



L'ASSOCIATION
CANADIENNE
DE PROTECTION
MÉDICALE

THE CANADIAN
MEDICAL
PROTECTIVE
ASSOCIATION



Guide sur les dossiers électroniques

La mise en place et l'utilisation des dossiers médicaux
électroniques (DME) et des dossiers de santé électroniques (DSE)

Table des matières



| | |
|--|----|
| Points importants à prendre en considération | 1 |
| Introduction | 2 |
| Choisir un système approprié | 3 |
| La réglementation des dossiers électroniques | 5 |
| Le consentement des patients et les droits d'accès | 6 |
| Les questions de sécurité et de protection des renseignements personnels | 8 |
| Le maintien de l'intégrité des données | 9 |
| L'envoi ou le transfert de dossiers | 14 |
| La destruction et l'élimination de dossiers | 15 |
| Le partage de données et les ententes entre médecins | 16 |
| Les nouveaux enjeux | 19 |
| Conclusion | 20 |
| Annexe A – Glossaire | 21 |
| Annexe B – Ressources complémentaires | 23 |
| Annexe C – Ententes sur le partage de données | 26 |

AVIS D'EXONÉRATION DE RESPONSABILITÉ/MODALITÉS D'UTILISATION

Le matériel didactique fourni ne sert qu'à des fins éducatives générales et ne constitue d'aucune façon des conseils professionnels, médicaux ou juridiques ni une « norme de diligence » professionnelle ou légale à l'intention des professionnels de la santé au Canada. Des divergences dans l'exercice de la médecine existent et peuvent s'avérer appropriées. Les suggestions présentées ne doivent pas être interprétées comme des règles à suivre en matière de prestation de soins aux patients et de communication avec les patients. L'emploi du matériel didactique de l'ACPM est assujéti aux dispositions susmentionnées ainsi qu'à l'avis d'exonération complet de l'ACPM disponible sur le site Web de l'Association à l'adresse www.cmpa-acpm.ca.

© Tous droits réservés ACPM 2009

This document is also available in English.

Ce document est aussi disponible sur le site Web de l'Association au www.cmpa-acpm.ca

Points importants à prendre en considération

- Le choix d'un système approprié dépend des besoins de la pratique du médecin ainsi que de toutes les exigences légales et réglementaires. Lorsque vient le moment de choisir ou de mettre en place un système de DME, il peut s'avérer avantageux d'obtenir les conseils d'un fournisseur de service qualifié ou d'un utilisateur expérimenté et prudent. Dans certains cas, l'hôpital, l'agence/régie régionale de la santé ou le gouvernement provincial ou territorial peut exiger l'utilisation d'un système précis de DSE. Consulter la page 3, Choisir un système approprié
- L'ACPM encourage les membres à passer en revue son document *Ententes sur le partage de données – Principes applicables aux dossiers médicaux électroniques/dossiers de santé électroniques* pour obtenir des détails sur la manière de conclure une entente concernant un DME partagé ou un DSE. L'entente devrait aborder des questions telles que l'accès continu aux dossiers des patients après avoir quitté un groupe de médecins ou à la fin des ententes avec des fournisseurs de service externes. Consulter l'annexe C, page 26, Ententes sur le partage de données – Principes applicables aux dossiers médicaux électroniques/dossiers de santé électroniques
- Les médecins doivent comprendre quelles sont leurs obligations lorsqu'ils participent à des systèmes de DSE gérés par des hôpitaux, des agences/régies régionales de la santé, des provinces/territoires ou qu'on leur demande de verser des extraits des DME de leur pratique à ce type de système. Les médecins devraient savoir quel est l'« ensemble de données de base » du DSE auquel ils contribuent. Consulter la page 16, Le partage de données et les ententes entre médecins
- Les médecins membres devraient discuter avec leurs patients de l'inclusion de leurs renseignements personnels sur la santé dans un DME/DSE. Un consentement explicite peut s'avérer nécessaire lorsque l'information sur le patient est partagée avec d'autres personnes à des fins autres que la prestation des soins de santé (c.-à-d. à l'extérieur du cercle de soins). Consulter la page 6, Le consentement des patients et les droits d'accès
- L'examen des exigences liées à la sécurité des DME/DSE devrait être prioritaire. Il s'agit notamment de veiller à ce qu'il y ait des exigences en matière de sécurité et de sauvegarde d'information, et de chiffrement des renseignements personnels sur la santé entreposés dans un format électronique. De plus, les DME/DSE devraient avoir une piste de vérification qui produit un relevé adéquat de leur accès et de leurs modifications. Les DME/DSE devraient permettre au médecin de contrôler l'accès aux renseignements sur le patient, notamment par l'intermédiaire des demandes de « verrouillage » ou de « masquage » faites par les patients. Consulter la page 8, Les questions de sécurité et de protection des renseignements personnels
- Les membres doivent envisager l'adoption de mesures et de procédures de sécurité appropriées lorsqu'ils transmettent des renseignements personnels sur la santé par courrier électronique ou autres modes électroniques. Consulter la page 14, L'envoi et le transfert de dossiers
- Les périodes de conservation des dossiers médicaux revêtent une importance aussi grande que celles des dossiers papier. Lorsque la période de conservation exigée pour les dossiers électroniques est échuë, les renseignements dans le DME/DSE peuvent être détruits de manière appropriée. Consulter la page 15, La destruction et l'élimination de dossiers
- Le fait de se fier exclusivement aux dossiers personnels de santé du patient soulève des questions particulières pour les médecins. Il faut faire preuve de prudence puisque c'est le patient qui déterminera généralement quelle information figurera dans ces dossiers. Les médecins qui utilisent des services de dossiers médicaux personnels ou qui ont accès à ces services ou à d'autres sites Web semblables sur Internet voudront discuter avec le patient des risques en matière de protection des renseignements personnels que comportent ces services. Consulter la page 19, Les nouveaux enjeux

Introduction

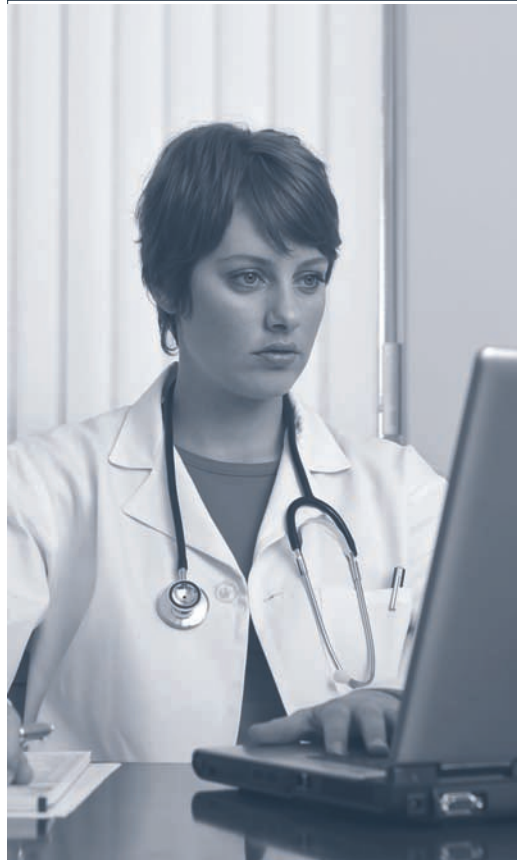
En raison des progrès technologiques constants, les dossiers médicaux électroniques (DME) et les dossiers de santé électroniques (DSE) sont devenus une partie intégrante de la prestation des soins de santé au Canada. Les DME/DSE ont le potentiel d'améliorer la gestion des soins des patients tout en appuyant l'efficacité globale du système de santé. Les gains en efficacité obtenus de ces progrès devraient accroître la qualité des soins, améliorer l'accès aux soins et réduire les coûts.

Reconnaissant les utilisations et les avantages possibles, le présent guide vise à donner aux membres une vue d'ensemble des questions liées à la mise en place et à l'utilisation des DME/DSE, y compris les questions technologiques et les risques médico-légaux. Il est destiné à être une ressource pratique pour les médecins.

DIFFÉRENCES ENTRE LES DME ET LES DSE

Un DME fait en général référence à la version électronique du dossier papier que les médecins utilisent depuis longtemps pour consigner l'information sur leurs patients. Le DME peut être un simple système en cabinet ou un DME partagé plus complexe auquel ont accès tous les professionnels d'un groupe de médecins, d'un établissement de santé ou d'un réseau de professionnels de la santé (p. ex., les médecins traitants, autres professionnels de la santé, les gestionnaires d'information, etc.).

Les DSE sont habituellement gérés par un hôpital, une autorité sanitaire ou un ministère provincial ou territorial de la santé et comportent en général un échantillon plus important de renseignements provenant d'un nombre de sources plus variées que les DME. Le DSE est une compilation de données de base sur la santé obtenues de sources multiples (p. ex, médecins, physiothérapeutes, pharmaciens, laboratoires, etc.). Il comprend habituellement différents dossiers fournis par divers professionnels et organisations et est accessible par plusieurs parties autorisées dans un certain nombre de lieux de soins, peut-être même dans d'autres provinces et territoires.



Un DME est une version électronique du dossier papier que les médecins ont en général utilisé pour consigner l'information sur leurs patients. Il peut s'agir d'un simple système en cabinet ou d'un dossier partagé qui relie des professionnels de la santé dans le cadre d'un réseau.

Un DSE est géré par un hôpital, une autorité sanitaire ou un gouvernement provincial ou territorial et comporte en général un échantillon plus important d'information issue de nombreuses sources.

Choisir un système approprié

- Évaluer les besoins de la pratique et choisir un système/un logiciel qui répond le mieux à ces besoins.
- Demander une aide professionnelle du fournisseur de logiciel et/ou d'un consultant en technologies de l'information, le cas échéant.
- Consulter des collègues qui ont mis en place un DME, ainsi que les associations médicales provinciales, territoriales et nationales.
- Consulter votre conseiller juridique personnel avant de conclure une entente de location ou d'achat d'équipement.

CHOISIR UN SYSTÈME DE DOSSIERS ÉLECTRONIQUES

Lorsque vient le temps de choisir un système approprié, les membres devraient évaluer les besoins de leur pratique et choisir un système qui répond à leurs attentes. Les membres sont invités à demander une aide professionnelle de différentes sources possibles, notamment un fournisseur de technologies, un consultant en technologies de l'information, des associations médicales provinciales, territoriales ou nationales et/ou de leur programme local d'aide technique aux médecins, si un tel programme est offert. Des collègues qui ont mis en place un DME peuvent fournir des commentaires utiles sur le processus de sélection. Certaines provinces et certains territoires ont une liste de fournisseurs pré-approuvés qui facilite le processus de sélection et peuvent aussi offrir des subventions pour compenser une partie ou l'intégralité des coûts d'acquisition et de mise en place.

Les membres devraient être au courant des exigences légales et réglementaires de leur province ou territoire et veiller à ce que le système choisi puisse répondre à ces exigences. De plus, s'ils le lient à un DSE, les membres doivent connaître les exigences en matière de compatibilité qui peuvent être prescrites par les autorités sanitaires ou les établissements de santé.

Le fournisseur du système exigera probablement que le médecin ou le groupe signe une licence d'utilisation du logiciel, laquelle est une entente juridique régissant l'utilisation et la distribution du logiciel de DME couvert par des droits d'auteur.

Bien qu'elles accordent au médecin ou au groupe de médecins la permission d'utiliser le logiciel, les licences d'utilisation imposent aussi certaines obligations et restrictions concernant l'utilisation du produit. Les membres devraient être au courant des modalités de la licence d'utilisation et sont fortement invités à communiquer avec leur conseiller juridique personnel et/ou leur association médicale provinciale, territoriale ou nationale pour obtenir des conseils avant de signer une licence d'utilisation d'un logiciel.

Le fournisseur du système peut fournir des ordinateurs, des tablettes informatiques, des assistants numériques, des serveurs ou autre matériel devant être utilisés avec un système de DME/DSE donné. Le médecin ou le groupe de médecins peut acheter ou louer ce matériel. Si le matériel est loué, les membres doivent connaître les modalités du contrat de location, y compris les paiements et les pénalités à verser en cas de résiliation. Si le matériel est acheté, les membres devraient se familiariser avec les modalités de la convention d'achat, y compris toutes les garanties applicables. Les médecins devraient consulter leur conseiller juridique personnel avant de conclure toute convention de location ou d'achat de matériel.

En plus de choisir le bon système (y compris le logiciel et le matériel), il faut prendre en compte un certain nombre de considérations d'ordre pratique, notamment :

- Comment le travail se poursuivra-t-il pendant l'installation du DME et la conversion des dossiers? Comment la prestation des soins aux patients et la tenue de dossiers seront-elles gérées pendant la transition? Qu'advient-il des dossiers papier convertis au format électronique ou aux dossiers partiellement convertis? Faut-il procéder à une « évaluation des éléments relatifs à la vie privée »?
- Quelle formation sera suivie par le médecin et son personnel, et qui fournira le soutien technique continu?
- Quels systèmes seront mis en place, tant du point de vue technique que de politique interne, pour veiller à la sécurité et à la

protection de la confidentialité des dossiers des patients?

- Comment l'intégrité des données sera-t-elle assurée (p. ex., pistes de vérification, systèmes de sauvegarde et de reprise, procédures d'assurance de la qualité comme des vérifications, etc.)?
- Quel système sera mis en place pour veiller à la destruction appropriée des dossiers après la période de conservation requise?
- Quelles sont les ententes de duplication à signer? Il peut s'agir d'ententes avec une autorité sanitaire (locale, régionale ou provinciale) ou d'un ministère utilisant un DSE. De plus, il peut s'avérer nécessaire de conclure des ententes avec des fournisseurs de service qui offrent des services en technologies de l'information. Lorsque le DME est mis en place dans un groupe de médecins, il peut être utile de conclure une entente avec les membres du groupe.

Ces questions, et bien d'autres, seront abordées dans les chapitres qui suivent.

TRAVAILLER AVEC DES SYSTÈMES D'AIDE À LA DÉCISION

Les médecins utilisent souvent des algorithmes ou des fiches d'aide à la décision pour analyser les faits cliniques et les aider dans le choix d'un traitement ou dans le diagnostic à poser. Certains DME/DSE sont dotés d'outils d'aide à la décision intégrés dans le logiciel qui invitent l'utilisateur à prendre en considération certains facteurs et/ou décisions possibles en réponse aux données saisies. La présence d'un outil d'aide à la décision dans un DME/DSE soulève des questions uniques et complexes qui doivent être prises en considération avant l'achat.

À titre d'exemple, les médecins doivent établir si le système permet aux utilisateurs de désactiver l'outil d'aide à la décision ou de ne pas en tenir compte. Si le système le permet, les membres voudront s'assurer qu'il y a une solide piste de vérification qui fait le suivi de l'acceptation ou du rejet fait par les utilisateurs. Bien que chaque système fonctionne différemment, les utilisateurs devraient savoir à l'avance de quelle manière un outil d'aide à la décision donné fonctionne et s'ils peuvent se fier à l'information générée.

Les outils d'aide à la décision ne doivent pas être utilisés pour remplacer le jugement du médecin.

Chaque suggestion offerte par l'outil doit être évaluée en fonction des circonstances propres au cas.

Les membres voudront consigner dans le dossier du patient les raisons pour lesquelles ils ont suivi ou non la suggestion offerte par l'outil d'aide à la décision. Si le diagnostic suggéré par le logiciel n'est pas retenu et qu'il s'avère être juste en rétrospective, le médecin peut, dans le cadre d'une action en justice ou d'une plainte auprès du Collège, devoir justifier pourquoi il n'a pas tenu compte de l'information. Dans ces circonstances, il serait utile que la justification du médecin de faire abstraction de la suggestion soit documentée. De même, si l'outil d'aide à la décision est désactivé, les médecins voudront documenter la raison derrière ce choix.



