FÉVRIER 2021

Considérations relatives à la protection de la vie privée et à la sécurité dans le contexte des visites de soins de santé virtuelles

LIGNES DIRECTRICES POUR LE SECTEUR DE LA SANTÉ

Les soins de santé virtuels font désormais partie intégrante du système de santé de l'Ontario. Ils peuvent être fournis par l'entremise d'un service de messagerie sécurisée et lors de consultations par téléphone ou par vidéoconférence. Ces formes de communication numériques sont très pratiques pour les dépositaires de renseignements sur la santé (les « dépositaires ») et pour leurs patients, lorsqu'il est difficile de maintenir la distanciation physique. Cependant, les soins de santé virtuels suscitent des préoccupations particulières en matière de protection de la vie privée et de sécurité, car ils nécessitent des technologies, des infrastructures de communication et des environnements distants. Ils présentent de nouveaux risques en matière de cybersécurité que l'on ne retrouve pas au même degré dans le monde analogique.

La *LPRPS* s'applique aussi bien aux soins virtuels qu'aux soins en présentiel

La *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario (*LPRPS*) s'applique aussi bien aux soins virtuels qu'aux soins en présentiel. Les dépositaires doivent se conformer aux dispositions de *LPRPS* de même qu'aux autres lois et règlements applicables, ainsi qu'aux directives des ordres professionnels pertinents.

Dans le présent guide, nous rappelons certaines des principales exigences de la *LPRPS* qui s'appliquent à tous les dépositaires, y compris ceux qui évoluent dans un contexte de soins de santé virtuels. Nous présentons ensuite quelques mesures pratiques que les dépositaires devraient prendre pour protéger les renseignements

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

personnels sur la santé, en particulier lorsqu'ils planifient et fournissent des soins de santé virtuels.

PRINCIPALES EXIGENCES DE LA *LPRPS*

Les principales exigences suivantes de la *LPRPS* s'appliquent à tous les dépositaires, qu'ils fournissent des soins de santé en présentiel ou virtuels :

Minimisation des données

- Le dépositaire ne doit pas recueillir, utiliser ou divulguer de renseignements personnels sur la santé à une fin que d'autres renseignements permettent de réaliser.
- Le dépositaire ne doit pas recueillir, utiliser ou divulguer plus de renseignements personnels sur la santé qu'il n'est raisonnablement nécessaire pour réaliser la fin visée.

Mesures de précaution

- Le dépositaire prend des mesures qui sont raisonnables dans les circonstances pour veiller à ce que les renseignements personnels sur la santé soient protégés contre le vol, la perte et une utilisation ou une divulgation non autorisée et à ce que les dossiers qui les contiennent soient protégés contre une duplication, une modification ou une élimination non autorisée.
- Le dépositaire veille à ce que les dossiers de renseignements personnels sur la santé soient conservés, transférés et éliminés de manière sécuritaire.

Le dépositaire veille à ce que les dossiers soient conservés, transférés et éliminés de manière sécuritaire.

Fournisseurs de services électroniques

Si le dépositaire fait appel à un fournisseur de services électroniques, il est assujetti, ainsi que le fournisseur, à des exigences supplémentaires, selon que le fournisseur est ou non un *mandataire* du dépositaire.

Si le fournisseur est un *mandataire* du dépositaire, il agit pour lui ou en son nom avec son autorisation, à ses fins à lui et non aux siennes.

S'il recourt à un *mandataire*, le dépositaire :

- demeure responsable des renseignements personnels sur la santé que son mandataire recueille, utilise, divulgue, conserve ou élimine;
- prend des mesures raisonnables pour éviter que son mandataire ne recueille, n'utilise, ne divulgue, ne conserve ou n'élimine des renseignements personnels sur la santé, sauf si la collecte, l'utilisation, la divulgation, la conservation ou l'élimination de ces renseignements, selon le cas :

  1. est autorisée par le dépositaire;

Si le fournisseur est un mandataire du dépositaire, il agit pour lui ou en son nom avec son autorisation, à ses fins à lui et non aux siennes.

2. est nécessaire aux fins de l'exercice de ses fonctions à titre de mandataire;
3. n'est pas incompatible avec la *LPRPS* ou une autre règle de droit;
4. est conforme à toute condition ou restriction qu'impose le dépositaire.

