie privée à l'intention des personnes concernées

Contenu d'un avis d'atteinte à la vie privée à l'intention des personnes concernées

- L'avis d'atteinte à la vie privée devrait :
  - contenir des détails sur l'atteinte à la vie privée pour les personnes concernées, y compris sa portée et les renseignements personnels sur la santé en cause;
  - faire savoir aux personnes concernées les mesures que vous prenez pour rectifier la situation et le fait qu'elles ont le droit de porter plainte au CIPVP, et préciser que vous avez signalé l'incident à ce dernier, le cas échéant;
  - fournir les coordonnées d'une personne-ressource de votre organisation qui peut fournir des renseignements supplémentaires et de l'aide et répondre aux questions.
- Si des renseignements financiers sont en cause, vous pouvez inclure les énoncés suivants dans l'avis :
  - Par précaution, nous vous recommandons fortement d'informer de cette atteinte à la vie privée les banques, sociétés émettrices de cartes de crédit et services gouvernementaux avec qui vous traitez. Vous devriez vérifier vos états de comptes bancaires, de cartes de crédit et d'autres opérations financières pour déceler toute activité louche. Si vous soupçonnez une utilisation abusive de renseignements personnels qui vous concernent, vous pouvez obtenir une copie de votre dossier de crédit auprès d'une agence d'évaluation du crédit pour vérifier si les opérations contenues dans votre dossier sont légitimes.
  - Equifax, 1 800 465-7166 ou **www.equifax.ca/fr**
  - TransUnion, 1 800 663-9980 ou **www.transunion.ca/fr**
  - Si vous croyez avoir été victime de fraude, vous pouvez demander à ces agences d'annexer une « alerte à la fraude » à votre dossier, qui demande aux prêteurs de communiquer avec vous avant d'ouvrir un nouveau compte.

Le tableau ci-dessous donne quelques suggestions sur ce qu'il faut inclure dans un avis d'atteinte à la vie privée.

Renseignements à inclure	Commentaires supplémentaires
Date à laquelle l'atteinte à la vie privée a été portée à votre attention	
Date à laquelle ou période au cours de laquelle l'atteinte à la vie privée s'est produite	
Description de l'atteinte à la vie privée	*Description générale de la nature et de l'étendue de l'atteinte à la vie privée, y compris les préjudices éventuels*

Renseignements à inclure	Commentaires supplémentaires
Nom de la personne responsable de l'accès non autorisé (le cas échéant)	
Description des renseignements personnels ou des renseignements personnels sur la santé visés par l'atteinte à la vie privée	*Description des renseignements consultés, recueillis, utilisés ou divulgués de manière inappropriée*
Description des mesures qui ont été ou seront prises pour réduire le risque de préjudice aux personnes concernées	
Description des mesures prises pour maîtriser l'atteinte à la vie privée et prévenir de futurs incidents	
Mesures que les personnes concernées peuvent prendre	*Renseignements sur la façon dont les gens peuvent se protéger, par exemple en communiquant avec ServiceOntario pour signaler un numéro de carte Santé perdu ou volé, ou avec des agences d'évaluation du crédit pour mettre en place une alerte à la fraude*
Coordonnées du CIPVP	*Si vous avez déjà communiqué avec le CIPVP, mentionnez-le dans la lettre d'avis*
Coordonnées pour obtenir de l'aide	*Coordonnées d'une personne-ressource de votre organisation qui peut fournir des renseignements supplémentaires et de l'aide et répondre aux questions*

Diffusion d'un avis indirect aux personnes concernées

Si vous avez établi, après avoir évalué les circonstances particulières d'une atteinte à la vie privée et consulté le CIPVP, qu'il est raisonnable de donner un avis indirect, vous devez diffuser cet avis de façon à ce qu'il soit raisonnable de s'attendre à ce que les personnes concernées puissent en prendre connaissance.

Il importe de bien réfléchir à la stratégie qui serait la plus efficace pour rejoindre les personnes concernées. Il est généralement préférable et plus efficace de recourir à plusieurs méthodes.

Ainsi, une stratégie de notification du public pourrait comprendre une partie ou la totalité des méthodes suivantes afin de porter l'avis à l'attention des personnes concernées :

- Un avis publié de façon bien visible dans le site Web de votre organisation ou un site Web spécialisé contenant des renseignements sur l'atteinte à la vie privée.

  - Si vous publiez l'avis dans le site Web de votre organisation, veillez à ce que cet avis ou un lien l'y menant figure à un endroit bien visible de la page d'accueil, et qu'il ne soit pas nécessaire de défiler ou d'effectuer une recherche pour le localiser.
  - Si vous publiez l'avis dans un site Web spécialisé, vous devriez afficher un lien vers ce site sur la page d'accueil du site Web de votre organisation, afin qu'il soit clairement visible et que les visiteurs puissent cliquer dessus pour se rendre au site Web sur l'atteinte à la vie privée.
  - L'avis numérique doit demeurer en ligne pendant une période raisonnable, afin de permettre aux personnes concernées de le lire.
- Prenez des mesures raisonnables pour porter l'avis numérique à l'attention des personnes concernées. Celles-ci seront peu susceptibles de visiter votre site Web ou de lire l'avis d'atteinte à la vie privée à moins d'être invitées à le faire par des annonces dans les médias, des publications dans les médias sociaux ou d'autres moyens.