La réglementation des dossiers électroniques

- Se familiariser avec les exigences des organismes de réglementation (Collèges), les lois, les règlements et autres attentes sur l'utilisation des dossiers électroniques.
- Passer en revue les lois sur la protection des renseignements personnels; dans certaines provinces et certains territoires, ces lois peuvent renfermer des dispositions ou des attentes précises concernant les DME/DSE.

Les règlements ou les lignes directrices déjà en place sur la création, la maintenance, la conservation et la destruction des dossiers médicaux papier s'appliquent en général aux DME/DSE. D'autres exigences peuvent s'appliquer spécifiquement aux dossiers électroniques. Celles-ci seront principalement établies par les organismes de réglementation (Collèges) et les gouvernements fédéral, provinciaux et territoriaux.

EXIGENCES DES ORGANISMES DE RÉGLEMENTATION (COLLÈGES)

Plusieurs Collèges ont adopté des politiques ou des règlements sur les DME/DSE qui incluent certaines ou la totalité des exigences suivantes :

- Le système peut afficher et imprimer rapidement les renseignements consignés pour chaque patient selon un ordre chronologique;
- Le système offre la possibilité d'accéder au dossier de chaque patient en fonction du nom du patient et du numéro d'assurance-maladie (le cas échéant);
- Le système a une piste de vérification qui :
 - consigne la date et l'heure de chaque entrée d'information pour chaque patient,
 - indique toute modification apportée aux renseignements consignés,
 - conserve les renseignements originaux lorsqu'il y a modification ou mise à jour, et
 - peut être imprimée séparément des renseignements consignés pour chaque patient.

- Le système doit être doté de dispositifs de sécurité solides (notamment le chiffrement, l'utilisation de mots de passe et de contrôles d'accès) afin d'assurer une protection contre des accès non autorisés;
- Le système fait automatiquement des copies de sauvegarde des fichiers et permet la reprise des fichiers de sauvegarde ou offre une protection raisonnable contre la perte, l'endommagement et l'inaccessibilité de l'information.

Bien que toutes ces exigences ne soient pas nécessairement applicables dans chaque province ou territoire, elles devraient être prises en considération lors de la mise en place d'un DME dans un cabinet.

RESPECTER LES LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Des lois sur la protection des renseignements personnels qui régissent la collecte, l'utilisation et la divulgation des renseignements personnels sont mises en application dans l'ensemble des provinces et des territoires. Dans de nombreuses provinces, ces lois ont des dispositions qui s'appliquent précisément aux dossiers de santé électroniques. Les lois régissant le commerce électronique peuvent aussi s'appliquer et en général stipulent que les dossiers électroniques sont équivalents aux dossiers papier, règlementent l'utilisation des signatures électroniques et abordent certaines questions en matière de preuve.

La plupart des lois sur la protection des renseignements personnels obligent les médecins et autres dépositaires d'information sur les patients à prendre toutes les précautions qui s'imposent pour minimiser le risque de perte, de vol ou d'accès non autorisé ou d'utilisation de cette information. Certaines lois sur la protection des renseignements personnels exigent que les dépositaires mettent en œuvre des mesures de protection précises lorsqu'ils gèrent de l'information sur les patients en format électronique.

Le consentement des patients et les droits d'accès

- Songer à aviser les patients que leurs renseignements personnels sur la santé seront conservés dans un DME/DSE, même si une telle notification n'est pas strictement nécessaire. Les renseignements personnels sur la santé peuvent en général être partagés dans le cadre d'un « cercle de soins » aux fins de prestation de soins de santé.
- Se demander si un consentement explicite est nécessaire, notamment lors de la divulgation à un tiers de renseignements sur le patient contenus dans un DME/DSE à des fins autres que la prestation de soins.
- Envisager d'avoir une entente écrite avec les fournisseurs de service qui énonce les obligations en matière de protection des renseignements personnels.
- Les membres peuvent choisir de discuter avec leur Collège afin de savoir s'il est nécessaire d'obtenir le consentement des patients avant de verser leurs renseignements sur la santé dans un ensemble de données de base.
- Les patients peuvent avoir la permission de limiter l'accès aux renseignements personnels sur la santé contenus dans un DME/DSE (p. ex., coffres-forts, masquage, directive en matière de divulgation/non-participation).
- Au besoin, donner aux patients un accès à leurs renseignements personnels sur la santé contenus dans un DME/DSE dans un format approprié.

En général, les médecins n'ont pas à obtenir le consentement explicite d'un patient pour inclure ses renseignements sur la santé dans un DME/DSE, ou pour partager cette information avec d'autres professionnels de la santé aux fins d'un traitement. Les médecins peuvent généralement se fier qu'ils ont le consentement implicite d'un patient pour le partage de l'information au sein du « cercle de soins », qui inclue les professionnels de la santé devant connaître ces renseignements pour la prestation de soins.

Les lois sur la protection des renseignements personnels permettent aussi en général aux dépositaires de partager les renseignements personnels sur la santé avec un « agent » (comme un fournisseur de service ou une entreprise qui aide le cabinet du médecin) sur la base d'un consentement implicite. À titre de dépositaire, le médecin qui retient les services d'un agent demeure responsable des renseignements personnels sur la santé que détient cet agent.

Par conséquent, les membres devraient s'assurer que le fournisseur comprend la nécessité de protéger les renseignements personnels sur la santé et de prendre les mesures appropriées dans l'exécution de ses fonctions. L'ACPM encourage les membres à conclure une entente écrite afin de confirmer que l'agent comprend ses obligations. Dans certaines provinces et certains territoires, le commissaire à la protection de la vie privée peut exiger une entente écrite.

Bien que le consentement puisse en général être implicite, il peut s'avérer prudent dans certaines circonstances d'aviser les patients que les renseignements sur leur santé seront entreposés électroniquement, en particulier s'ils sont entreposés dans un DME partagé ou dans un DSE auquel de nombreuses personnes auront accès.

Les lois sur la protection des renseignements personnels dans certaines provinces ou certains territoires exigent que les patients soient avisés dans ces circonstances par une conversation personnelle, l'envoi d'une lettre ou une affiche dans le cabinet.

Le consentement explicite devrait être obtenu lorsqu'un médecin se voit demander de divulguer des renseignements sur le patient contenus dans un DME/DSE :

- a) À un tiers ne faisant pas partie du cercle de soins (p. ex., une compagnie d'assurance ou un employeur) et qui n'est pas un agent du médecin; ou
- b) Lorsque les renseignements seront utilisés à des fins autres que la prestation de soins au patient et que cela n'est pas permis ou requis par la loi.

On fait souvent référence à la divulgation dans le dernier cas comme une « utilisation secondaire » des renseignements personnels sur la santé. Parmi d'autres exemples d'« utilisations secondaires », notons le marketing, la recherche ou la divulgation de renseignements personnels sur la santé à une organisation ou à une agence gouvernementale à des fins de planification des systèmes de santé. Certaines lois sur la protection des renseignements personnels permettent expressément l'emploi des renseignements sur la santé à ces fins. Les membres voudront se familiariser avec les exemptions prévues dans les lois sur la protection

des renseignements personnels pertinentes. Le cas échéant, les renseignements sur le patient doivent, dans la mesure du possible, être dépersonnalisés avant leur utilisation à d'autres fins que la prestation des soins de santé.

Lorsqu'un consentement explicite est requis, il est en général prudent de demander au patient de signer un formulaire de consentement. Si un consentement verbal est obtenu, l'information doit être consignée dans le dossier médical du patient. Peu importe l'approche utilisée, il doit s'agir d'un consentement éclairé.

ENSEMBLE DE DONNÉES DE BASE

Le terme « ensemble de données de base » renvoie habituellement à la partie du dossier du patient à laquelle ont aussi accès les professionnels de soins non primaires ou les établissements de santé. Cet ensemble peut être considéré comme un sous-ensemble ou, dans certains cas, un résumé ou un aperçu du dossier médical complet du patient. Puisqu'il est créé dans le but d'être partagé entre les professionnels de la santé et autres intervenants dans la prestation des soins, il ne fait en général partie que d'un DSE.

Les membres utilisant des DME devraient se demander si leur système permet le masquage, comment ils géreront les demandes de verrouillage/masquage, et quelles sont les obligations d'informer les destinataires que l'information peut être incomplète.

Les membres voudront discuter avec leur Collège, leur autorité sanitaire ou leur commissaire à la protection de la vie privée afin de savoir s'il est nécessaire d'obtenir le consentement des patients avant de verser leurs renseignements sur la santé dans un ensemble de données de base. Des précisions doivent aussi être obtenues auprès de l'autorité pertinente quant aux renseignements à inclure.

DEMANDES DES PATIENTS CONCERNANT L'ACCÈS À LEURS RENSEIGNEMENTS PAR D'AUTRES PERSONNES

Les patients peuvent demander que l'accès à leurs renseignements sur la santé contenus dans un DME/DSE soit limité, même à des fins de prestation de soins. Ceci peut être fait à l'aide d'un processus communément appelé « verrouillage » ou « masquage ». Les membres utilisant des DME devraient se demander si leur système permet le masquage, comment ils géreront les demandes de verrouillage/masquage, et quelles sont les

obligations d'informer les destinataires que l'information peut être incomplète. S'ils conservent des renseignements sur un patient dans un DME partagé ou un DSE, les membres devraient aussi demander aux responsables des systèmes partagés de quelle manière traiter ces demandes de verrouillage ou de masquage.

Dans les provinces et territoires ayant des DSE provinciaux ou territoriaux, il peut y avoir en place des processus en matière de « directive de divulgation ou de non participation » qui permettent aux personnes de contrôler l'information. Bien que la portée et les restrictions de la directive ou de la non-participation puissent varier, elles peuvent avoir trait au type de renseignements personnels sur la santé contenus dans le DSE, les fins pour lesquelles les renseignements peuvent être divulgués à partir du DSE, et les personnes ou les groupes de personnes pouvant avoir accès aux renseignements dans le DSE. Lorsqu'un tel processus existe et est reconnu par la loi, il peut servir à limiter l'accès d'un professionnel de la santé aux renseignements, sauf dans certaines circonstances telles qu'une incapacité, une situation d'urgence ou le consentement explicite du patient.

ACCÈS DU PATIENT

En général, les patients ont le droit d'accéder à leurs propres renseignements sur la santé. Les médecins doivent avoir un moyen de donner accès aux patients à leurs renseignements sur la santé contenus dans un DME/DSE dans un format approprié. Les médecins peuvent facturer des frais raisonnables pour des copies des dossiers des patients.

Malgré cette obligation, dans certaines circonstances, les médecins peuvent être réticents à donner accès à certains renseignements. À titre d'exemple, un psychiatre peut être d'avis qu'il serait néfaste pour un patient de voir l'information liée à ses impressions ou son analyse de la santé mentale du patient. Bien que dans des circonstances exceptionnelles un patient puisse se voir refuser l'accès à des parties de son dossier médical, on s'attend en général à ce que l'information possiblement néfaste soit isolée du dossier, plutôt que de refuser l'accès du patient au dossier.

Les questions de sécurité et de protection des renseignements personnels

- S'assurer que le système de DME/DSE est doté de dispositifs de sécurité robustes, y compris de contrôles d'accès fondés sur le rôle et les responsabilités de l'utilisateur.
- Songer à mettre en place une protection par chiffrement à tous les systèmes informatiques et à tous les dispositifs portables de stockage de données renfermant des renseignements personnels sur la santé. Certains commissaires à la protection de la vie privée et Collèges ont énoncé que les médecins et autres dépositaires doivent chiffrer les renseignements sur les patients entreposés dans des appareils mobiles.
- Consulter le commissaire à la protection de la vie privée ou l'ombudsman sur la manière de faire une « évaluation des facteurs relatifs à la vie privée ».
- Il s'avère prudent pour les membres de soumettre périodiquement le système de DME à des vérifications de la protection des renseignements personnels après leur mise en place.

Tout comme dans le cas des dossiers papier, les médecins ont une obligation déontologique et juridique d'assurer la confidentialité de tous les renseignements sur les patients. Toutefois, lorsque ces renseignements sont conservés dans un DME/DSE, ils sont probablement accessibles à un plus grand nombre de personnes qu'un dossier papier traditionnel. Par conséquent, la protection de l'information s'avère plus complexe.

Des dispositifs et des politiques solides en matière de sécurité doivent être mis en place pour veiller à ce que l'information contenue dans un DME/DSE soit seulement accessible dans le cercle de soins pour prodiguer des soins adéquats aux patients, ou pour d'autres fins autorisées par la loi ou avec le consentement explicite du patient. Il est possible d'y arriver en ayant recours à des identificateurs d'utilisateurs et à des mots de passe à l'ouverture d'une session. Outre des mécanismes de sécurité qui limitent l'accès aux personnes autorisées, il est prudent, dans la mesure du possible, de doter le système de DME/DSE de contrôles qui limitent l'accès en fonction du rôle et des responsabilités de l'utilisateur. Une autre façon de protéger les renseignements sur le patient consiste à mettre les imprimantes dans des lieux à accès limité.

L'ACPM recommande fortement aux médecins de mettre en place une protection par chiffrement à tous les systèmes informatiques (y compris les ordinateurs de bureau et les portables) renfermant des renseignements personnels sur la santé. Les membres qui entreposent de l'information sur les patients dans des dispositifs portables de stockage de données comme des assistants numériques personnels, des clés USB, des disques durs portables, devraient aussi doter ces appareils d'un logiciel de chiffrement. En effet, certains commissaires à la protection de la vie privée et Collèges ont énoncé que les médecins et autres dépositaires doivent chiffrer les renseignements sur les patients conservés dans des appareils mobiles.

Lorsqu'ils utilisent un réseau sans fil pour accéder aux renseignements sur des patients contenus dans un DME/DSE ou pour envoyer cette information, les membres voudront prendre des mesures pour s'assurer que le réseau est sécurisé. D'autres exigences peuvent s'appliquer pour la transmission de renseignements personnels sur la santé d'un patient à l'extérieur de la province ou territoire où l'information a été recueillie. À titre d'exemple, il peut être requis d'aviser les patients lorsqu'un fournisseur de service à l'extérieur du Canada est utilisé (p. ex., pour la transcription de dictée).

ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE/VÉRIFICATION DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Certaines provinces et certains territoires exigent une évaluation des facteurs relatifs à la vie privée avant la mise en place ou la modification d'un système de DME. Bien qu'une telle évaluation ne soit pas une exigence de la loi dans toutes les provinces et tous les territoires, il s'agit d'une procédure prudente et utile. Les évaluations des facteurs relatifs à la vie privée cernent et réduisent les risques en matière de protection des renseignements personnels liés à la mise en place d'un système de DME. L'ACPM encourage ses membres à consulter leur commissaire à la protection de la vie privée ou ombudsman respectif sur la manière de procéder à une évaluation des facteurs relatifs à la vie privée. Certains commissaires à la protection de la vie privée ont publié des lignes directrices à ce sujet.

Dans certaines provinces et certains territoires, il peut s'avérer nécessaire de présenter au commissaire une évaluation des facteurs relatifs à la vie privée dûment remplie.