Pour sa part, le fournisseur de services électroniques, en tant que *mandataire* du dépositaire, doit :

- respecter les quatre conditions précédentes;
- aviser le dépositaire à la première occasion raisonnable en cas d'atteinte à la vie privée.

Si le fournisseur de services ***n'est pas*** le mandataire du dépositaire, d'autres restrictions s'appliquent. Sauf si la loi l'exige, le fournisseur de services électroniques ***ne doit pas :***

- utiliser de renseignements personnels sur la santé auxquels il a accès lorsqu'il fournit des services pour le dépositaire, sauf dans la mesure nécessaire à la fourniture de ces services;
- divulguer de renseignements personnels sur la santé auxquels il a accès lorsqu'il fournit des services pour le dépositaire;
- permettre à ses employés ou à quiconque agit en son nom d'avoir accès aux renseignements, sauf s'ils conviennent de satisfaire aux restrictions applicables au fournisseur de services électroniques.

Fournisseurs de réseaux d'information sur la santé

La prestation de soins de santé nécessite souvent des communications entre plusieurs dépositaires. Un fournisseur de réseau d'information sur la santé est un fournisseur de services électroniques qui fournit de tels services à deux dépositaires ou plus, principalement dans le but de leur permettre de communiquer. Le fournisseur de réseau d'information sur la santé est assujetti à des obligations supplémentaires en vertu de la *LPRPS*, notamment :

Le fournisseur de réseau d'information sur la santé est assujetti à des obligations supplémentaires en vertu de la *LPRPS*.

- tenir un dossier électronique de tous les cas d'accès à des renseignements personnels sur la santé ou de transfert de ces renseignements et le mettre à la disposition des dépositaires sur demande;
- aviser les dépositaires de tout incident où il y a eu accès non autorisé à des renseignements;
- remettre aux dépositaires une description claire des services qu'il fournit et des mesures de précaution qu'il a mises en place;
- publier cette description ainsi que ses directives, lignes directrices et politiques pertinentes;
- évaluer l'incidence sur la vie privée, les menaces et les risques, et fournir aux dépositaires une copie des résultats obtenus;

- veiller à ce que les tiers qu'il engage pour l'aider à fournir des services aux dépositaires conviennent de respecter les restrictions et conditions auxquelles il est lui-même assujetti;
- conclure avec chaque dépositaire un accord écrit sur les services à fournir et sur les mesures de précaution qui existent afin d'assurer le caractère confidentiel et la protection des renseignements personnels sur la santé, et obligeant le fournisseur de réseau à se conformer à la *LPRPS.*

MESURES VISANT À AMÉLIORER LA PROTECTION DE LA VIE PRIVÉE ET LA SÉCURITÉ DANS LES SOINS DE SANTÉ VIRTUELS

Le dépositaire devrait aussi élaborer et mettre en œuvre une politique sur les soins de santé virtuels

Préparatifs

Le dépositaire devrait commencer par déterminer les dispositions législatives, les règles professionnelles et les autres lignes directrices réglementaires qui s'appliquent à lui, et s'assurer de les comprendre. Il devrait consulter les ordres des professions de la santé réglementées concernés et se renseigner sur leurs politiques et sur toute autre loi applicable, en plus de la *LPRPS*, qui est susceptible de lui imposer des obligations supplémentaires en ce qui concerne les soins de santé virtuels.

Le dépositaire devrait effectuer des **évaluations de l'incidence sur la vie privée** afin de relever et de gérer les risques précis pour la vie privée et la sécurité des renseignements qui sont associés à la prestation de soins de santé virtuels. Pour en savoir davantage, consulter les ***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 de l'Ontario*** du CIPVP.

Le dépositaire devrait aussi élaborer et mettre en śuvre une **politique sur les soins de santé virtuels**. Cette politique devrait porter sur les circonstances où des soins de santé pourront être fournis de façon virtuelle, à quelles fins et selon quelle méthode, les conditions ou restrictions applicables et les mesures de précaution d'ordre administratif, technique et matériel qui seront en place. Cette politique devrait prévoir expressément que les employés et mandataires auront accès uniquement au minimum de renseignements personnels sur la santé nécessaire pour exercer leurs fonctions. Le dépositaire doit informer ses patients de cette politique.

