Tenue de dossier – dossiers papier et numérisé : une même réalité ?

par **Bernard Cadieux**, inh., M.A.P., M.Sc., syndic et **Magali Cournoyer-Proulx**, avocate associée, Fasken Martineau.

La mise en place des dossiers cliniques informatisés (DCI)*, des dossiers patients électroniques (DPE)* et du Dossier Santé Québec (DSQ)* illustre bien le virage numérique que le réseau de santé est en voie de réaliser.

L'avènement de ces nouveaux outils qui ont pour avantage d'offrir l'accès, en temps réel, à une information santé contemporaine, n'est pas sans soulever plusieurs questions de la part des inhalothérapeutes. Parmi ces enjeux, notons les questions liées à l'intégrité, à la sécurité et à la confidentialité des informations inscrites aux dossiers patients.

En réponse aux questions soulevées, le présent texte reprend sommairement quelques principes généraux sur la tenue de dossier applicables dans les secteurs public et privé, tout en soulignant les éléments à retenir dans un contexte de tenue de dossier numérique.

La rédaction de la note : rappel de principes généraux

L'article 50 du *Règlement sur l'organisation et l'administration des services*, RLRQ c S-5, r 5 (le « ROAE ») établit l'obligation pour les établissements de santé et de services sociaux de tenir un dossier pour chacun de ses usagers :

> « Un établissement doit tenir un dossier sur chacun des bénéficiaires qui en obtient des services, sauf ceux visés aux articles 45 et 51. …
>
> Rien dans le présent règlement ne doit être interprété comme excluant l'utilisation de l'informatique ou de toute autre technique pour la constitution et la tenue des dossiers des bénéficiaires d'un établissement. »
> (Les soulignés ont été ajoutés.)

L'article 1 du *Règlement sur les dossiers, les autres effets, les cabinets et la cessation d'exercice des membres de l'Ordre professionnel des inhalothérapeutes du Québec*, RLRQ c C-26, r 171 énonce pareille obligation qui incombe aux inhalothérapeutes, peu importe le lieu où ils exercent leurs fonctions.

Dans le secteur privé, la *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1 encadre de manière générale l'accès et la confidentialité des dossiers constitués en vertu de cette loi.

* Voir l'encadré 01 à la page 35.

encadré 01

« Le Dossier clinique informatisé (DCI) et le Dossier médical électronique (DMÉ) sont des dossiers électroniques locaux, c'est-à-dire des dossiers patients qui se trouvent soit dans un établissement (hôpital, CLSC, etc.), comme c'est le cas des DCI, soit dans un bureau de médecin, comme c'est le cas des DMÉ. Les DCI remplacent les dossiers papier des patients dans les établissements, alors que les DMÉ remplacent les dossiers papier des patients dans les cliniques et les bureaux de médecin.

Plus particulièrement, un DCI est un dossier patient informatisé, tenu par un établissement de santé. Ce dossier contient tous les renseignements consignés par les cliniciens de cet établissement lors des consultations, des traitements et des hospitalisations d'un patient. L'accès aux renseignements inscrits dans un DCI est limité à ces cliniciens, aux équipes soignantes et au patient lui-même, sauf si ce dernier a donné son consentement pour que d'autres personnes y aient accès.

Le DMÉ est un dossier patient informatisé, tenu par un médecin dans son bureau ou dans la clinique où il travaille. Ce dossier contient tous les renseignements consignés par le médecin au sujet d'un de ses patients. L'accès aux renseignements inscrits dans un DMÉ est limité à ce médecin, à l'équipe soignante et au patient lui-même, sauf si le patient a donné son consentement pour que d'autres personnes y aient accès.

Contrairement au DCI et au DMÉ, le DSQ n'est PAS un dossier médical complet. Il ne remplace ni les DCI, ni les DMÉ, ni le dossier papier. »

Source : MSSS [http://www.dossierdesante.gouv.qc.ca/population/FAQ/index.php#16].