Il est également prudent pour les membres d'effectuer des vérifications périodiques des systèmes de contrôle visant à assurer la protection des renseignements personnels après la mise en place d'un système de DME. Des vérifications de routine veillent à ce que l'accès aux dossiers des patients dans le DME/DSE soit limité aux personnes et aux fins autorisées. En procédant à des vérifications de façon régulière, il est possible de relever tout accès non autorisé et d'y réagir rapidement.

TRANSPORT DES DONNÉES

Il peut aussi y avoir des risques associés au transport physique de renseignements personnels sur la santé conservés électroniquement. L'Agence des services frontaliers du Canada et certains gouvernements étrangers ont publié des déclarations énonçant clairement leur pouvoir de fouiller et d'éventuellement saisir les appareils électroniques qu'un voyageur pourrait tenter d'entrer au pays. Dans certains cas, l'information obtenue lors d'une fouille à la frontière peut être largement partagée. Cela soulève des préoccupations évidentes concernant la protection et la sécurité des renseignements personnels sur la santé des patients lorsqu'ils sont conservés dans un appareil qui peut être assujéti à une fouille à la frontière.

L'ACPM encourage ses membres à communiquer avec elle avant de transporter physiquement ou de transmettre électroniquement des données sur la santé à l'extérieur du pays.



Le maintien de l'intégrité des données

- S'assurer que le DME/DSE a une piste de vérification indiquant clairement les corrections sans éclipser le dossier original.
- Envisager de faire une sauvegarde des renseignements électroniques sur les patients sur une base quotidienne ou hebdomadaire.
- Les demandes de patients visant à corriger ou à modifier une entrée faite par un autre professionnel de la santé devraient être acheminées au professionnel de la santé en question.
- Si un membre se rend compte que le DME/DSE qu'il consulte contient de l'information périmée, incomplète ou inexacte, il est prudent d'alerter immédiatement les autres utilisateurs du DME/DSE afin de ne pas compromettre le traitement du patient.
- Tous les professionnels de la santé utilisant le DME/DSE devraient déployer des efforts raisonnables pour savoir qui y contribue, comment on y accède, et comment l'information qu'ils y ont versée devrait apparaître sur l'écran ou l'imprimé.
- Dans le cas d'une éventuelle action en justice, un membre utilisant un dispositif de signature électronique voudra être en mesure d'expliquer le fonctionnement du dispositif et d'en attester la fiabilité.

Les médecins ont un devoir envers leurs patients de tenir des dossiers précis, complets et à jour. En ce qui a trait aux systèmes de dossiers électroniques, les médecins doivent veiller à l'authenticité et à l'intégrité des données électroniques et des processus qui mènent à leur création. Certaines mesures peuvent être exigées par la loi et/ou par le Collège du membre.

PISTES DE VÉRIFICATION

Un DME/DSE devrait avoir une piste de vérification qui détaille l'accès des utilisateurs et les modifications apportées au dossier. Une piste de vérification permet de démontrer que l'information contenue dans le DME/DSE est authentique et fiable. Elle aide aussi à assurer la continuité des soins aux patients, notamment lorsque de nombreux professionnels de la santé ont accès au dossier.

Le système de piste de vérification devrait permettre au médecin de faire les activités suivantes :

- Démontrer la solidité de la chaîne de garde du dossier ou des entrées;
- Relever, le cas échéant, quelles modifications ont été apportées au dossier;
- Déterminer qui a apporté une modification donnée, et quand;
- Imprimer et visualiser une copie de la version originale non modifiée du dossier (toutes les modifications devraient être visibles séparément sans effacer de façon permanente l'entrée originale).

MODIFIER/EFFACER/CORRIGER

Il incombe aux médecins d'avoir des dossiers précis. L'acquiescement de cette responsabilité inclut d'obtempérer aux demandes des patients qui veulent avoir accès à leur dossier. Un patient a le droit d'accéder à son dossier et de demander une correction. Les médecins ont en général le droit de refuser les demandes de correction d'opinions ou de renseignements médicaux nécessaires à des fins cliniques. La décision doit être prise en fonction de chaque cas et dans le respect de toutes les lois et toutes les exigences des Collèges applicables. À titre d'exemple, les lois sur la protection des renseignements personnels peuvent fixer des échéanciers pour répondre aux demandes des patients, définir les paramètres pour accepter ou refuser les demandes de correction, déterminer de quelle manière corriger un dossier et exiger la prise de certaines mesures une fois une demande acceptée ou refusée. Les membres devraient connaître ces dispositions et s'y conformer.

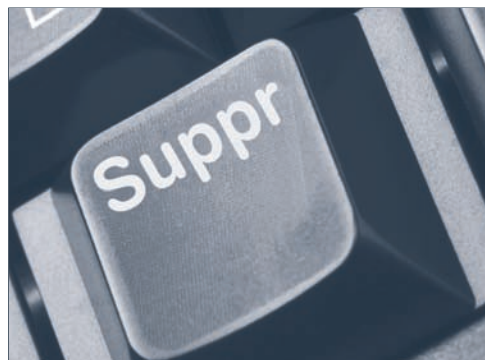
Les membres devraient aussi être conscients que, dans le cas d'un DME/DSE, de nombreux professionnels de la santé peuvent traiter le patient et faire des entrées dans le dossier. Si un patient demande que le médecin corrige ou modifie une entrée faite par un autre professionnel de la santé, il serait sage d'acheminer cette demande au professionnel en question. Par contre, si l'entrée est pertinente au traitement que le membre prodigue ou a prodigué au patient, le membre peut aussi choisir de consulter ce professionnel de la santé afin de déterminer si la modification doit être apportée et par qui.

S'il refuse la demande de modification d'un patient, le membre devrait garder dans le dossier une copie de la demande du patient, de la lettre de refus établissant les raisons du refus, ainsi que toutes communications reçues ou envoyées par courrier électronique ou tout autre mode de communication électronique. Certaines lois sur la protection des renseignements personnels exigent aussi que les médecins gardent des copies de toute lettre de désaccord envoyée par le patient après qu'il ait pris connaissance du refus.

Les médecins ont aussi un devoir général de corriger un renseignement inexact dans le dossier d'un patient, notamment si ce renseignement est essentiel au traitement du patient.

Les membres devraient se référer aux exigences applicables et à l'entente sur le partage de données lorsqu'ils envisagent d'apporter une correction.

Si un membre est d'avis qu'il faut apporter un changement au dossier, la modification devrait être faite d'une manière qui répond le plus aux exigences des Collèges applicables aux dossiers papier. La modification ne devrait pas éclipser ou effacer l'entrée originale. Dans un environnement électronique, les modifications peuvent habituellement être faites à l'aide d'un addenda ou d'une biffure électronique. La date, l'heure et les initiales (ou signature électronique) de la personne apportant la modification devraient figurer au dossier électronique. La fonction de « suivi des modifications » (offerte dans la plupart des logiciels de traitement de texte pour surveiller les modifications apportées aux documents) devrait être utilisée à cette fin. Si cette fonction n'est pas offerte, un addenda devrait être mis dans le dossier, de préférence à côté de l'entrée originale, expliquant quel changement est nécessaire.



AVISER LES AUTRES UTILISATEURS DE LA PRÉSENCE DE RENSEIGNEMENTS ERRONÉS OU PÉRIMÉS

Si un membre se rend compte que le DME/DSE qu'il consulte contient de l'information périmée, incomplète ou inexacte, il est prudent d'alerter immédiatement les autres utilisateurs du DME/DSE afin de ne pas compromettre le traitement du patient. Des efforts devraient alors être déployés pour corriger l'information erronée le plus rapidement possible, de la manière décrite précédemment. Les membres devraient aussi savoir que les lois de protection des renseignements personnels exigent en général que les dépositaires qui corrigent des dossiers avisent les personnes à qui l'information pertinente a été divulguée.

Les ententes sur le partage de données (une entente qui définit les modalités du partage des renseignements électroniques sur la santé; consulter la section 9) devraient idéalement contenir une disposition qui traite de la procédure à suivre pour corriger un DME/DSE et exiger une notification lorsque des renseignements qui ont déjà été consultés sont erronés ou périmés. Les membres devraient se référer aux exigences applicables et à l'entente sur le partage de données lorsqu'ils envisagent d'apporter une correction.

RECEVOIR DES DONNÉES/DOSSIERS D'AUTRES PROFESSIONNELS DE LA SANTÉ

Le fait que d'autres professionnels de la santé aient accès aux données et puissent contribuer directement au DME/DSE représente un défi unique lié aux DSE (et aux DME partagés).

Un médecin peut aussi recevoir d'autres professionnels de la santé des données ou des dossiers qui ont été intégrés dans le DME d'un patient. Ces médecins ne connaissent peut-être pas bien la pratique des autres professionnels et ne se consultent peut-être pas régulièrement, si consultation il y a.

La précision est d'autant plus importante dans de telles circonstances et tous les professionnels de la santé utilisant le DME/DSE devraient déployer des efforts raisonnables pour savoir qui y contribue, comment on y accède, et comment l'information qu'ils y ont versée devrait apparaître sur l'écran ou l'imprimé (p. ex., entrées paraphées ou signées et datées, utilisation du biffage ou d'addenda pour les changements apportés aux entrées originales, etc.).

CONVERTIR DES DOSSIERS PAPIER EN FORMAT ÉLECTRONIQUE

S'ils choisissent d'adopter un DME, les membres peuvent se demander si leurs dossiers papier doivent être convertis dans un format électronique, et si les dossiers originaux peuvent être détruits après leur numérisation.

Bien que le transfert des dossiers papier dans un format électronique puisse procurer des avantages énormes pour les médecins en terme d'augmentation de l'efficacité et d'amélioration des soins prodigués aux patients, les membres devraient néanmoins savoir que les documents convertis dans un format électronique sont considérés comme des copies (autrement appelés « preuve secondaire »), mais qui peuvent être admissibles dans les actions en justice si certaines étapes sont suivies. Les règles concernant l'admissibilité des copies ont été modifiées dans la plupart des provinces et territoires au Canada de façon à tenir compte des dossiers électroniques.

La réponse à une demande juridique visant la production d'un dossier électronique peut s'avérer problématique. Il peut être nécessaire de produire les « métadonnées » intégrées dans tous les documents électroniques. Une aide technique spécialisée peut être requise pour veiller à ce que toutes les données exigées soient incluses. À la réception d'un subpoena ou d'une ordonnance demandant la production de dossiers médicaux (en format papier ou électronique), les médecins devraient communiquer avec l'ACPM pour obtenir des conseils.

Certains Collèges permettent la destruction des dossiers papier après leur numérisation. Toutefois, l'ACPM encourage ses membres à suivre les lignes directrices suivantes pour s'assurer que les dossiers papier convertis dans un format électronique répondent aux exigences en matière de preuve :

- Une entreprise commerciale expérimentée et digne de confiance peut aider à établir les procédures de conversion;
- La conversion devrait se dérouler de manière uniforme et minutieuse, en prenant des mesures de protection appropriées pour assurer une fiabilité suffisante des copies numériques;
- Des procédures écrites doivent être établies et suivies de façon constante pour la conversion (y compris la documentation du type de processus de conversion utilisé), et le membre doit en conserver une copie;

- Le processus devrait comprendre une quelconque forme d'assurance de la qualité (p. ex., la comparaison des copies numériques avec l'original pour veiller à ce que l'information ait bien été convertie), et il faudrait prendre note des mesures d'assurance de la qualité prises pour chaque document.

Les dossiers numériques devraient être gardés en format « lecture » de sorte qu'ils ne puissent pas être modifiés ou manipulés après leur conversion. Les membres devraient connaître les différences entre la « numérisation » et la « reconnaissance optique de caractères » (ROC). La numérisation produit seulement une représentation numérique non modifiable d'une image, tandis que la ROC est un procédé technologique qui convertit l'image d'un texte manuscrit ou typographié en un texte pouvant être modifié. Lorsqu'une image a été convertie à l'aide de la ROC, le texte peut être modifié, faire l'objet de recherche ou être manipulé d'autre façon. La ROC peut être utilisée de concert avec la numérisation. Toutefois, la ROC ne devrait pas être utilisée seule pour la conversion de dossiers papier en format électronique, à moins que les dossiers originaux soient aussi numérisés ou conservés en version papier.

Lorsque les mesures appropriées ont été prises, il peut être raisonnable de détruire le dossier original. Par contre, dans des cas exceptionnels, notamment lorsque la qualité des dossiers papier rend difficile la lecture du document converti, il peut s'avérer prudent de conserver les dossiers papiers pendant la période de conservation recommandée par l'ACPM; c'est-à-dire au moins dix ans à compter de la date de la dernière entrée ou, dans le cas des mineurs, dix ans à compter de l'atteinte de la majorité. La destruction éventuelle des dossiers papier devrait être effectuée conformément aux obligations du médecin en matière de confidentialité et à toutes exigences applicables de la loi ou du Collège.

MIGRATION DE DONNÉES

Les médecins qui utilisent déjà un DME et souhaitent passer à un nouveau logiciel ou fournisseur de DME devront prendre en considération un moyen de préserver l'intégrité des données telles qu'elles ont été entrées dans l'ancien système de DME. Parmi les options possibles : la migration des données de l'ancien système au nouveau système ou l'archivage des données dans l'ancien système. Peu importe le processus utilisé,

les médecins voudront s'assurer d'avoir un accès continu aux données sur leurs patients pendant la période de conservation applicable. Ils voudront aussi veiller à ce que les renseignements, y compris les métadonnées, ne soient pas compromis ou modifiés de quelque façon pendant le processus.

COPIE DE SAUVEGARDE ET RÉCUPÉRATION

Il n'est pas rare que les systèmes informatiques tombent en panne; ce qui peut entraîner la perte de renseignements sur les patients contenus dans un DME. Dans certaines provinces et certains territoires, les lois et/ou les politiques des Collèges exigent que les médecins veillent à faire régulièrement une sauvegarde des fichiers électroniques et que le système permette la récupération de ces fichiers.

Les membres voudront peut-être aussi vérifier régulièrement le processus de récupération de ces fichiers de sauvegarde

Même en l'absence d'exigences réglementaires dans une province ou un territoire, il est bon de faire une sauvegarde des renseignements sur les patients sur une base quotidienne ou hebdomadaire et de veiller à ce que les fichiers de sauvegarde soient chiffrés. Les membres voudront peut-être aussi vérifier régulièrement le processus de récupération de ces fichiers de sauvegarde. De plus, les membres pourraient souhaiter utiliser un système externe de sauvegarde afin de protéger les dossiers des patients advenant le vol, la perte ou la destruction d'un ordinateur du cabinet. Les médecins devraient consulter leur vendeur ou leur fournisseur de service afin d'obtenir plus de renseignements sur les capacités de sauvegarde et de récupération du système utilisé.

SIGNATURES ÉLECTRONIQUES

La fonction essentielle d'une signature consiste à associer le signataire au contenu du document. Une signature électronique peut-elle être utilisée efficacement à cette fin dans un DME/DSE? En fait, elle peut légalement servir à cette fin. Une signature électronique, bien qu'elle ne soit pas concrète, peut tout de même prouver le lien du signataire avec le document et son contenu.

Le terme « signature électronique » est un terme générique qui fait référence à un grand nombre d'options de signature non manuscrite, y compris la signature numérique. Il est couramment défini

comme une donnée électronique créée ou adoptée par une personne pour signer un document. La donnée est alors jointe ou associée au document.

La « signature numérique » est un type de signature électronique propre à une technologie donnée. Il s'agit d'une des nombreuses techniques qui répondent aux fonctions recherchées par l'utilisation d'une signature électronique. Il s'agit d'une erreur courante de considérer la signature électronique comme la simple version électronique d'une signature manuscrite. Bien que la signature apposée sur une tablette informatique soit un exemple de signature électronique, un exemple plus courant serait la signature composée d'au moins une lettre, caractère, numéro ou symbole qui est jointe ou associée à un document électronique.