Il est essentiel de fournir une **formation complète sur la protection de la vie privée et la sécurité** afin de réduire le risque de collecte, d'utilisation et de divulgation non autorisées de renseignements personnels sur la santé. Le dépositaire devrait s'assurer que ses employés et mandataires suivent une formation continue sur ces sujets, de même que sur les politiques de leur organisation concernant les soins de santé virtuels et les circonstances particulières associées à ces soins.

Le dépositaire devrait également fournir des directives et une orientation à ses employés et mandataires en télétravail afin de réduire les risques de ce dernier pour la vie privée et la sécurité. Pour en savoir davantage, consultez la feuille-info du CIPVP intitulée ***Le télétravail pendant la pandémie de COVID-19***[1]**.**

Le dépositaire doit établir un **cadre solide de gestion de la sécurité de l'information** afin de surveiller régulièrement, d'évaluer et d'atténuer tout risque pour la sécurité qui pourrait découler de l'utilisation de la plateforme virtuelle. Ce cadre doit prévoir toutes les mesures de précaution d'ordre administratif, technique et matériel requises de la part des employés, des mandataires et des fournisseurs de services électroniques. Il faut notamment mettre en ŝuvre et tenir à jour les contrôles d'accès, tenir des registres des accès, se renseigner régulièrement sur la disponibilité de mises à jour logicielles et effectuer ces mises à jour, et faire régulièrement des vérifications et des évaluations des menaces et des risques.

Le CIPVP s'attend à ce que le dépositaire instaure un **protocole de gestion des atteintes à la vie privée** énonçant les exigences relatives à l'identification et au signalement des atteintes à la vie privée confirmées ou soupçonnées, ainsi qu'à la maîtrise de la situation, à la notification, aux enquêtes et aux mesures correctives. L'obligation de signaler les atteintes à la vie privée à la première occasion raisonnable aux personnes concernées et, dans certaines situations, au CIPVP, continue de s'appliquer dans un contexte virtuel. Pour savoir quoi faire en cas d'atteinte à la vie privée, consultez les documents ***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 du CIPVP***.

Le CIPVP s'attend à ce que le dépositaire instaure un protocole de gestion des atteintes à la vie privée.

L'obligation de signaler les atteintes à la vie privée continue de s'appliquer dans un contexte virtuel.

Sélection du fournisseur

Pour aider les dépositaires à choisir des solutions de soins virtuels, Santé Ontario a élaboré une **norme relative aux solutions** de soins virtuels. Cette norme provinciale a été élaborée afin d'aider les dépositaires et les fournisseurs à fournir des soins de santé virtuels de façon sécuritaire en utilisant des « plateformes sűres, sécuritaires et interopérables »2. Cette norme établit les exigences obligatoires à respecter pour qu'un produit ou un service soit désigné comme étant une solution vérifiée par Santé Ontario. Une liste des solutions vérifiées sera publiée **en ligne** pour aider les dépositaires à faire leur choix.

Le dépositaire devrait vérifier comment les solutions qu'il envisage pour les soins de santé virtuels peuvent être intégrées dans son infrastructure

1 Cette feuille-info s'applique aux organisations du secteur privé et du gouvernement; cependant, bon nombre des recommandations et pratiques exemplaires qu'elle contient s'appliquent aussi aux dépositaires. En cas d'incompatibilité entre la feuille-info et les exigences de la *LPRPS*, le dépositaire doit observer la *LPRPS*.

2 Il incombe toujours au dépositaire de se conformer aux exigences de la LPRPS dans le cadre de l'utilisation d'une solution de soins virtuels provenant d'un fournisseur qui souscrit à la norme relative aux solutions de soins virtuels de Santé Ontario.

globale de gestion de l'information. Il doit s'assurer que les solutions qu'il utilise sont conformes aux spécifications d'interopérabilité de Santé Ontario.

Le dépositaire qui fait appel à un fournisseur de services de l'extérieur pour assurer la prestation de soins virtuels doit s'assurer que ce fournisseur s'engage par contrat à se conformer aux mesures de protection de la vie privée et de sécurité prises en application des exigences de la *LPRPS.* Entre autres engagements, le fournisseur de services doit accepter :

- d'informer immédiatement le dépositaire en cas d'atteinte à la vie privée;
- de subir des vérifications périodiques de la sécurité à la demande du dépositaire;
- de s'assurer que ses employés ou toute personne agissant en son nom peuvent accéder aux renseignements personnels sur la santé uniquement si cela est nécessaire;
- de rendre ou de détruire les renseignements à la fin de l'entente.