Organisez d'autres activités d'information du public afin de porter l'avis à l'attention des personnes concernées :

- Installez des avis ou des affiches dans les secteurs fréquentés de votre établissement pendant une certaine période, afin que les personnes concernées puissent les lire.
- Publiez des avis dans des journaux nationaux ou locaux.
- Faites paraître des publications dans les médias sociaux pertinents.
- Faites diffuser des annonces et messages publicitaires à la radio ou à la télévision à l'intention des personnes concernées.
- Publiez des communiqués de presse et des avis communautaires destinés aux personnes concernées.
- Tenez des séances d'information ou des webinaires afin de renseigner la population.
- Recourez à d'autres stratégies de communication publique qui pourraient être efficaces afin de joindre les personnes concernées par l'atteinte à la vie privée.

Annexe 4 : Ressources du CIPVP

Vidéo : La série *Info CIPVP* est une série de brèves vidéos captivantes sur divers sujets liés à la protection de la vie privée dans le domaine de la santé, accessibles sur la chaîne **YouTube** du CIPVP.

- **Le partage de données sur la santé**
- **Guide sur les pénalités administratives pécuniaires**
- **La LPRPS**

Balados : *L'info, ça compte* est un balado sur les gens, la protection de la vie privée et l'accès à l'information animé par Patricia Kosseim, commissaire à l'information et à la protection de la vie privée de l'Ontario, qui porte sur des questions concernant l'accès à l'information et la protection de la vie privée. Les épisodes suivants peuvent présenter un intérêt particulier pour le secteur de la santé :

- **1re saison – épisode 10 : Du chevet au conseil d'administration – Instaurer une culture de la vie privée et de la sécurité dans les établissements de santé**
- **1re saison – épisode 5 : La confiance des patients au cœur de la santé virtuelle**
- **3e saison – épisode 5 : Concevoir des systèmes de santé numériques en collaboration avec les patients et les familles**
- **4e saison – épisode 4 : L'intelligence artificielle dans les soins de santé : mettre en balance l'innovation et la protection de la vie privée**
- **4e saison – épisode 10 : La protection de la vie privée dans le secteur de la santé : principaux enseignements de 2024**

Affaires marquantes : Brefs comptes rendus d'affaires et de décisions marquantes du CIPVP.

- **Décision 249 en vertu de la LPRPS**
- **Décision 243 en vertu de la LPRPS**
- **Réponse à une cyberattaque : l'obligation d'aviser les particuliers en vertu de la LPRPS et de la LSEJF**
- **L'élimination sécuritaire des dossiers de santé**
- **Préservation des dossiers médicaux abandonnés**
- **Prévention des atteintes à la vie privée dans le secteur de la santé : l'importance de la formation, des politiques et des ententes de confidentialité**

Feuilles-info :

- **La communication de renseignements personnels sur la santé par courriel**
- **Un plan de relève peut contribuer à prévenir l'abandon de dossiers**
- **Se protéger contre les rançongiciels**
- **Se protéger contre l'hameçonnage**
- **Comment se débarrasser des supports électroniques**

- **Le chiffrement fort dans les soins de santé**
- **Le verrouillage**
- **Le télétravail pendant la pandémie de COVID-19**
- **Les activités de financement en vertu de la LPRPS**

Documents d'orientation :

- **Guide de la Loi de 2004 sur la protection des renseignements personnels sur la santé**
- **Le cercle de soins : Communication de renseignements personnels sur la santé pour la fourniture de soins de santé**
- **L'accès non autorisé aux renseignements personnels sur la santé : détection et dissuasion**
- **Considérations relatives à la protection de la vie privée et à la sécurité dans le contexte des visites de soins de santé virtuelles**
- **Foire aux questions : *Loi de 2004 sur la protection des renseignements personnels sur la santé*** (en anglais seulement)
- **Utilisation et divulgation de renseignements personnels sur la santé à des fins générales de santé publique**
- **Les soins de santé numériques sous le régime de la LPRPS : Aperçu sélectif**
- **Lignes directrices sur les interventions en cas d'atteinte à la vie privée dans le secteur de la santé**
- **Le signalement d'une atteinte à la vie privée au commissaire : Lignes directrices pour le secteur de la santé**
- **Rapport statistique pour le Commissaire à l'information et à la protection de la vie privée de l'Ontario sur les atteintes à la vie privée concernant des renseignements personnels sur la santé – Cahier de préparation et guide**
- **La protection de la vie privée et les appareils mobiles**
- **Éviter l'abandon des dossiers médicaux : Conseils pour les dépositaires de renseignements sur la santé en cas de changement de leurs activités**
- **Lignes directrices sur la dépersonnalisation des données structurées** (en anglais seulement)
- **Planifier pour réussir : Guide d'évaluation de l'incidence sur la vie privée**
- **Lignes directrices concernant l'évaluation de l'incidence sur la vie privée sous le régime de la Loi sur la protection des renseignements personnels sur la santé**
- Acquisition, mise en œuvre et utilisation de transcripteurs par IA : considérations clés pour le secteur de la santé

Guide de gestion de la protection de la vie privée à l'intention des petits organismes de soins de santé

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

2, rue Bloor Est, bureau 1400
Toronto (Ontario)
Canada M4W 1A8

www.ipc.on.ca/fr
416-326-3333
info@ipc.on.ca

Mai 2025