Bien que la signature électronique soit en général reconnue comme étant aussi valide que la signature manuscrite, elle ne peut pas encore être utilisée dans toutes les circonstances. À titre d'exemple, dans certaines provinces et certains territoires, un médecin ne peut pas utiliser une signature électronique pour les ordonnances.

Lorsqu'ils sont admissibles, les dispositifs de signature électronique doivent répondre à certaines exigences en matière de fiabilité. Dans l'éventualité d'une action en justice, un membre qui utilise un tel dispositif voudra être en mesure d'expliquer le fonctionnement du dispositif et d'en attester la fiabilité. Sans cette attestation de la fiabilité, un tribunal pourrait ne pas accepter que le document signé électroniquement soit admis à titre de preuve ou pourrait en réduire la portée.

Par conséquent, il est important de pouvoir démontrer que la signature électronique a été associée de façon appropriée au document en question (p. ex., rapport, formulaire de consentement, etc.). Sans cette assurance de la fiabilité, l'autre partie d'un différend pourrait présenter l'argument que le patient ne savait pas à quel document il apposait sa signature lorsqu'il signait une tablette de signature à l'aide d'un stylet. D'autre part, l'argument pourrait être avancé que la signature du médecin n'était pas associée au bon rapport et que le médecin n'a pas, en fait, passé en revue le bon document.

Afin d'être en position de répondre efficacement à de tels arguments, les membres devraient envisager d'utiliser un système ayant les caractéristiques suivantes :

- La personne qui signe un document de manière électronique doit être en mesure de vérifier la signature électronique à l'écran.
- Il doit y avoir une fonction de vérification qui permet au médecin de déterminer la date et l'heure de la signature et à quel document cette signature a été associée à ce moment.
- Les gens sont en mesure d'entrer leur propre signature électronique.

L'ACPM encourage les membres à étudier les différentes options de signature électronique avec un consultant en technologies de l'information.

L'envoi ou le transfert de dossiers

- Envisager d'utiliser des mesures de sécurité appropriées lors de l'envoi électronique de renseignements personnels au patient ou à un autre professionnel de la santé.

Les dossiers électroniques facilitent une transmission rapide des renseignements sur le patient à d'autres professionnels de la santé ou au patient. Dans un DME partagé ou un DSE, il est probable que d'autres professionnels de la santé participant aux soins du patient auront un accès direct et indépendant au dossier du patient et à l'information nécessaire pour assurer un traitement. Dans ces circonstances, le médecin traitant a un rôle limité en ce qui a trait à rendre disponible l'information sur le patient.

S'ils téléversent de l'information sur un patient à partir d'un DME à un autre DME/DSE, les membres devraient se demander si le réseau qu'ils utilisent possède une protection suffisante. Encore une fois, les membres devraient consulter leur Collège respectif afin de savoir quelles sont les politiques et les lignes directrices applicables à ce sujet. De même, lorsqu'il reçoit une demande d'un autre professionnel de la santé pour de l'information sur le patient contenue dans un DME qui n'est pas partagé, le médecin devrait choisir une transmission sécurisée pour les différents moyens de communication électronique, comme le télécopieur, le courrier électronique ou un autre DME/DSE.

COMMUNIQUER ÉLECTRONIQUEMENT AVEC LES PATIENTS ET D'AUTRES PERSONNES

Les Collèges peuvent avoir des politiques ou des lignes directrices sur la communication avec les patients par courrier électronique ou télécopieur. Avant de communiquer avec des patients par courrier électronique ou par télécopieur, les membres devraient discuter avec les patients pour leur faire part des risques et obtenir leur consentement pour transmettre leurs renseignements sur la santé à l'aide de ces modes de communication. Toutes les discussions avec le patient devraient être consignées dans le dossier médical du patient. Il est conseillé d'utiliser un formulaire de consentement [voir le *Bulletin d'information* (mars 2009) intitulé « Utilisation du courrier électronique dans les communications

avec les patients : les risques juridiques », et le modèle de formulaire de consentement joint].

COURRIER ÉLECTRONIQUE

L'envoi de courriers électroniques aux patients soulève des questions juridiques uniques. Au moins un commissaire provincial à la protection de la vie privée a suggéré que les médecins évitent de communiquer des renseignements personnels sur la santé par courrier électronique, à moins que le service de courrier ne soit protégé et n'offre une fonction de chiffrement solide. Les membres devraient établir des politiques et des procédures sur la manière de traiter les communications par courrier électronique. Les employés devraient être informés, par l'intermédiaire d'une politique ou d'un autre moyen, des risques connexes à une communication par courrier électronique inappropriée.

Si le membre travaille ou détient des privilèges dans une organisation, un établissement de santé ou un hôpital, il peut être difficile d'empêcher l'organisation en question d'accéder à la correspondance électronique de nature délicate. À titre d'exemple, un membre travaillant dans un hôpital pourrait s'exposer à ce que l'administration accède à la correspondance électronique rédigée à partir d'un ordinateur de l'hôpital ou transmis à l'aide du système de l'hôpital. S'il est nécessaire d'utiliser le courrier électronique pour aborder des questions personnelles délicates, il faut envisager d'utiliser un compte personnel de courrier électronique accessible à partir d'un ordinateur dont vous avez le contrôle au bureau ou à la maison. Cette précaution s'avère particulièrement pertinente pour les membres qui reçoivent l'aide d'un conseiller juridique pour une question légale.

TÉLÉCOPIEUR

Les membres devraient aussi mettre en place des normes de procédure pour l'envoi par télécopieur de renseignements sur le patient afin de réduire les risques d'erreur d'acheminement des télécopies. À titre d'exemple, selon le destinataire et la nature de l'information télécopiée, il peut être prudent d'envisager de communiquer avec le destinataire avant d'envoyer l'information par télécopie pour confirmer le numéro du télécopieur et s'assurer que le destinataire est présent pour recevoir le document.

La destruction et l'élimination de dossiers

- Lors de la destruction de renseignements sur un patient dans un format électronique, s'assurer que le DME/DSE est supprimé de façon permanente ou effacé de manière irréversible. Cela pourrait nécessiter une destruction physique du dispositif de stockage électronique.

Tout comme dans le cas des dossiers papier, il faut des procédures pour veiller à une destruction adéquate des dossiers électroniques. Les éléments qui suivent sont des points essentiels à garder à l'esprit lorsque vous prenez en considération la conservation ou la destruction de DME :

- La période de conservation requise pour les dossiers médicaux, de format papier ou électronique, varie énormément en général selon la province ou le territoire. L'ACPM recommande aux membres de conserver des dossiers cliniques pendant au moins dix ans à partir de la date de la dernière entrée, ou au moins dix ans à compter de l'âge de la majorité dans le cas des mineurs.
- Au-delà de la période de conservation requise, les renseignements sur le patient contenus dans un DME/DSE devraient normalement être conservés aussi longtemps que cela est nécessaire aux fins pour lesquelles l'information a été recueillie.
- Lorsque la période de conservation est expirée, l'information dans un DME/DSE devrait en général être détruite de manière à en assurer la confidentialité.
- Les médecins devraient être au courant de toutes les règles et obligations applicables à la destruction des dossiers médicaux.

Certaines lois sur la protection des renseignements personnels exigent que les médecins gardent en dossier l'information suivante :

- La personne dont les renseignements personnels sur la santé sont détruits et la période à laquelle l'information s'applique; et
- Le mode de destruction et la personne chargée de superviser cette destruction.

Une destruction efficace nécessite que le DME/DSE soit supprimé de façon permanente ou effacé de manière irréversible. Lors de la destruction de renseignements, les membres doivent déterminer s'il est nécessaire de détruire non seulement les dossiers « originaux », mais aussi toutes les copies de ces dossiers, y compris les fichiers de sauvegarde.

Certains commissaires à la protection de la vie privée ont recommandé la destruction physique des dispositifs de stockage électroniques (p. ex., disque dur) pour garantir la suppression permanente des renseignements sur le patient conservés dans ces dispositifs. Cela peut signifier détruire physiquement le dispositif de stockage électronique, ou il peut suffire d'employer un logiciel de nettoyage pour supprimer l'information du disque dur. Toutefois, selon le degré de complexité du logiciel, le nettoyage peut ne pas effacer irréversiblement toutes les données sur un disque dur. Il faut éviter de vendre ou de donner des dispositifs de stockage électroniques qui contiennent ou qui ont déjà contenu des renseignements sur les patients.

Étant donné l'expertise en technologies nécessaire pour détruire efficacement de l'information entreposée électroniquement, il est préférable d'engager un fournisseur de service homologué pour détruire les renseignements sur les patients contenus dans les DME. Certains commissaires à la protection de la vie privée ont déclaré que lorsque les médecins engagent un fournisseur de service commercial pour éliminer les renseignements sur les patients, ces médecins doivent avoir une entente contractuelle écrite avec ce fournisseur de service. L'entente doit clairement définir les responsabilités du fournisseur visant à détruire de façon sécuritaire les dossiers de santé, la manière dont la destruction sera effectuée, dans quelles conditions, et par qui. Bien qu'il ne s'agisse pas actuellement d'une exigence dans l'ensemble des provinces et des territoires, il s'agit d'une pratique prudente que devraient adopter tous les membres qui retiennent les services d'une entreprise de destruction de dossiers.

Le partage de données et les ententes entre médecins

- Passer en revue le document de l'ACPM intitulé *Ententes sur le partage de données – Principe applicables aux dossiers médicaux électroniques/dossiers de santé électroniques* (annexe C), y compris les questions de protection des renseignements personnels et de confidentialité.
- Faire preuve de diligence raisonnable et s'assurer de bien comprendre l'entente conclue avec le fournisseur du système de DME/DSE.
- Lorsqu'il n'y a aucune entente de gestion de l'information pour un système de DSE établi par une autorité sanitaire, ou lors de l'établissement d'un lien à partir d'un DME vers un DSE, envisager de conclure une entente sur le partage de données.
- S'assurer que l'entente entre médecins traite de l'accessibilité des dossiers des patients, notamment après le départ d'un médecin de la pratique.

ENTREPOSAGE DE DONNÉES ÉLECTRONIQUES SUR LA SANTÉ CHEZ DES TIERS

L'arrivée de nouvelles méthodes de tenue de dossiers apporte de nouveaux modes d'entreposage et de gestion des données contenues dans les dossiers électroniques. Même le médecin le plus au fait des dernières technologies demandera probablement l'aide d'un fournisseur de service externe pour la mise en place, la maintenance et l'entreposage des dossiers médicaux électroniques. De plus, dans bon nombre de provinces et territoires, les autorités sanitaires et les hôpitaux cherchent à mettre en place leur propre DSE qui pourrait intégrer les systèmes de DME des médecins. De ce fait, de nombreux scénarios différents et de structures différentes feront en sorte qu'un médecin fera appel à un tiers pour mettre en place un système de DME/DSE.

Parmi les ententes contractuelles qu'un membre pourrait envisager de conclure au sujet d'un système de DME/DSE, notons :

- Une entente de partage/gestion de données auprès d'un vendeur ou d'un autre fournisseur de service (p. ex., logiciel, matériel, hébergement, etc.);
- Une entente de partage/gestion de données auprès d'une agence gouvernementale provinciale ou territoriale, une autorité sanitaire ou un hôpital;
- Une entente entre médecins dans un groupe de médecins (p. ex., un groupe de partage de garde, une clinique où les médecins partagent les mêmes dossiers, un groupe de médecine familiale ou un réseau de médecine familiale, une société de médecins par actif ou en nom collectif).

Dans chacune de ces situations, certains principes fondamentaux doivent être pris en considération lorsque vient le temps de signer une entente. L'ACPM, en collaboration avec l'Association médicale canadienne, a publié un document intitulé *Ententes sur le partage de données – Principes applicables aux dossiers médicaux électroniques/dossiers de santé électronique*, lequel est reproduit à l'annexe C. Les membres devraient consulter ce document ainsi que leur conseiller juridique personnel lorsqu'ils envisagent de conclure une entente sur le partage de données ou une entente entre médecins.

CHOISIR UN FOURNISSEUR INDÉPENDANT POUR L'INSTALLATION ET LA MAINTENANCE D'UN DME/DSE

Les membres qui envisagent de mettre en place un système de DME peuvent devoir faire appel aux services d'un fournisseur indépendant pour leur donner les conseils nécessaires sur les questions telles que le logiciel, le matériel, l'archivage électronique, etc. Certains gouvernements provinciaux ou territoriaux ont mis en place des programmes précis pour offrir de l'aide technique et financière aux médecins à ce sujet. Ils peuvent inclure la présélection et l'approbation des fournisseurs pour veiller à ce qu'ils répondent aux exigences applicables.

Bien que l'approbation d'un DME reçue d'un gouvernement ou d'une autre autorité puisse offrir une certaine garantie quant à la pertinence du système, les membres devront faire preuve de diligence raisonnable et s'assurer de bien comprendre l'entente qu'ils signent avec un fournisseur de système de DME/DSE. L'entente devrait décrire en détails les services et les fonctionnalités offertes par le système de DME. L'étendue des services du fournisseur doit être adéquatement établie afin que le fournisseur soit

tenu responsable de son rendement en regard à l'entente. Les membres voudront poser les questions suivantes au fournisseur et s'assurer que l'entente sur le partage des données en tient compte :

- Quels services sont offerts?
- Quelle est la fonctionnalité du service?
- Comment le service sera-t-il documenté?
- Dans le cadre de l'entente, quels sont les rôles et les responsabilités du fournisseur, du membre et de toutes autres parties à l'entente?
- Quels sont les conditions financières? (p. ex., quel est le coût du service? Y a-t-il d'autres frais additionnels ou cachés? Y a-t-il des sanctions financières?)
- Le fournisseur est-il propriétaire du système de DME ou a-t-il l'autorisation appropriée de le vendre?)
- Comment s'effectue l'importation et l'exportation de données du système de DME?
- Quelles attentes le membre devrait-il avoir quant au rendement du système de DME?
- Quels niveaux de service le fournisseur offre-t-il?
- Quelles sont les conséquences si le fournisseur ne satisfait pas aux niveaux de service?
- Quelles sont les obligations du fournisseur en matière de soutien et de maintenance?
- Comment la sécurité du système sera-t-elle assurée?
- À quel endroit sera situé le serveur?
- Quel rapport le fournisseur doit-il donner et quand?
- Comment et quand une sauvegarde des données sera-t-elle effectuée?
- Quelles sont les dispositions prises pour la reprise des activités en cas de sinistre?
- Quelles sont les exigences en matière de matériel?
- Quelles sont les exigences en matière de logiciel?
- Comment peut-on résilier l'entente et comment la continuité des soins est-elle maintenue?

METTRE EN PLACE UNE ENTENTE ENTRE MÉDECINS POUR DES DME PARTAGÉS

Lorsqu'un membre pratique au sein d'un groupe ou d'une société de médecins, il peut être sensé d'un point de vue pratique et financier d'avoir un système de DME partagé que tous les médecins peuvent utiliser. Ce système peut ou non être intégré au système de DSE d'un hôpital, d'une région ou d'une province ou d'un territoire.

Une entente conclue au sein d'un groupe ou d'une société de médecins avec un consultant en technologies de l'information devrait faire l'objet des mêmes considérations que celles mentionnées précédemment au sujet du choix d'un fournisseur. De plus, il devrait y avoir une entente concernant le système de DME partagé entre les médecins et les professionnels de la santé formant le groupe ou la société. Une entente liée à un DME partagé peut être distincte ou être intégrée dans une entente plus large entre les médecins qui régit d'autres questions concernant la gestion du groupe, de la clinique ou d'une autre organisation (p. ex., entente de société en nom collectif ou convention d'actionnaires).