Le dépositaire ne devrait pas faire appel à un fournisseur qui exige que les particuliers s'inscrivent auprès de lui ou acceptent des conditions d'utilisation et des politiques de confidentialité qui comportent la collecte, l'utilisation ou la divulgation de renseignements personnels ou de renseignements personnels sur la santé à des fins autres que la fourniture de soins de santé de la part du dépositaire.

Le dépositaire doit également tenir compte des risques et avantages d'une visite virtuelle plutôt qu'en présentiel.

Préparation aux visites virtuelles

Avant de planifier une visite virtuelle, le dépositaire doit déterminer si une telle visite est effectivement appropriée, en tenant compte des besoins du patient, des exigences informatiques et techniques, de l'objet de la visite et des dispositions réglementaires pertinentes.

Le dépositaire doit également tenir compte des risques et avantages d'une visite virtuelle plutôt qu'en présentiel, notamment des facteurs pratiques touchant la mobilité du patient et l'accessibilité, ainsi que sa propre capacité de respecter son obligation de protéger la vie privée et la sécurité des renseignements personnels sur la santé dans un contexte virtuel.

Obtention du consentement du patient

En utilisant un langage simple, le dépositaire devrait informer ses patients des limites et risques des visites de santé virtuelles, notamment du risque d'atteinte à la vie privée découlant d'une interception illicite d'ordre matériel ou électronique, du piratage, de failles logicielles, de défectuosités techniques et d'erreurs de paramétrage.

Le dépositaire doit obtenir le consentement du patient pour recueillir, utiliser et divulguer des renseignements personnels sur la santé par l'entremise de technologies et de services de soins virtuels. Il devrait

documenter la discussion sur les limites et risques des visites de santé virtuelles, y compris le risque d'atteintes à la vie privée, et le consentement obtenu. Il devrait aussi informer le patient de son droit de retirer son consentement en tout temps.

Mesures de précaution efficaces

Le dépositaire doit instaurer des mesures de précaution d'ordre technique, matériel et administratif afin de protéger les renseignements personnels sur la santé. Il est essentiel de bien planifier pour assurer la confidentialité et la sécurité des visites virtuelles.

Le dépositaire devrait éviter d'utiliser une adresse de courriel personnelle, un service de messagerie texte non chiffré ou des plateformes de vidéoconférence gratuites basées sur l'infonuagique pour communiquer avec les patients. Ces plateformes présentent des risques sérieux pour la vie privée. Le dépositaire devrait mettre en place des mesures de précaution afin de protéger les renseignements personnels sur la santé au moyen de systèmes sécurisés de courriel, de messagerie ou de conférence que son organisation a vérifiés et dont elle a approuvé l'utilisation. Voici des exemples de telles mesures :

Mesures de précaution d'ordre technique

- Utiliser uniquement des comptes, des logiciels et du matériel approuvés par l'organisation pour le courriel, la messagerie et la vidéoconférence.
- Utiliser des coupe-feu et des mesures de protection contre les vulnérabilités logicielles.
- Mettre à jour régulièrement les logiciels de sécurité et les logiciels antivirus.
- Chiffrer les données sur tous les appareils de stockage mobiles et portables, qu'ils soient en transit ou non[3].
- Tenir, surveiller et passer en revue des registres électroniques des accès.
- Utiliser des mots de passe forts.
- Examiner les paramètres par défaut et les régler à la confidentialité la plus stricte.
- Vérifier et confirmer l'identité du patient avant de communiquer avec lui par courriel, clavardage ou vidéoconférence.

Utiliser uniquement des comptes, des logiciels et du matériel approuvés par l'organisation pour le courriel, la messagerie et la vidéoconférence.

3 Le CIPVP ne considère pas la perte ou le vol d'un appareil électronique contenant des renseignements personnels sur la santé chiffrés comme étant une atteinte à la vie privée (terme qui s'applique aux failles de sécurité faisant intervenir des renseignements personnels sur la santé) lorsque le risque d'accès non autorisé à des renseignements non chiffrés est manifestement faible. Cependant, que les renseignements soient chiffrés ou non, le dépositaire devrait exiger que ses employés et mandataires signalent toute perte et tout vol. Il pourra ainsi déterminer au cas par cas si les renseignements étaient adéquatement protégés.