En ce qui concerne les dossiers créés sur un support autre qu'un support-papier, l'article 5 de la *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c C-1.1 précise que :

> « 5. La valeur juridique d'un document, notamment le fait qu'il puisse produire des effets juridiques et être admis en preuve, n'est ni augmentée ni diminuée pour la seule raison qu'un support ou une technologie spécifique a été choisi.
>
> Le document dont l'intégrité est assurée a la même valeur juridique, qu'il soit sur support-papier ou sur un autre support, dans la mesure où, s'il s'agit d'un document technologique, il respecte par ailleurs les mêmes règles de droit. […] »
> (Les soulignés ont été ajoutés.)

On peut affirmer, de manière générale, que les mêmes normes applicables au dossier papier s'appliqueront au dossier informatisé. Ceci implique notamment que :

- les professionnels doivent constituer et maintenir un seul dossier par patient/client ;
- la note est le reflet de l'acte clinique. Elle se doit d'être pertinente, objective, lisible, informative, concise et explicite ;
- la disponibilité des données et des systèmes d'information doit être assurée en tout temps.

Intégrité de la note

L'article 6 de la *Loi concernant le cadre juridique des technologies de l'information* précise ce qui suit :

> « L'**intégrité** du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue.
>
> L'intégrité du document doit être maintenue au cours de son cycle de vie, soit depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction.
>
> Dans l'appréciation de l'intégrité, il est tenu compte, notamment des mesures de sécurité prises pour protéger le document au cours de son cycle de vie. »
> (Les soulignés et caractères gras ont été ajoutés.)

Voici donc quelques conseils à suivre afin d'assurer l'intégrité de la note contenue au dossier informatisé :

- ☐ être en mesure de démontrer la solidité de la chaîne de garde du dossier ou de ses entrées tout au long du cycle de vie des documents ajoutés au dossier ;
- ☐ offrir l'assurance que les données déjà inscrites ne pourront être ni effacées, ni remplacées, ni altérées :
  - ☐ l'inaltérabilité des entrées doit être garantie ;
  - ☐ toutes les entrées doivent être enregistrées ;
  - ☐ la note originale doit toujours figurer au dossier afin que les modifications apportées y soient apparentes. Aucun enregistrement ne peut être effacé. La modification (*addenda* ou biffure électronique) ne doit pas éclipser ou effacer l'entrée originale ;
  - ☐ une piste de vérification indiquant clairement les corrections, sans éclipser le dossier original, doit permettre d'identifier l'auteur de la correction ou de la modification ;
  - ☐ un relevé des modifications apportées au dossier doit être disponible ;
- ☐ s'assurer que le logiciel utilisé permette le transfert intégral des données dans un format universel vers une autre plateforme ;
- ☐ s'assurer que le professionnel respecte un processus de validation des écrits afin d'éviter toute erreur ;

- veiller à ce que le logiciel de gestion permette d'imprimer et de 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.

Confidentialité

Les règles en matière de confidentialité des dossiers s'appliqueront tout autant que l'on soit en format papier ou numérique. Voici quelques rappels des règles à suivre.

- Toutes les demandes d'accès doivent être traitées avec diligence dans le respect des lois et règlements en vigueur.
- La confidentialité des données doit être assurée en tout temps. À cet effet, les écrans devraient être orientés de façon à ce que la clientèle ne puisse voir les informations inscrites.
- Les utilisateurs doivent fermer leur session à la fin de chaque utilisation ou lors d'une interruption dans l'édition ou la consultation d'une note. Le temps de débranchement automatique du système doit être suffisamment court pour ne pas permettre à des regards indiscrets de consulter les données que les professionnels inscrivent.
- Un consentement explicite du patient est requis pour que les données de son dossier soient partagées avec des partenaires ou pour communiquer des renseignements à un tiers. En l'absence d'un consentement implicite évident, il serait de bonne pratique d'obtenir un consentement explicite du patient pour que les données de son dossier soient partagées avec des partenaires d'un cercle de soins (équipe interdisciplinaire). En tout temps, le consentement du patient est requis pour communiquer des renseignements à un tiers.
- L'accès doit être limité aux utilisateurs autorisés. Les profils d'utilisateur doivent correspondre et être liés à l'organisation de soins et de services.