Lorsque le dossier médical d'un patient renferme des entrées de diverses personnes et peut être accédé par un certain nombre de professionnels de la santé, les questions de propriété et de sécurité deviennent beaucoup plus complexes. Outre les principes fondamentaux susmentionnés, il faut porter une attention particulière au contenu de l'entente entre médecins de façon à y prévoir que les dossiers de patients ne seront accessibles qu'aux utilisateurs autorisés et aux fins autorisées. Il sera probablement nécessaire d'envisager des mécanismes pour limiter l'accès aux médecins et au personnel qui ont besoin d'accéder à un dossier de patient donné pour la prestation de soins et d'autres fins autorisées.

ENTENTES SUR LE PARTAGE DE DONNÉES AVEC LES AUTORITÉS SANITAIRES

Dans certaines provinces et certains territoires, l'association médicale négociera une certaine forme d'entente sur le partage de données ou la gestion de l'information pour régir l'utilisation que font les médecins d'un DSE géré par une autorité sanitaire. Lorsqu'il n'y a aucune entente de gestion de l'information, les membres qui veulent devenir un utilisateur d'un système de DSE établi par une autorité sanitaire, ou lier un DME à un DSE devraient envisager de conclure une entente sur le partage des données. Les principes de cette

entente sont les mêmes que ceux abordés précédemment et à l'annexe C.

La protection des dossiers liés à l'assurance ou à l'amélioration de la qualité peut faire partie de questions particulières. Lorsqu'un comité d'amélioration de la qualité d'un hôpital constitue des dossiers aux fins d'évaluation d'événements indésirables ou de l'efficacité des pratiques et des procédures de l'hôpital, ces dossiers devraient être séparés des autres dossiers afin qu'ils puissent bénéficier des protections législatives empêchant leur divulgation. L'entente sur le partage des données devrait stipuler la manière dont les dossiers seront séparés des autres dossiers et dont l'accès aux dossiers sera limité. À titre d'exemple, l'entente sur le partage des données devrait énoncer que cette information (c.à-d. l'information personnelle et l'information sur l'amélioration et l'assurance de la qualité) ne sera pas divulguée à moins que la loi ne l'exige.

Il faut aussi se demander dans ce contexte si les renseignements personnels d'un médecin (contenus dans un DSE) seront divulgués au Collège de ce médecin ou à un autre organisme d'enquête (p. ex, dans le cadre d'une vérification de la facturation).

PROTECTION CONTRE LA RESPONSABILITÉ LORS DU PARTAGE DE RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ

Un certain nombre de dispositions peuvent et devraient être intégrées dans toute entente sur le partage de données ou entente entre médecins afin de minimiser le risque de responsabilité dans un contexte de DME/DSE, notamment sur les questions suivantes :

- Indemnisation;
- Limitation de la responsabilité;
- Représentations (déclarations) et garanties;
- Règlement des litiges; et
- Compétence juridictionnelle.

Ces dispositions sont décrites en détails à l'annexe C.

RÉSILIATION D'UNE ENTENTE ET CONTINUITÉ DES OPÉRATIONS

Il est possible qu'un jour les parties conviennent mutuellement de mettre fin à une entente sur le partage de données ou une entente entre médecins (p. ex., un groupe de médecins peut être dissous). L'entente peut aussi être résiliée en raison d'un manquement ou d'une insolvabilité de la part des autres parties.

De nombreuses autres raisons peuvent expliquer la fin de la participation d'un membre à un système de DME/DSE (p. ex., départ de la province ou du territoire, ou arrêt de la pratique de la médecine à la suite d'une incapacité ou d'un décès). Les membres devraient s'assurer que leur entente sur le partage des données ou entente entre médecins comporte une clause permettant la résiliation sans raison, simplement sur avis aux autres parties.

Les indemnités et les obligations en matière de confidentialité prévues dans l'entente doivent continuer de s'appliquer malgré la résiliation. Les membres doivent aussi s'assurer d'avoir un accès continu aux renseignements contenus dans le DME/DSE conformément à leurs obligations en matière de conservation des dossiers. Même si un membre ne pratique plus la médecine, des patients peuvent lui demander un accès à leurs dossiers médicaux. Les membres pourraient aussi avoir besoin des dossiers dans le cadre d'une question médico-légale. L'entente devrait exiger que les dépositaires des dossiers les gardent dans leur état original et prennent des mesures raisonnables pour empêcher la perte, le vol des renseignements ou un accès inapproprié à l'information. Des dispositions devraient être prévues pour veiller à ce que les dossiers originaux soient détruits de manière appropriée à la fin de la période de conservation applicable.

Les membres devraient s'assurer que leur entente sur le partage des données ou entente entre médecins comporte une clause permettant la résiliation sans raison, simplement sur avis aux autres parties.

Les nouveaux enjeux

- Les membres voudront faire preuve de prudence s'ils se fient exclusivement aux renseignements contenus dans un dossier de santé électronique sur Internet, notamment s'il a été créé par le patient.

Les médecins au Canada constatent que la technologie joue un rôle grandissant dans la gestion des renseignements sur la santé des patients. Les DME et les DSE continueront probablement d'offrir de nouvelles fonctionnalités, notamment l'utilisation de portails où les patients peuvent avoir accès à leurs renseignements, interagir avec des professionnels de la santé et possiblement téléverser des données. Au-delà des DME et des DSE, les produits sur Internet qui facilitent la création de dossiers de santé par les patients font rapidement leur entrée dans le marché. Bien qu'elles reposent sur de bonnes intentions, ces innovations soulèvent des questions médico-légales imprévues qui devront être abordées.

DOSSIERS DE SANTÉ PERSONNELS DU PATIENT ET PORTAILS DES PATIENTS

Contrairement à un DME ou à un DSE qui est habituellement créé et géré par un professionnel de la santé ou un établissement de santé, le dossier de santé personnel du patient fait souvent référence à une compilation de renseignements (y compris les antécédents médicaux, les médicaments pris et les allergies) que le patient a personnellement réunis et gérés à l'aide d'un service ou d'un outil offert par un tiers. Certaines de ces applications offrent un outil d'auto-diagnostic utilisant d'autres renseignements trouvés sur Internet portant sur les symptômes, les causes et les traitements.

Les patients peuvent choisir de donner accès à leur dossier de santé en ligne à des médecins ou à d'autres professionnels de la santé. De nombreux produits permettent aussi aux hôpitaux, aux cliniques, aux laboratoires, aux pharmacies et aux médecins de téléverser d'autres renseignements sur la santé dans un dossier de santé électronique créé par un patient. Les technologies émergentes peuvent permettre aux patients non seulement d'accéder à leurs renseignements en ligne, mais aussi d'interagir avec des professionnels de la santé et possiblement de téléverser des données,

comme les résultats de la mesure de la tension artérielle, de la température ou de la glycémie.

Les membres devraient faire preuve de prudence s'ils se fient exclusivement aux renseignements contenus dans un dossier de santé électronique sur Internet, notamment s'il a été créé par le patient. Dans certaines circonstances, il peut être aussi prudent de prendre des mesures pour vérifier l'exactitude et l'exhaustivité de l'information. Les dossiers de santé créés par les patients ne devraient pas remplacer les obligations du médecin de tenir des dossiers, ni l'évaluation individualisée d'un patient (y compris les questions posées directement sur les antécédents médicaux). Lorsqu'un patient demande au médecin de verser de l'information dans un dossier en ligne, le médecin devrait discuter de cette demande avec le patient, et passer minutieusement en revue les questions de consentement et de sécurité.

Les médecins peuvent choisir de créer un site Web accessible par leurs patients et/ou d'autres professionnels de la santé. Bien que de tels sites Web offrent quasiment des possibilités d'utilisation illimitées, bon nombre d'entre eux servent de moyen de communication avec les patients. Certains des sites de médecins et des services Internet des patients les plus perfectionnés offrent des outils qui permettent de faciliter et de surveiller le suivi des soins (p. ex., la prise en charge des maladies chroniques). Ces outils permettent en général au patient d'entrer ses renseignements sur la santé par l'intermédiaire d'un portail Web sécurisé aux fins d'examen et de suivi par le médecin. Le médecin peut réagir aux données entrées en communiquant avec le patient à l'aide d'alertes envoyées par courriel ou d'une messagerie sécurisée.

Les avancées technologiques en matière de portails et de dossiers de patients sur Internet nécessiteront une analyse de questions telles que la protection des renseignements personnels, la sécurité et l'intégrité de ces dossiers. Il faut étudier plus à fond dans quelle mesure les médecins peuvent se fier à l'information obtenue dans les communications avec le patient ou les dossiers créés par le patient, permettre une interconnexion entre ces dossiers et les DME/DSE, et considérer que ces modes de communication sont assez sécuritaires.

Conclusion

Les dossiers électroniques possèdent le potentiel d'améliorer la prise en charge des patients ainsi que l'efficacité du système de santé dans son ensemble. Ce potentiel est encourageant, mais la mise en place et l'utilisation des dossiers électroniques dans la pratique médicale sont source de complexité.

Avant d'entamer le processus de conversion aux dossiers électroniques, les médecins seraient bien avisés de se familiariser avec les lois, les exigences des Collèges, les conventions en matière de protection des renseignements personnels, les règles et toutes attentes qui s'appliquent à l'utilisation des dossiers électroniques. D'autres questions importantes, telles que l'accès et la sécurité, l'intégrité des données, le consentement et les ententes sur le partage de données, devraient être examinées et évaluées en profondeur avant la mise en place des dossiers électroniques.

Il y a une multiplicité de lois sur la protection des renseignements personnels au Canada. Seulement certaines d'entre elles abordent directement les renseignements personnels sur la santé, et elles sont encore moins nombreuses à régir spécifiquement l'utilisation des dossiers électroniques. Il est à souhaiter qu'avec le temps un cadre législatif uniforme sera mis en place et s'appliquera à tous les renseignements personnels sur la santé, peu importe la manière dont ils sont conservés. L'ACPM continue de travailler avec des partenaires afin d'examiner cette question et d'autres questions émergentes. Entre-temps, les médecins devraient s'assurer de connaître les dispositions applicables dans leur province ou territoire.

L'ACPM encourage ses membres à être à l'affût de ses publications sur ce sujet et à communiquer avec l'Association s'ils ont des questions ou des préoccupations concernant l'adoption et la mise en place de DME ou de DSE.



Annexe A – Glossaire

| | |
|--|--|
| Chiffrement | Transformation de l'information dans un format inintelligible pour les personnes qui ne possèdent pas les connaissances ou l'autorisation pour la déchiffrer, comme un flux confus de symboles en apparence aléatoires. |
| Communication préalable électronique | Présentation de données électroniques dans le cadre d'une action en justice. |
| Dépositaire (des DME/DSE) | Responsable des tâches associées à la collecte, à l'utilisation et à la divulgation des renseignements (dans un DME/DSE). |
| Dispositif portable de stockage des données | Tout dispositif électronique portable permettant le stockage de données, comme un portable, un téléphone cellulaire, un assistant numérique personnel, une clé USB ou un disque dur portatif. |
| DME partagé | Dossier médical électronique centralisé qui permet à un certain nombre d'utilisateurs (p. ex., les médecins traitants, d'autres professionnels de la santé, les gestionnaires d'information) d'avoir accès à l'ensemble ou à une partie du dossier d'un patient. |
| Dossier de santé électronique (DSE) | Compilation de données de base sur la santé fournies par divers professionnels et organisations de la santé, accessibles par de nombreuses parties autorisées à partir d'un certain nombre de points de service, peut-être même à partir de différentes provinces ou différents territoires. |
| Dossier de santé personnel du patient | Dossier électronique généralement créé et mis à jour par le patient, parfois à l'aide d'un service en ligne offert par un tiers. À la différence des DME/DSE, qui sont en général créés et mis à jour par un professionnel de la santé ou un établissement de santé, le terme « dossier de santé personnel du patient » fait référence à une compilation de renseignements réunis personnellement et gérés par le patient concernant sa santé. Le patient contrôle l'accès au dossier et l'information qui y est versée. |
| Dossier médical électronique (DME) | Version électronique du dossier papier que les médecins ont traditionnellement utilisé pour consigner les renseignements sur leurs patients et qui n'est en général accessible que dans l'établissement ou le cabinet qui en a le contrôle. Il faut faire la distinction entre un « DME simple », qui fait souvent référence à un dossier électronique créé et géré par un seul médecin dans une pratique en cabinet, et un « DME partagé » (voir ci-dessus) ou le « DSE » (voir cidessous). |
| Ensemble de données de base | Sous-ensemble de renseignements sur la santé requis pour le traitement d'un patient et créé aux fins du partage de données précises entre les professionnels de la santé. (Peut aussi être appelé « ensemble de données cliniques », « ensemble de données sur la patient », « dossier sur la continuité des soins », « résumé médical électronique », « profil de santé du patient à partager », « profil cumulatif du patient » et « registre principal des patients ».) |
| Entente entre médecins | Entente entre médecins, dans le contexte d'un groupe de médecins ou dans une société de médecins, qui établit de quelle manière l'information versée dans un DME partagé sera gérée. |
| Entente sur le partage des données | Entente entre un professionnel de la santé, ou un groupe de professionnels, et un établissement, une autorité sanitaire ou un fournisseur de service, dans le cadre de laquelle l'utilisation de l'information électronique sur la santé et l'accès à celle-ci peuvent être partagés. |
| Évaluation des facteurs relatifs à la vie privée | Procédé de gestion des risques qui permet de relever les risques réels et potentiels en matière de protection des renseignements personnels en lien avec la mise en place d'un système d'information. |

| | |
|---|---|
| Gestion des données | Responsabilité de gérer et de protéger de manière appropriée les données faisant partie d'un DME/DSE. |
| Intégrité des données | Protection de l'information de sorte qu'elle demeure inchangée et authentique. |
| Licence | Accord juridique régissant l'utilisation et la distribution d'un logiciel protégé par des droits d'auteur, y compris l'imposition de restrictions aux personnes qui utilisent le logiciel et d'obligations juridiques pour les concepteurs et les utilisateurs du logiciel. |
| Masquage | Dissimulation des renseignements personnels sur la santé d'un patient, ou de parties de ceux-ci, à la demande expresse du patient en vue de limiter ou de contrôler l'information divulguée à d'autres professionnels de la santé. (Terme souvent utilisé de manière interchangeable avec le concept de « verrouillage » ci-dessous.) |
| Métadonnée | Renseignements de base électroniques obtenus lors de la création et de la gestion d'un dossier électronique, p. ex, les dates et les heures des ajouts et des suppressions, les détails de l'accès par les utilisateurs. |
| Piste de vérification | Information sur l'historique d'un document électronique, incluant souvent des détails sur les ajouts, les suppressions ou les autres modifications apportées aux données. |
| Propriété (des DME /DSE) | Concept de garde juridique et du contrôle d'un système de DME/DSE et des données qu'il contient, même si un certain nombre d'utilisateurs ont le droit d'y contribuer et d'y tirer de l'information. |
| Reconnaissance optique de caractères (ROC) | Processus technologique qui convertit l'image d'un texte manuscrit ou typographié en texte pouvant être modifié, faire l'objet de recherche ou être manipulé d'autre façon. |
| Signature électronique | Terme générique faisant référence à un grand nombre d'options de signature non manuscrite. Une signature électronique peut être une série de lettres, de caractères, de chiffres ou de symboles en format numérique, jointe ou associée à un document électronique. |
| Signature numérique | Forme sécurisée d'une signature électronique où l'identité du signataire ainsi que l'authenticité et l'intégrité du document peuvent être vérifiées (p. ex., l'image numérisée d'une signature manuscrite saisie à l'aide d'une tablette de signature, l'utilisation d'un certificat de signature numérique doté d'une clé privée). |
| Utilisation secondaire | Utilisation de renseignements personnels sur la santé à d'autres fins que la prestation de soins de santé, notamment pour la recherche ou la planification des systèmes de santé. |
| Vérification de la protection des renseignements personnels | Examen et évaluation périodiques pour veiller à l'efficacité des contrôles de protection des renseignements personnels. |
| Verrouillage | (Peut aussi être appelé « coffre-fort » ou « verrou ») Dispositif de sécurité qui permet, à la demande expresse du patient, de limiter l'accès aux renseignements personnels sur la santé d'un patient, ou à une partie de ceux-ci, à certains utilisateurs. (Terme souvent utilisé de manière interchangeable avec le concept de « masquage » susmentionné.) |

Annexe B – Ressources complémentaires

La liste qui suit n'est pas exhaustive, mais offre de simples suggestions d'ouvrages que les médecins peuvent consulter au sujet des DME/DSE.