Mesures de précaution d'ordre matériel

- Conserver tous les appareils contenant des renseignements personnels sur la santé, notamment les ordinateurs de bureau et serveurs, dans un endroit sécurisé.
- Conserver les appareils portables contenant des renseignements personnels sur la santé, comme les téléphones intelligents, tablettes et ordinateurs portables, dans un endroit sécurisé, comme une armoire ou un tiroir verrouillé, lorsqu'ils sont sans surveillance.
- Limiter l'accès aux locaux, utiliser des systèmes d'alarme et verrouiller les pièces où se trouve du matériel utilisé pour envoyer, recevoir ou stocker des renseignements personnels sur la santé.
- Ne prêter à personne des appareils contenant de renseignements personnels sur la santé sans autorisation.
- Veiller à ce qu'aucune personne non autorisée ne se trouve dans les locaux ou ne soit en mesure d'entendre ou de voir des renseignements personnels sur la santé.
- Séparer physiquement les serveurs et en limiter l'accès aux seules personnes autorisées.

Conserver tous les appareils contenant des renseignements personnels sur la santé, notamment les ordinateurs de bureau et serveurs, dans un endroit sécurisé.

Mesures de précaution d'ordre administratif

- S'assurer que les employés et mandataires reçoivent une formation suffisante pour utiliser les systèmes de courriel et de messagerie et les plateformes de vidéoconférence sécurisés.
- Instaurer un système rigoureux de contrôles d'accès, et s'assurer régulièrement que l'accès est réservé aux personnes qui ont besoin des renseignements.
- Veiller à ce que les employés et autres mandataires soient conscients de leur obligation de toujours éviter de recueillir, d'utiliser ou de divulguer plus de renseignements personnels sur la santé que nécessaire.
- Veiller à ce que les ententes de confidentialité comportent des dispositions décrivant explicitement les obligations des employés et des autres mandataires qui utilisent des systèmes sécurisés de courriel, de messagerie ou de vidéoconférence pour fournir des soins de santé virtuels.

S'assurer que les employés et mandataires reçoivent une formation suffisante pour utiliser les systèmes de courriel et de messagerie et les plateformes de vidéoconférence sécurisés.

Il faut toujours se prémunir contre les risques pour la vie privée et la sécurité dans le contexte des soins virtuels. Le dépositaire devrait toujours surveiller les menaces à la cybersécurité et les contrer, notamment par les moyens suivants :

- mettre à jour régulièrement les logiciels;
- fournir une formation continue en matière de sécurité aux employés et aux autres mandataires pour assurer la détection des tentatives d'hameçonnage;

- effectuer régulièrement des évaluations des menaces et des risques.

Considérations particulières sur l'utilisation du courrier électronique ou de la messagerie sécurisée

Les paragraphes qui suivent portent sur la communication de renseignements personnels sur la santé par courriel. Des règles semblables devraient s'appliquer à leur communication par messagerie sécurisée.

La communication par courriel entre dépositaire et patient comporte une difficulté particulière, celle de s'assurer que cette communication se fait avec la bonne personne, *surtout lorsqu'il est impossible de voir ou d'entendre le patient*. Le dépositaire devrait vérifier l'identité du destinataire et veiller à bien adresser les courriels ou messages pour éviter qu'ils ne parviennent à quelqu'un d'autre. Par exemple, envoyer un message test à l'avance et demander un accusé de réception pour confirmer que le message est parvenu au bon destinataire.

Voici d'autres mesures de précaution à prendre pour communiquer des renseignements personnels sur la santé par courriel :

- indiquer dans le courriel un avis selon lequel les renseignements qu'il contient sont confidentiels;
- fournir des directives à suivre si un courriel a été envoyé par erreur à un mauvais destinataire;
- utiliser un compte de courriel professionnel et non personnel, car les comptes personnels pourraient être moins sécuritaires et plus vulnérables au piratage;
- confirmer que l'adresse de courriel est toujours valable;
- s'assurer que l'adresse de courriel du destinataire est bien la bonne;
- vérifier régulièrement les adresses de courriel mémorisées pour s'assurer qu'elles sont toujours valables;
- limiter l'accès au système de courriel et aux courriels eux-mêmes;
- informer les patients de tout changement d'adresse de courriel;
- accuser réception des courriels;
- éviter dans toute la mesure du possible d'inclure des renseignements personnels sur la santé sur la ligne objet et dans le corps du message;
- instaurer des contrôles d'accès stricts aux comptes de courriel utilisés par le dépositaire;
- recommander aux patients d'utiliser un compte de courriel protégé par mot de passe auquel personne d'autre ne peut avoir accès.