DOCUMENTS DE L'ACPM (accessibles en ligne au www.cmpa-acpm.ca)

Les dossiers de santé électroniques : perspective de la responsabilité médicale
ACPM, août 2008

Comment minimiser les risques médico-légaux découlant de la technologie,
Bulletin d'information de l'ACPM, juin 2008, IS0884-F

Problèmes médico-légaux découlant des nouvelles technologies en soins de santé
Bulletin d'information de l'ACPM, décembre 2007, IS0777-F

Protection des renseignements électroniques confidentiels sur la santé – le recours aux technologies de chiffrement
Bulletin d'information de l'ACPM, septembre 2007, IS0771-F

Que faites-vous pour assurer la protection de la vie privée?
Bulletin d'information de l'ACPM, décembre 2006 - volume 21, numéro 4, (révisé en avril 2008), IL0640-1-F

Protection des renseignements médicaux personnels enregistrés sur disque dur
Bulletin d'information de l'ACPM, octobre 2003 – volume 18, numéro 3, (révisé en mars 2008), IL0330-1-F

Utilisation du courrier électronique dans les communications avec les patients : les risques juridiques
Bulletin d'information de l'ACPM, mars 2005 – volume 20, numéro 1, (révisé en juin 2009), IS0586-F

AUTRES RESSOURCES

Canada

Inforoute Santé du Canada www.infoway-inforoute.ca

Association médicale canadienne www.cma.ca
Consulter les rapports de recherche sur les technologies de l'information sur la santé, y compris l'orientation sur l'adoption du DME.

Canadian EMR www.canadianemr.ca
Site privé de ressources destinées aux médecins, au personnel, aux fournisseurs et autres intervenants au sujet des systèmes de DME.

Le Collège des médecins de famille du Canada www.cfcp.ca
La Trousse d'outils en soins de première ligne pour les médecins de famille a une section « Technologie de l'information », qui renferme de l'information et des ressources sur les dossiers électroniques.

Colombie-Britannique

College of Physicians and Surgeons of British Columbia www.cpsbc.ca
Consulter le manuel de ressources pour obtenir une orientation sur les dossiers médicaux électroniques et la propriété des données.

British Columbia Medical Association www.bcma.org
Consulter les énoncés de politique sur la gestion et la technologie de l'information sur la santé.

Physician Information Technology Office www.pito.bc.ca
Initiative conjointe de l'association médicale et le ministère de la Santé de la Colombie-Britannique en vue d'aider les médecins qui mettent en place des DME dans leur pratique.

Society of General Practitioners of BC www.sgp.bc.ca
La section bibliothèque comprend des documents sur les questions connexes aux technologies de l'information, y compris les DME et le Physician Information Technology Office.

Office of the Information and Privacy Commissioner for British Columbia www.oipcbc.org

Surveille et applique la loi sur la protection des renseignements personnels et offre des ressources aux médecins.

British Columbia Ministry of Health Services - eHealth www.health.gov.bc.ca/ehealth

Aperçu des projets de cybersanté en Colombie-Britannique.

Alberta

College of Physicians and Surgeons of Alberta www.cpsa.ab.ca

Consulter la section sur la propriété des données, notamment les documents *CPSA Data Stewardship Framework* et *CPSA Data Sharing Principles - Information Sharing Agreements*.

Alberta Medical Association www.albertadoctors.org

La section sur le « Computerized Office » donne de l'information sur les choix de DME (y compris les DME partagés) et l'initiative de l'Alberta en matière de DSE.

Physician Office System Program www.posp.ab.ca

Initiative conjointe du ministère de la Santé et du Bien-être, de l'association médicale et des services de santé de l'Alberta visant à aider les médecins à mettre en place des DME dans leur pratique et à assurer une interopérabilité avec l'infrastructure provinciale de gestion de l'information sur la santé.

Office of the Information and Privacy Commissioner of Alberta www.oipc.ab.ca

Surveille et applique la loi sur les renseignements sur la santé et fournit de l'information sur la conformité des dépositaires.

Alberta Netcare www.albertanetcare.ca

Organisme responsable de la mise en place d'un DSE dans l'ensemble de la province.

Saskatchewan

College of Physicians and Surgeons of Saskatchewan www.quadrant.net/cps/

Consulter les règlements sur les dossiers médicaux.

Saskatchewan Medical Association Privacy Toolkit www.sma.sk.ca/privacy/

Trousse produite conjointement avec le Collège des médecins et des chirurgiens de la Saskatchewan et donnant une orientation et des formulaires types aux fins de conformité avec la loi sur la protection des renseignements personnels.

Office of the Saskatchewan Information and Privacy Commissioner www.oipc.sk.ca

Surveille et applique la loi sur la protection des renseignements sur la santé et offre des ressources sur la manière d'effectuer des évaluations des facteurs relatifs à la vie privée.

Office of the Saskatchewan Information and Privacy Commissioner www.oipc.sk.ca

Monitors and enforces the Health Information Protection Act and includes resources for conducting privacy impact assessments.

Saskatchewan Ministry of Health - Health Information Solutions Centre www.health.gov.sk.ca/health-information-solutions-centre

Aperçu des projets de cybersanté en Saskatchewan.

Manitoba

College of Physicians and Surgeons of Manitoba www.cpsm.mb.ca

Consulter les énoncés et les lignes directrices sur les dossiers médicaux et les systèmes informatiques médicaux.

Manitoba eHealth www.manitoba-ehealth.ca

Le site Web a une section « Médecins » destinée aux médecins qui offre des ressources aux médecins dans les collectivités et aux professionnels des soins de santé primaires.

Manitoba Ombudsman www.ombudsman.mb.ca

La Division de l'accès à l'information et de la protection de la vie privée est chargée de l'application de la Loi sur les renseignements médicaux personnels et offre des ressources notamment de l'orientation sur l'envoi par courrier électronique de renseignements personnels sur la santé.

Manitoba eHealth www.manitoba-ehealth.ca

Aperçu des projets de cybersanté du Manitoba, y compris une section destinée aux médecins et portant sur la mise en place des DME.

Ontario

Ordre des médecins et chirurgiens de l'Ontario www.cpso.on.ca

Consulter la politique sur les dossiers médicaux, y compris les dossiers électroniques.

OntarioMD www.ontariomd.ca

Filiale de l'association médicale de l'Ontario qui fournit aux médecins des renseignements et de l'aide en matière d'adoption de technologies de l'information. Le site donne accès à EMRadvisor.ca, lequel offre de la recherche et une communication entre pairs sur l'adoption de DME.

cyberSanté Ontario www.ehealthontario.on.ca

Agence gouvernementale chargée de la mise en place de technologies de l'information dans le domaine des soins de santé.

Commissaire à l'information et la protection de la vie privée de l'Ontario www.ipc.on.ca

Chargé de la surveillance et l'application de la Loi sur la protection des renseignements personnels sur la santé. Parmi les ressources offertes : boîte à outils, orientation sur les évaluations des facteurs liés à la vie privée, et des feuille-info sur la destruction sécurisée des renseignements personnels, le verrouillage et le chiffrement dans les appareils mobiles.

Québec

Collège des médecins du Québec www.cmq.org

Consulter le guide sur les dossiers médicaux, y compris les dossiers et les communications électroniques.

Dossier de santé www.dossierdesante.gouv.qc.ca

Chargé de l'élaboration du dossier de santé électronique du Québec.

Nouveau-Brunswick

Collège des médecins et chirurgiens du Nouveau-Brunswick www.cpsnb.org

Consulter les règlements et les lignes directrices sur les dossiers médicaux.

Nouvelle-Écosse

College of Physicians and Surgeons of Nova Scotia www.cpsns.ns.ca

Consulter les lignes directrices sur les dossiers médicaux.

Nova Scotia Department of Health - Electronic Medical Records (eResults) www.gov.ns.ca/health/eResults

Le site contient des renseignements sur un programme de gestion de l'information en soins de santé primaires pour la mise en place de systèmes de DME.

Île-du-Prince-Édouard

College of Physicians and Surgeons of Prince Edward Island www.cpspei.ca

Consulter la politique sur les principes de protection des renseignements personnels.

Terre-Neuve-et-Labrador

College of Physicians and Surgeons of Newfoundland & Labrador www.nmb.ca

Consulter les règlements et les lignes directrices sur les dossiers médicaux.

Newfoundland & Labrador Centre for Health Information www.nlchi.nl.ca

Ce centre est chargé de l'élaboration d'une infrastructure pour les technologies de l'information sur la santé, y compris un DSE pour l'ensemble de la province. Le site Web a une section sur les ressources liées au DME.

Annexe C – Ententes sur le partage de données

Principes applicables aux dossiers médicaux électroniques/dossiers de santé électroniques (août 2008)

INTRODUCTION

Le présent document a pour but d'identifier, de façon générale, les grandes questions auxquelles devrait s'attarder tout médecin qui s'apprête à signer une entente portant sur un système de dossier médical électronique (DME) ou de dossier de santé électronique (DSE) ainsi que les principes juridiques applicables. Le DME/DSE fait habituellement référence à l'entreposage électronique unique et centralisé des dossiers médicaux, assorti de règles définissant les droits d'accès et d'utilisation des renseignements sur la santé des patients. Tout fournisseur de service de soins de santé, ou dépositaire de renseignements sur la santé, a accès à une partie ou à la totalité du dossier médical pour prodiguer des soins au patient.

Ce document tient compte du fait que les questions relatives au partage d'information électronique peuvent être soulevées dans plusieurs types d'ententes utilisées pour mettre en œuvre un système de DME/DSE. Par exemple, les questions relatives au partage d'information électronique peuvent être soulevées lorsque des médecins créent un DME à l'usage d'un groupe de médecins, lorsque des médecins négocient avec une agence gouvernementale de santé pour la création d'un DSE à l'échelle d'une région et lorsque des médecins négocient la création d'un DME avec un fournisseur de services (p. ex., matériel, logiciel ou service d'hébergement). Ce document a pour but d'identifier les principes pertinents au partage d'information électronique dans de multiples contextes, sans égard au type de contrat considéré.

Les questions et les principes dont fait état le présent document ne sont pas exhaustifs et ce dernier n'a pas pour but de présenter des conclusions quant aux risques ou avantages potentiels de la participation à un système de DME/DSE. Chaque médecin devra évaluer les risques et avantages dans le cadre de ses conditions individuelles. En tant que dépositaire d'information très délicate, le médecin devra considérer soigneusement dans quelle mesure les renseignements sur le patient seront divulgués à partir du système de DME/DSE. Lorsque ces renseignements délicats sont partagés dans le cadre d'un système de DME/DSE, il est impératif qu'une entente détermine qui sera responsable d'assurer la sécurité et la confidentialité de l'information. Le médecin devra également décider de la manière d'obtenir le consentement du patient pour l'utilisation et la divulgation de ses renseignements de santé au moyen du DME/DSE.

Le présent document n'est produit qu'à titre d'information et de texte de référence général. Il ne doit pas être utilisé comme source de conseils juridiques ou financiers, ni remplacer les conseils d'un avocat ou de tout autre professionnel. Chaque entente devrait être revue par le conseiller juridique et les autres conseillers professionnels du médecin.

Bien que ces principes visent à donner une orientation aux médecins, l'ACPM espère qu'ils aideront tous les participants à aborder les questions de gestion d'information liées aux systèmes de DME complexes ou de DSE.

APPROCHES CONTRACTUELLES

La mise en place d'un système de DME/DSE peut se faire au moyen de diverses approches et arrangements contractuels. Puisqu'il est impossible de se pencher sur toutes les approches possibles, ce document vise à identifier les questions et les principes les plus pertinents sans égard au type d'arrangement contractuel.

1. Médecins, groupes de médecins et sociétés de médecins

Les médecins peuvent s'organiser de plusieurs façons pour les fins d'un contrat de DME/DSE.

En voici quelques-unes :

- 1.1 un médecin individuel (un « médecin exerçant seul ») qui agit à son propre titre;
- 1.2 un groupe non incorporé de médecins (un « groupe de médecins ») qui peut inclure :
 - (a) un groupe de partage de garde;
 - (b) une clinique au sein de laquelle les médecins partagent les mêmes dossiers; ou
 - (c) un groupe de médecine familiale ou un réseau de médecine familiale; et
- 1.3 une société de médecins (une « société »), qui peut être une société par action ou une société en nom collectif.

2. Fournisseurs de service, régions sanitaires et centres hospitaliers

Les parties avec lesquelles chacune des entités ci-dessus peut signer un contrat pour un système de DME/DSE incluent :

- 2.1 un vendeur ou un autre fournisseur de service (p. ex., logiciel, matériel, ASP, hébergement) (« fournisseur de service »);
- 2.2 une agence de santé et de services sociaux, ou une organisation comme un office régional de la santé ou un réseau local d'intégration des services de santé ou un ministère (« région sanitaire »); ou
- 2.3 un centre hospitalier (« hôpital »).

3. Les contrats

Les ententes suivantes devraient être élaborées en tenant compte des principes établis dans le présent document :

- 3.1 « Entente sur le partage de données » — entente entre un médecin exerçant seul, un groupe de médecins ou une société de médecins, d'une part, et un fournisseur de service, une région sanitaire ou un hôpital, d'autre part;
- 3.2 « Entente entre médecins » — dans cette forme d'entente, un médecin signera un contrat avec d'autres médecins. Ce type d'entente comprend les ententes entre membres d'un groupe de médecins ou d'une société de médecins. L'entente peut porter uniquement sur la façon de gérer le système de DME auquel les médecins participent. Les principes peuvent également être intégrés à une entente plus large, qui régit les questions relatives à la gestion de la pratique de groupe, la clinique ou la société (p. ex., entente de société en nom collectif, convention d'actionnaires).

LES PRINCIPES

Ce document donne un aperçu des principes dont on devrait tenir compte dans l'élaboration de toute entente sur le partage de données ou de toute entente entre médecins :

1. Gestion et propriété des données

1.1 Ce dont il s'agit :

Depuis de nombreuses années, les tribunaux considèrent que le médecin, l'établissement ou la clinique qui constitue les dossiers médicaux est également propriétaire des dossiers physiques (*McInerney c. MacDonald*, 1992). Le propriétaire des dossiers médicaux contrôle historiquement les questions d'accès et de conservation. Dans le cadre d'un DME/DSE, il y a mélange de données provenant de plusieurs sources, ce qui complique la question des droits de propriété, de l'accès et de la conservation.