Le dépositaire devrait aussi se conformer aux mesures de précaution prévues dans les autres politiques et procédures, le cas échéant, y compris celles concernant l'utilisation d'appareils personnels au travail.

Les patients devraient être inscrits dans un système de messagerie sécurisé qui confirme leur identité avant qu'ils ne puissent accéder à leurs messages.

Le dépositaire devrait chiffrer les courriels à destination et en provenance de patients s'ils contiennent des renseignements personnels sur la santé. Il devrait aussi chiffrer les pièces jointes ou les protéger par mot de passe, et communiquer le mot de passe séparément par un autre moyen ou dans un autre message. S'il n'est pas possible de recourir au chiffrement, le dépositaire doit déterminer s'il est raisonnable dans les circonstances d'utiliser des courriels non chiffrés en tenant compte de tous les facteurs pertinents, dont le caractère délicat des renseignements, l'objet du message et l'urgence de la situation (voir la ***Feuille-info : La communication de renseignements personnels sur la santé par courriel*** du CIPVP). Le dépositaire doit aussi utiliser le chiffrement lorsqu'il envoie des renseignements personnels sur la santé par courriel à un autre dépositaire.

Le dépositaire devrait chiffrer les courriels à destination et en provenance de patients s'ils contiennent des renseignements personnels sur la santé.

Le dépositaire doit rappeler à ses employés, à ses autres mandataires et à ses patients les risques associés à l'hameçonnage pour éviter qu'ils ne soient la cible de logiciels malveillants ou espions ou d'autres attaques d'ingénierie sociale. L'hameçonnage est une attaque en ligne lors de laquelle l'attaquant, en recourant à des tactiques 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 semblent souvent provenir de sources légitimes, et exploitent la confiance, la curiosité ou la peur des gens, ou encore leur volonté de se rendre utiles et leur souci d'efficacité. Il faut faire preuve de prudence lorsqu'on reçoit un message inattendu ou qui contient des pièces jointes ou des hyperliens douteux.

Le dépositaire devrait conserver des renseignements personnels sur la santé dans des serveurs de courriel uniquement pendant la période nécessaire pour les fins visées. Par exemple, si les renseignements ont été versés dans le dossier du patient, il pourrait être inutile d'en conserver des copies dans un serveur de courriel. De même, le dépositaire doit s'assurer que toutes les copies de courriels contenant des renseignements personnels sur la santé qui se trouvent dans des appareils portables sont supprimées de façon sécurisée lorsqu'elles ne sont plus nécessaires et que les renseignements en question ont été versés dans le dossier du patient.

Pour en savoir davantage sur les pratiques exemplaires, consulter les feuilles-info ***La communication de renseignements personnels sur la santé par courriel*** et **Protect against Phishing** du CIPVP.

Considérations particulières sur les vidéoconférences

Le dépositaire qui recourt à des plateformes de vidéoconférence pour fournir des soins devrait prévoir des mesures supplémentaires pour préparer son patient à sa visite virtuelle. Par exemple, il pourrait demander si le patient a besoin de sous-titres ou d'un lecteur d'écran par souci d'accessibilité, et passer en revue ce que le patient peut faire pour protéger sa vie privée.

Il est préférable que le dépositaire et le patient participent chacun à la vidéoconférence dans un endroit privé, en utilisant une connexion Internet sécurisée. Ils peuvent, par exemple, s'installer dans une pièce fermée et insonorisée, ou dans un endroit calme et privé muni de rideaux au besoin. Il y a lieu également d'utiliser un casque d'écoute au lieu du haut-parleur pour éviter que d'autres personnes n'entendent, et de placer l'écran de façon judicieuse.

Il est préférable que le dépositaire et le patient participent chacun à la vidéoconférence dans un endroit privé, en utilisant une connexion Internet sécurisée.

Une fois en ligne pour la vidéoconférence, le dépositaire devrait en vérifier les paramètres pour s'assurer qu'elle sera inaccessible aux participants non autorisés. Si le logiciel ou l'application peut enregistrer la rencontre, cette fonction doit être utilisée uniquement si elle est nécessaire et si le patient a donné son consentement exprès.