L'entente sur le partage de données peut également régir la question des droits de propriété intellectuelle du système de DME/DSE.

1.2 En quoi est-ce important :

La perspective historique des droits de propriété sur les dossiers médicaux est dépassée par les DME/DSE qui vont plus loin que le modèle traditionnel du dossier médical sauvegardé et contrôlé par un seul médecin ou groupe de médecins. Le système de DME/DSE se caractérise par le partage du contrôle de l'information dans le dossier en fonction de son origine. Dans ce contexte, il est difficile d'appliquer le concept traditionnel des droits de propriété.

Même si l'entente sur le partage de données peut également traiter de la propriété des dossiers, son but premier doit être d'assurer que le médecin a un droit d'accès approprié aux renseignements personnels sur la santé, et qu'il peut permettre à ses patients d'avoir accès à leur dossier médical.

1.3 Recommandations :

L'entente sur le partage de données et l'entente entre médecins devrait énoncer explicitement qu'aucune de ses dispositions n'empêche ou ne fait obstacle à la capacité du médecin :

- (i) de se conformer à ses obligations à l'égard du dossier médical;
- (ii) d'avoir accès à ses dossiers comme le prévoit la présente entente; ou
- (iii) de confier les données à un autre fournisseur de service en cas de résiliation de l'entente sur le partage de données.

Il peut arriver que le DME/DSE soit considéré un bien qui pourrait être grevé par son propriétaire, par exemple, pour le donner en garantie en faveur d'un tiers. Le fournisseur de service, la région sanitaire ou l'hôpital doit être tenu de garantir que le médecin pourrait continuer de se conformer à ses obligations et droits susmentionnés, quel que soit l'intérêt que pourrait réclamer un tiers sur le système de DME/DSE.

2. Confidentialité et vie privée

2.1 Ce dont il s'agit :

Selon leur code de déontologie, les médecins ont l'obligation de préserver la confidentialité des renseignements de leurs patients. Dans la plupart des provinces et des territoires, les médecins et autres dépositaires de renseignements et de renseignements personnels sur la santé sont également soumis aux obligations que leur imposent les lois en matière de protection des renseignements personnels.

Que ce soit en vertu d'une loi sur la protection des renseignements personnels, du droit civil ou de la common law, les patients ont en général un droit d'accès à leurs renseignements médicaux et le droit de s'assurer que leurs renseignements demeurent confidentiels.

2.2 En quoi est-ce important :

Lorsque des renseignements médicaux personnels sont entreposés dans un système de DME/DSE, de nombreuses personnes y ont accès outre le médecin qui les a versés au système. En raison de leur obligation de confidentialité ou des exigences que leur imposent les lois en matière de protection des renseignements personnels, les médecins peuvent avoir l'obligation de contrôler l'accès aux renseignements médicaux personnels qu'ils ont entreposés dans le système de DME/DSE.

Les médecins ont aussi l'obligation de s'assurer que leurs patients peuvent consulter leurs dossiers médicaux.

2.3 Recommandations :

Toute entente sur le partage des données et toute entente entre médecins doivent expressément permettre aux médecins de se conformer aux lois et règlements pertinents en matière de protection des renseignements personnels, au droit civil, à la common law et aux politiques des organismes de réglementation provinciaux ou territoriaux (collèges) qui régissent la confidentialité des renseignements des patients.

L'entente sur le partage des données doit préciser quels renseignements du patient peuvent être recueillis, utilisés et divulgués en vertu d'un consentement implicite. L'entente sur le partage des données devrait aussi préciser que la loi applicable en matière de protection des renseignements pertinents exige le consentement explicite pour l'utilisation ou la divulgation de certains renseignements, le cas échéant. De même, l'entente sur le partage des données doit indiquer quels renseignements du patient peuvent être recueillis, utilisés et divulgués sans le consentement du patient. L'entente sur le partage des données doit interdire toute collecte, utilisation ou divulgation qui n'est pas permise par la loi.

Les ententes sur le partage de données et les ententes entre médecins ne doivent imposer aucune contrainte à la capacité d'un médecin de remplir ses obligations législatives de divulguer des

renseignements confidentiels, comme l'obligation de signaler la violence faite aux enfants, l'inaptitude à conduire ou toute autre obligation.

Toute entente sur le partage de données et toute entente entre médecins doivent prévoir comment le patient pourra avoir accès à ses propres renseignements médicaux.

3. Sécurité et accès au système de DME/DSE

3.1 Ce dont il s'agit :

La plupart des lois en matière de protection des renseignements personnels exigent que les dépositaires des renseignements médicaux personnels prennent toutes les précautions nécessaires pour minimiser les risques de perte, de vol ou d'accès non autorisé à ces renseignements. Ces exigences sont conformes à l'obligation de confidentialité du médecin. Dans certaines provinces et certains territoires, le médecin peut avoir l'obligation d'aviser ses patients d'un bris de sécurité.

3.2 En quoi est-ce important :

Le médecin devra se conformer à toutes les obligations juridiques et déontologiques pertinentes en matière de sécurité des renseignements médicaux personnels conservés au moyen d'un système de DME/DSE.

3.3 Recommandations :

L'entente sur le partage de données devrait prévoir des protocoles de sécurité appropriés pour donner accès à l'information à ceux qui en ont besoin pour soigner le patient ou à d'autres fins autorisées par les lois en matière de protection des renseignements personnels.

L'entente sur le partage de données devrait prévoir des mécanismes pour assurer qu'aucune personne non autorisée n'ait accès à l'information ou que personne n'y ait accès à des fins non autorisées. Le médecin doit être avisé de tout bris de sécurité. L'entente sur le partage de données doit préciser la manière d'en aviser les patients, lorsqu'un avis est requis.

Si les lois en matière de protection de renseignements personnels prévoient que le patient puisse limiter l'accès à ses renseignements personnels sur la santé contenus dans un système DME/DSE, l'entente sur le partage de données devra préciser la manière de mettre en œuvre de telles restrictions.

4. Exactitude et qualité des données

4.1 Ce dont il s'agit :

Le médecin et les membres de son personnel qui faisaient usage d'un dossier médical papier étaient les seuls professionnels à utiliser l'information qu'il contenait. Ce n'est pas le cas des systèmes de DME/DSE, que de nombreux professionnels de la santé peuvent consulter. Ces professionnels de la santé peuvent se fier à de l'information que renferme le DME/DES pour soigner le patient sans consulter le médecin qui a consigné l'information.

De plus, la plupart des lois en matière de protection des renseignements personnels exigent des dépositaires qu'ils maintiennent une information exacte.

4.2 En quoi est-ce important :

Les professionnels de la santé doivent pouvoir se fier aux renseignements entreposés dans le système de DME/DSE. L'importance que le DME/DES contienne de l'information exacte est accrue lorsque les professionnels de la santé qui s'y fient ne se consultent pas régulièrement ou pas du tout.

4.3 Recommandation :

Toute entente sur le partage de données doit prévoir des mécanismes pour assurer l'exactitude et l'actualité des données conservées dans le système de DME/DSE. Cela inclut les mécanismes nécessaires pour modifier l'information conformément aux exigences prescrites, et pour signaler aux utilisateurs qu'ils auraient consulté de l'information désuète ou erronée, le cas échéant.

5. Exigences en matière de tenue des dossiers

5.1 Ce dont il s'agit :

Il y a dans la plupart des provinces et territoires des exigences réglementaires ou légales qui régissent la création, la conservation et la destruction des dossiers médicaux. On prévoit parfois des exigences particulières applicables aux dossiers médicaux électroniques. Les dossiers médicaux contiennent également les preuves des soins fournis aux patients.

5.2 En quoi est-ce important :

Les médecins sont tenus de se conformer aux lois, y compris aux lois en matière de protection des renseignements personnels applicables, aux principes de droit civil, à la common law ainsi qu'aux politiques des organismes de réglementation (collèges) provinciaux ou territoriaux qui régissent la création, la tenue et la destruction des dossiers médicaux.

Les médecins devraient avoir accès au système de DME/DSE pendant la période de conservation précisée par le Collège ou par règlement. Bien que la période de conservation varie d'une province ou d'un territoire à l'autre, l'ACPM recommande que ses membres conservent les dossiers cliniques pendant au moins dix ans à compter de la date de la dernière entrée ou pour une période d'au moins dix ans à compter de l'âge de la majorité, pour les mineurs. La recommandation de l'ACPM vise une période de conservation qui est la même, ou plus longue, que celle qui est requise dans la plupart des provinces et territoires. Toutefois, en Ontario, le Collège recommande que les médecins conservent les dossiers médicaux pendant au moins 15 ans.

5.3 Recommandations :

L'entente sur le partage de données doit permettre aux médecins de se conformer au droit applicable en matière de création, de conservation et de destruction des dossiers médicaux.

Elle ne doit pas limiter, enfreindre ou nuire au droit du médecin de demander des conseils médico-légaux à l'ACPM ou à un avocat, ou aux deux.

Lorsqu'un médecin est impliqué dans une affaire médico-légale, il voudra s'assurer qu'il aura à sa disposition un dossier des soins fournis au patient. Les documents doivent être créés, mis à jour ou conservés dans le but de satisfaire aux exigences des tribunaux à l'égard de l'intégrité des documents introduits en preuve et du processus de création. Les dossiers doivent être conservés pendant une période qui correspond aux exigences en matière de conservation des dossiers et mis à la disposition du médecin en cas de question médico-légale. L'entente sur le partage de données doit également traiter de la destruction des dossiers à la fin de la période de conservation. Elle doit assurer qu'au moment où il faut les détruire, les dossiers sont détruits d'une façon appropriée (p. ex., destruction physique des unités de disque dur, des systèmes de sauvegarde).

L'entente sur le partage de données doit préciser quelle information sera versée au système de DME/DSE afin que le contenu et le format des données se conforment aux exigences applicables en matière de gestion des dossiers électroniques.

6. Assurance de la qualité

6.1 Ce dont il s'agit :

Les dossiers du comité de l'assurance de la qualité sont ceux préparés par un comité d'hôpital afin d'examiner les événements indésirables et d'évaluer l'efficacité des pratiques et procédures de l'hôpital.

6.2 En quoi est-ce important :

Pour qu'un programme d'assurance de la qualité soit efficace, il est généralement reconnu que les médecins et les intervenants doivent obtenir des assurances satisfaisantes que les dossiers du comité ne serviront qu'au processus d'assurance de la qualité. Les dispositions législatives qui empêchent la divulgation des dossiers d'assurance de la qualité dans le cadre des procédures judiciaires reflètent bien la politique publique d'encourager les professionnels de la santé à participer aux processus d'assurance de la qualité. De telles dispositions sont maintenant en vigueur dans l'ensemble des provinces et des territoires au Canada.

6.3 Recommandation :

L'entente sur le partage de données doit prévoir comment les dossiers d'assurance de la qualité seront séparés des autres dossiers afin d'assurer qu'ils puissent bénéficier des protections législatives applicables.

7. Étendue et fonctionnalité des services

7.1 Ce dont il s'agit :

Acquérir, exploiter et maintenir un système de DME/DSE, ainsi que l'infrastructure technique connexe, requiert un effort important. L'entente sur le partage de données doit préciser l'étendue des services auxquels s'engage le fournisseur de service, la région sanitaire ou l'hôpital en lien avec le système de DME/DSE.

7.2 En quoi est-ce important :

L'étendue des services fournis doit faire l'objet d'une entente exécutoire de sorte que le fournisseur de service, la région sanitaire ou l'hôpital, selon le cas, puisse être redevable de son rendement. Il faut faire preuve de diligence raisonnable dans le choix d'un fournisseur de service pour s'assurer qu'il est digne de confiance et expérimenté.

7.3 Recommandations :

L'entente sur le partage de données doit traiter des éléments suivants :

- (a) les caractéristiques du service offert;
- (b) la fonctionnalité du service;
- (c) la documentation;
- (d) les rôles et responsabilités des parties à l'entente;
- (e) les conditions financières;
- (f) le droit de propriété du vendeur;
- (g) l'importation et l'exportation de données du système de DME/DSE;
- (h) les attentes en matière de rendement;
- (i) les niveaux de service;
- (j) les conséquences de tout défaut d'atteindre les niveaux de service prévus;
- (k) les obligations en matière de soutien et de conservation;
- (l) la sécurité du système;
- (m) l'emplacement du serveur;
- (n) les rapports;
- (o) la sauvegarde des données;
- (p) la reprise après sinistre;
- (q) les exigences en matière de matériel; et
- (r) les exigences en matière de logiciel.

L'entente sur le partage de données doit également préciser le moyen pour le médecin, le groupe de médecins ou la société de médecins de résilier l'entente et d'assurer la transition à un autre fournisseur de service (y compris le transfert des données du système de DME/DSE) en cas d'insatisfaction à l'égard du service offert. La continuité et la qualité des soins doivent être maintenues pendant la durée d'une telle période de transition.

8. Résiliation et continuité des opérations du système médical électronique

8.1 Ce dont il s'agit :

Toute entente sur le partage de données peut être résiliée par consentement mutuel des parties ou par une partie en cas de non-respect de l'entente ou d'insolvabilité de l'autre partie. De plus, tout groupe de médecins peut être dissout. Il en va de même pour toute société de médecins.

8.2 En quoi est-ce important :

L'accès ininterrompu à l'information du système de DME/DSE est essentiel pour que le médecin puisse se conformer aux obligations qui lui incombent en matière de conservation des dossiers, décrites plus haut.

8.3 Recommandations :

Toute entente sur le partage de données et toute entente entre médecins doivent prévoir la continuité des opérations du système de DME/DSE ou alors préciser ce que deviennent les dossiers du système à la fin de l'entente sur le partage de données ou du retrait d'un médecin d'un groupe de médecins ou d'une société de médecins.

Comme nous l'expliquons plus bas, les ententes doivent prévoir la conservation des DME sous leur forme originale après la résiliation, de même que l'accès continu à ces dossiers par le médecin et le retrait possible des DME du système. Cela peut inclure de copier des dossiers médicaux de tout patient que le médecin a soigné, la mise hors service de la solution technique, l'accès aux dossiers et leur archivage éventuel, les rapports aux patients et aux autres organismes nécessaires sur la manipulation du dossier médical après la résiliation. L'entente doit traiter du départ, de la résiliation et du décès.

Le médecin voudra s'assurer que ses anciens collègues de pratique de groupe conserveront adéquatement les dossiers médicaux originaux et lui donneront accès à ces dossiers et à la piste de vérification correspondante. Le médecin voudra avoir l'assurance que les médecins qui continuent à être dépositaires du système de DME/DSE prendront toutes les mesures raisonnables pour prévenir que l'information soit perdue, volée ou consultée de façon inappropriée. Le médecin voudra également s'assurer que les dossiers originaux sont détruits après la fin de la période de conservation prescrite.

9. Résiliation pour des raisons de commodité

9.1 Ce dont il s'agit :

La résiliation pour des raisons de commodité permet à une partie à une entente de la résilier sans raison, simplement sur avis aux autres parties.

9.2 En quoi est-ce important :

Il y a de nombreuses raisons pour qu'un médecin puisse avoir à résilier sa participation à un système de DME/DSE en vertu d'une entente sur le partage de données ou d'une entente entre médecins. Entre autres, le médecin peut vouloir quitter la province ou le territoire ou cesser de pratiquer la médecine à cause d'un handicap, de son décès ou d'autres circonstances.