Au début de la première visite, le dépositaire devrait vérifier l'identité du patient. S'il s'agit d'un nouveau patient, il devrait comparer l'image à une photo qu'il a dans ses dossiers, ou demander au patient de mettre sa carte Santé devant la caméra pour confirmer son identité.

Le dépositaire devrait se présenter, et présenter toute personne qui l'accompagne, et s'assurer que le patient consent à la présence de ces autres personnes, s'il y a lieu. Le dépositaire devrait aussi demander si une personne accompagne le patient, et confirmer que ce dernier consent à sa présence.

Pendant la vidéoconférence, le dépositaire doit s'assurer que le son est d'assez bonne qualité et que l'image est d'une définition suffisante pour lui permettre de recueillir des renseignements (y compris des indications verbales et non verbales) qui sont aussi exacts et complets que nécessaire pour fournir des soins de santé.

Après la visite virtuelle

Le dépositaire devrait documenter ses interactions virtuelles avec ses patients dans leur dossier, comme il le ferait après ses interactions en présentiel. Les mêmes exigences quant à la conservation des dossiers s'appliquent aux interactions virtuelles, et les patients conservent le droit d'accéder à ces dossiers et d'en demander la rectification.

Le dépositaire pourrait envisager de solliciter les commentaires de ses patients, pour s'assurer que les plateformes numériques leur semblent sécuritaires et qu'ils n'hésitent pas à faire part de renseignements en raison des risques pour leur vie privée et la sécurité de ces renseignements.

Le dépositaire pourrait envisager de solliciter les commentaires de ses patients, pour s'assurer que les plateformes numériques leur semblent sécuritaires.

Au sujet des portails pour patients

Le dépositaire peut choisir une solution de soins virtuels qui est intégrée dans son système électronique de tenue de dossiers médicaux, comme un portail pour patients. Selon le type de plateforme ou ses fonctionnalités, les patients pourraient être en mesure de consulter leurs résultats de tests et leurs dossiers, gérer leurs rendez-vous et communiquer avec le dépositaire par l'entremise de ce portail.

Le dépositaire devrait indiquer à ses patients les types de renseignements qui sont accessibles par l'entremise du portail, qui peut y accéder et combien de temps ils resteront accessibles, et préciser tout aspect relatif à la protection de la vie privée et à la sécurité.

Étant donné le degré variable de culture de la santé chez les patients, le dépositaire devrait envisager comment les aider à comprendre les renseignements accessibles par l'entremise du portail. Si ce dernier permet au patient de fournir des renseignements, par exemple, sa pression artérielle, son degré de douleur ou des données d'ordre social ou comportemental, le dépositaire doit lui faire savoir s'il examinera ces renseignements et dans quelles circonstances il les passera en revue.

Le dépositaire doit obtenir le consentement du patient pour recueillir, utiliser et divulguer des renseignements personnels sur la santé par l'entremise du portail. Il doit aussi prévoir des contrôles d'accès appropriés pour les mandataires spéciaux au besoin. Si le patient souhaite déléguer à une autre personne son accès au portail ou encore transférer ou exporter certains des renseignements qui s'y trouvent à d'autres fins, notamment pour les communiquer à un employeur ou à une compagnie d'assurances, le dépositaire devrait discuter avec lui de ce que cela comporte et de la façon de le faire qui protégera le mieux possible sa vie privée.

Le dépositaire devrait mettre en place des mesures de précaution appropriées pour l'accès au portail. Il pourrait notamment élaborer une procédure que le patient devra suivre la première fois qu'il accédera au portail, et prévoir le mécanisme d'identification et d'authentification qui sera suivi la prochaine fois que le patient ouvrira une session.

Le dépositaire devrait donner des directives claires aux patients sur le paramétrage du portail, afin d'assurer la sécurité et la confidentialité, et sur l'utilisation de ce portail. Il devrait notamment encourager les patients à utiliser des mots de passe forts, et expliquer les risques associés au partage de mots de passe ou de captures d'écran. Le dépositaire devrait renseigner ses patients sur l'importance d'accéder au portail dans un endroit discret et privé, et de bien fermer la session ensuite. Il serait souhaitable pour le dépositaire de prévoir un paramètre par défaut qui déconnecte automatiquement l'utilisateur après une période d'inactivité précise.

Le dépositaire doit obtenir le consentement du patient pour recueillir, utiliser et divulguer des renseignements personnels sur la santé par l'entremise du portail.

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