9.3 Recommandations :

En plus du droit de résilier l'entente sur le partage de données en cas de non-respect de l'entente ou d'insolvabilité de l'autre partie, le médecin doit s'assurer que l'entente sur le partage de données et l'entente entre médecins lui donnent le droit de résilier sa participation au système de DME/DSE sans raison en donnant avis écrit à la société de médecins, au groupe de médecins, au fournisseur de service, à la région sanitaire, à l'hôpital ou à toute autre partie concernée.

L'entente sur le partage de données doit préciser que certaines de ses dispositions concernant le médecin qui la résilie, comme les indemnités et les obligations en matière de confidentialité, survivent à la résiliation, et qu'une telle résiliation ne change en rien les droits et obligations pertinents des autres parties qui demeurent.

10. Indemnisation

10.1 Ce dont il s'agit :

L'indemnité a pour but d'allouer à une partie au contrat le risque et la responsabilité qui peuvent découler du contrat et exige habituellement que cette partie s'engage à assumer une certaine responsabilité à l'égard soit :

- (i) des aspects du contrat qui relèvent de sa responsabilité, soit; et
- (ii) des conséquences qui découlent de sa négligence, son inconduite ou le non-respect de ses obligations.

10.2 En quoi est-ce important :

La responsabilité peut émerger de plusieurs scénarios en rapport avec un système de DME/DSE dans le cadre d'une entente sur le partage de données. Par exemple, et sans limiter la généralité de ce qui précède : (i) un système de DME/DSE peut tomber en panne et le médecin ne plus avoir accès à l'information nécessaire pour soigner les patients; (ii) l'information des patients peut être divulguée ou consultée de façon indue par un tiers ou (iii) le système de DME/DSE peut contenir de l'information inexacte à laquelle un médecin ou tout autre professionnel de la santé se fie sans savoir qu'elle est erronée. Sans indemnité pour le médecin qui connaît de telles difficultés, on ne saurait comment partager la responsabilité des dommages causés à un patient dans ces cas-là.

Dans le cadre de toute entente sur le partage de données, on peut demander à un médecin d'indemniser un groupe de médecins ou une société de médecins, un fournisseur de service, une région sanitaire ou un hôpital, par exemple, s'il : (i) divulgue ou permet indûment l'accès non autorisé à l'information d'un patient ou (ii) fournit de l'information inexacte sur le patient à un système de DME/DSE.

Il est important de souligner que la partie qui indemnise est habituellement responsable d'une gamme plus étendue de dommages en vertu de l'indemnité que ce ne serait le cas si la partie ne respectait tout simplement pas le contrat.

En général, lorsqu'on considère s'engager à accorder une indemnité et qu'on évalue sa portée, on devrait prévoir que la partie qui accorde l'indemnité ne devrait être responsable que des actes ou omissions dont elle est responsable en droit, ce qui revient habituellement aux actes et omissions qui sont sous le contrôle de cette partie.

Veillez prendre note qu'un médecin peut être tenu personnellement responsable d'un dommage subi par un patient peu importe qu'il fasse partie d'un groupe de médecins ou d'une société de médecins; par conséquent, les indemnités mentionnées plus haut devraient être prévues à l'entente sur le partage de données entre la société de médecins, d'une part, et le fournisseur de service, la région sanitaire ou l'hôpital, d'autre part. L'indemnité devrait prévoir, par exemple, que l'une ou les deux parties indemniseront le médecin qui n'est pas partie à l'entente sur le partage de données. Une indemnité ne libère pas le médecin de sa responsabilité en cas de dommages causés à un patient à cause de données inaccessibles ou inexacts. Cependant, dans le cas de tels dommages et de poursuite du patient contre le médecin, cette disposition permettra au médecin de demander à l'autre partie une indemnité pour ces dommages.

10.3 Recommandations :

- (a) Tout médecin devrait demander d'être indemnisé advenant :
 - (i) toute divulgation ou utilisation inappropriée de renseignements personnels sur la santé par une société de médecins, un groupe de médecins, un fournisseur de service, une région sanitaire, un hôpital ou par toute autre partie à l'entente sur le partage de données ou toute entente entre médecins; et
 - (ii) tout défaut du système de DME/DSE qui entrainerait des dommages à un patient.
- (b) Toute indemnité accordée par un médecin, un groupe de médecins ou une société de médecins ne devrait pas dépasser la responsabilité qui découle des actes sur lesquels le médecin, le groupe de médecins ou la société de médecins (ou de actes dont ils sont responsables en droit). Toute disposition d'indemnisation doit prévoir un mécanisme d'avis et de coopération, et le droit pour chaque partie de retenir les services d'un avocat. Elle doit aussi permettre à la partie qui accorde l'indemnité d'approuver toute transaction de règlement. En cas d'indemnité, le médecin doit garder à l'esprit que l'ACPM ne se considère pas liée par une indemnité accordée à un tiers par ses membres. Cependant, lorsque l'indemnité accordée à un tiers a un rapport direct avec la pratique de la médecine ou la prestation directe de soins à un patient par un membre, ce dernier peut avoir droit à une assistance de l'ACPM pour les difficultés médico-légales qui résultent de ses actes. Les membres ne sont pas nécessairement admissibles à l'aide de l'ACPM advenant des promesses d'indemnisation en lien avec des actes administratifs et non médicaux, dont le médecin aurait assumé la responsabilité en vertu d'une entente sur le partage de données ou d'une entente entre médecins.

Dans les cas où des professionnels de la santé de plusieurs disciplines seraient partie à une entente sur le partage de données, il serait sans doute préférable de demander une indemnisation de chacun de ces professionnels.

Un médecin devrait toujours obtenir les conseils juridiques de son avocat à l'égard de toute indemnité qu'il accorde ou qu'on lui accorde. L'indemnité accordée par une société de médecins requiert une attention particulière, puisqu'elle pourrait engager la responsabilité de tous les médecins de la société. L'avocat devra étudier cette disposition dans le contexte de tout le contrat.

11. Limitation de responsabilité

11.1 Ce dont il s'agit :

Toute partie à une entente sur le partage de données ou à une entente entre médecins peut limiter sa responsabilité à l'égard des dommages qui découlent de l'application de l'entente en ajoutant une disposition qui limite sa responsabilité. Ces clauses visent généralement à limiter la responsabilité d'une partie à l'égard des dommages directs et à exclure complètement certains autres types de dommages, comme les dommages indirects, spéciaux et punitifs.

11.2 En quoi est-ce important :

Quand un médecin considère participer à un système de DME/DSE, la nature des risques et l'étendue de sa responsabilité éventuelle en lien avec cette participation ne sont pas claires. Par exemple, il est difficile de prévoir avec suffisamment d'exactitude les dommages qui pourraient être réclamés en cas de divulgation indue ou d'utilisation des renseignements personnels sur la santé. De plus, comme nous l'avons mentionné plus haut, les pannes de matériel et de logiciel causant l'« interruption » du système de DME/DSE peuvent donner lieu à une responsabilité civile.

Une clause visant à restreindre la responsabilité d'un fournisseur de service, d'une région sanitaire ou d'un hôpital peut limiter le droit d'un médecin, d'un groupe de médecins ou d'une société de médecins de réclamer des dommages encourus en raison de la violation de l'entente sur le partage de données par l'autre partie ou de sa négligence. Cette disposition peut également limiter le droit d'un médecin de réclamer le remboursement des dommages-intérêts qu'on lui a ordonné de payer suite à une réclamation faite par un tiers contre lui, son groupe ou sa société en conséquence d'un acte ou d'une omission du fournisseur de service, de région sanitaire ou de hôpital partie à l'entente sur le partage de données.

11.3 Recommandations :

- (a) Un médecin ne devrait permettre à aucune autre partie à l'entente sur le partage de données de limiter ou d'exclure sa responsabilité pour tout acte ou omission qui pourrait entraîner l'indemnisation d'un patient ou de tout autre tiers. Par exemple, là où c'est possible, un médecin ne devrait pas permettre à un fournisseur de service, à une région sanitaire ou à un hôpital de limiter leur responsabilité à l'égard de la divulgation ou l'utilisation induite des renseignements personnels sur la santé par ledit fournisseur de service, région sanitaire ou hôpital.
- (b) Le médecin doit tenter d'intégrer une disposition visant à limiter sa responsabilité éventuelle pour sa négligence ou son non-respect de l'entente sur le partage de données. En général, il est difficile pour une partie de limiter unilatéralement sa responsabilité en vertu d'un contrat à moins qu'elle ne dispose d'un pouvoir de négociation de beaucoup supérieur à celui de l'autre partie. Il est plus réaliste de penser que si un médecin demande une limitation de responsabilité en sa faveur, l'autre partie en demandera tout autant.
- (c) Le médecin devrait demander à son avocat de revoir toute clause de limitation de responsabilité. L'étude d'une telle clause devrait se faire dans le contexte de l'ensemble du contrat.

12. Représentations (déclarations) et garanties

12.1 Ce dont il s'agit :

Une représentation ou déclaration est la déclaration d'un fait (présent ou passé) et une garantie est la promesse qu'un fait particulier est vrai. Dans le cadre d'une entente sur le partage de données, une partie peut faire diverses représentations et garanties liées à l'exactitude des renseignements personnels sur la santé versés au système de DME/DSE, à la méthode par laquelle le consentement du patient a été obtenu et/ou au respect des dispositions législatives applicables.

12.2 En quoi est-ce important :

Une partie est responsable envers les autres parties au contrat si elle fait une déclaration qui est inexacte ou offre une garantie qui n'est pas comblée.

12.3 Recommandations :

- (a) Un médecin devrait obtenir des représentations et garanties des autres parties à l'entente sur :
 - (i) leur existence, leur statut et leur pouvoir de conclure l'entente;
 - (ii) la légalité de l'entente;
 - (iii) le fait que de conclure et d'exécuter l'entente ne contrevient à aucune loi, aucun document constitutif ou autre entente à laquelle elles sont parties; et
 - (iv) toute autre question propre à l'entente.
- (b) Le médecin devrait obtenir des représentations que le fournisseur de service n'enfreindra aucun droit de propriété intellectuelle d'un tiers.
- (c) Le médecin ne devrait faire aucune représentation et n'offrir aucune garantie à l'égard de circonstances qu'il ne contrôle pas ou dont il n'a aucune connaissance. Le médecin devrait s'assurer que toute représentation qu'il fait ou garantie qu'il fournit est vraie et exacte. Dans la mesure où un médecin fait des représentations ou donne des garanties, elles devraient, autant que possible, se limiter à ce que le médecin connaît, être qualifiées par le concept de l'importance relative et porter une période de survie déterminée.
- (d) Le médecin devrait demander à son avocat de revoir, dans le contexte de l'ensemble du contrat, toute représentation et garantie qu'il se propose d'offrir.

13. Règlement des litiges

13.1 Ce dont il s'agit :

Une entente sur le partage de données ou une entente entre médecins peut comprendre une disposition sur la résolution ou l'arbitrage des litiges à titre de mécanisme de règlement des conflits qui surviennent dans le cadre de l'entente en remplacement des procédures devant les tribunaux.

13.2 En quoi est-ce important :

Le mode alternatif de résolution ou d'arbitrage des litiges peut être avantageux en ce qu'il est habituellement moins coûteux, plus efficace et plus privé que les procédures devant les tribunaux.

13.3 Recommandations :

- (a) La disposition sur la résolution ou l'arbitrage des litiges ne doit pas empêcher le médecin de recourir à l'assistance de l'ACPM ou de son avocat personnel pour s'assurer que ses intérêts soient bien représentés en cas de litige.

(b) La disposition sur la résolution ou l'arbitrage des litiges ne doit pas empêcher le médecin d'obtenir une injonction d'un tribunal lorsqu'il y a risque de dommage immédiat et permanent.

14. Compétence juridictionnelle

14.1 Ce dont il s'agit :

Les parties à une entente peuvent préciser en vertu des lois de quelle province ou de quel territoire l'entente devra être interprétée ou exécutée. Les parties peuvent également préciser dans quelle province ou quel territoire et à quel endroit dans cette province ou ce territoire les différends devront être entendus.

14.2 En quoi est-ce important :

Lorsque l'entente sur le partage de données ne traite pas de compétence juridictionnelle, le tribunal devant lequel une poursuite est intentée peut accepter ou nier sa compétence. Le médecin, le groupe de médecins ou la société de médecins peut se voir forcé de régler un litige à un endroit plus commode et favorable au ministère, au fournisseur de service, à la région sanitaire ou à l'hôpital qui a intenté la poursuite ou qui y répond.

14.3 Recommandation :

Toute entente sur le partage de données devrait prévoir une disposition qui précise que la loi applicable est celle de la province ou du territoire canadien où le médecin exerce, et que toute procédure judiciaire devra être intentée à un endroit qui convient au médecin.

15. Financement

15.1 Ce dont il s'agit :

L'exploitation, la mise à jour et le soutien d'un système de DME/DSE comportent des frais.

15.2 En quoi est-ce important :

Les frais liés à l'exploitation, à la gestion et au soutien d'un système de DME/DSE seront importants.

15.3 Recommandations :

Le financement et l'infrastructure de soutien du système de DME/DSE devraient répondre aux besoins des médecins.

Lorsque des médecins considèrent la création d'une société par action ou d'une société en nom collectif aux fins d'un système de DME/DSE, il serait prudent de consulter un fiscaliste pour s'assurer que la structure de la société soit avantageuse pour les médecins concernés.

L'ACPM : une valeur sûre pour les membres

En tant que principal fournisseur de protection en matière de responsabilité médicale, l'ACPM s'engage à protéger l'intégrité professionnelle des médecins et à promouvoir des soins médicaux plus sécuritaires. Pour remplir ce mandat, l'ACPM offre une gamme complète de services à ses membres, en français et en anglais :

PROTECTION

- Protection en matière de responsabilité médicale fondée sur la survenance de l'événement
- Compensation appropriée versée aux patients ayant subi un préjudice prouvé à la suite de soins médicaux négligents pour le compte des médecins membres

CONSEILS ET ASSISTANCE

- Contact de médecin à médecin
- Conseils médico-légaux de la part de médecins-conseils chevronnés et assistance sur des sujets tels que :
 - Actions en justice au civil découlant du travail professionnel
 - Organismes de réglementation (Collège) – plaintes, enquêtes et audiences disciplinaires
 - Enquêtes du coroner ou autres enquêtes sur des décès
 - Vérifications ou enquêtes relatives à la facturation
 - Privilèges hospitaliers
 - Procès criminels découlant du travail professionnel
 - Certaines questions relatives aux contrats généraux et aux contrats de recherche
 - Violations de la loi sur la protection des renseignements personnels et plaintes relatives à la protection de la vie privée
 - Plaintes à la Commission des droits de la personne
- Prestation de services axés sur les membres et assistance avec des problèmes d'ordre professionnel

GESTION DES RISQUES ET ÉDUCATION

- Éducation en gestion des risques accréditée et fondée sur des données probantes, notamment des présentations, des symposiums, des conférences régionales donnant droit à des crédits de DPC
- Ateliers d'apprentissage en ligne
- Diffusion de résultats de recherche fondée sur des données probantes visant à améliorer la sécurité des soins médicaux

PUBLICATIONS

- *Perspective ACPM*, publiée trimestriellement
- Manuels et rapports sur des questions médico-légales, en versions imprimées et électroniques

POLITIQUE D'INTÉRÊT PUBLIC

- Commentaires d'experts en élaboration de politiques, y compris en ce qui a trait aux textes législatifs et aux règlements, ainsi qu'aux initiatives en matière de sécurité des patient
- Présentations, rapports, publications, engagement des partenaires