Sécurité

En matière de sécurité des données informationnelles, les experts recommandent certaines précautions. Il est entre autres suggéré que :

- un répertoire distinct soit constitué pour les dossiers patients ;
- le système d'information permette l'impression des données tout en identifiant l'auteur de la note et l'auteur de cette impression. L'impression doit être limitée dans le cadre de gestion du dossier numérique afin d'éviter de créer un dossier patient satellite. La journalisation des impressions de documents est requise ;
- l'accès aux données soit protégé :
  - utilisation d'une clé de sécurité ;
  - processus d'authentification des utilisateurs (en donnant un code d'accès propre à chaque utilisateur) ;
  - contrôle d'accès fondé sur le rôle des utilisateurs ;
  - système de fermeture des sessions ;
  - journalisation des accès. Enregistrement de la date, de l'heure et de l'identité de l'utilisateur qui accède au dossier. Enregistrement des actions posées soit lecture-consultation, édition ou impression de la note ;
  - logiciel de protection contre les virus, les programmes malveillants et les logiciels espions ;
  - solides dispositifs de sécurité, notamment le chiffrement, l'utilisation de mots de passe et de contrôle d'accès ;
- les données soient inaltérables, en ce sens que les renseignements originaux sont conservés lorsqu'il y a modification ou mise à jour ;
- une procédure de sauvegarde automatique des entrées soit en place. Une copie de sécurité cryptée sur un serveur distant est recommandée en cas de panne du système ;
- le plan d'urgence (contingence) en cas de panne du système de dossier numérique soit connu de tous les utilisateurs. Les données doivent faire partie du dossier et le plan de relève doit prévoir la fusion des données ou l'inscription de ces données pour garder la structure du dossier intacte afin d'assurer la continuité et la sécurité des soins.

Conclusion

En tout temps, il faut se rappeler que le professionnel, qui utilise les technologies de l'information et de communication, est régi par les mêmes normes de pratique, lois et règlements que pour les médias papier traditionnels. Les inhalothérapeutes doivent être conscients malgré certaines nuances concernant l'intégrité, la confidentialité et la sécurité que les ***dossiers papier et numérisé constituent une même réalité***.

Documents consultés — références

COLLÈGE DES MÉDECINS DU QUÉBEC. 2015. *Le médecin, la télémédecine et les technologies de l'information et de la télécommunication.* [http://www.cmq.org/publications-pdf/p-1-2015-02-01-fr-medecin-telemedecine-et-tic.pdf].

COLLÈGE DES MÉDECINS DU QUÉBEC. 2015. *La rédaction et la tenue des dossiers par le médecin en milieu extrahospitalier.* [http://www.cmq.org/publications-pdf/p-1-2013-04-01-fr-redaction-et-tenue-des-dossiers-milieu-extrahospitalier.pdf].

GOUVERNEMENT DU QUÉBEC. 2014. *Avis: La télésanté au Québec — un regard éthique*, Commission de l'éthique en science et technologie. [http://www.ethique.gouv.qc.ca/fr/assets/documents/Telesante/Telesante_avis_A.pdf].

GOUVERNEMENT DU QUÉBEC. *Loi concernant le cadre juridique des technologies de l'information — Chapitre C1.1.* [http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_1_1/C1_1.html].

ASSOCIATION CANADIENNE DE PROTECTION MÉDICALE. 2014. *Guide sur les dossiers électroniques.* [https://www.cmpa-acpm.ca/documents/10179/24937/com_electronic_records_handbook-f.pdf].

GOUVERNEMENT DU QUÉBEC. *Loi sur la protection des renseignements personnels dans le secteur privé — P 39.1.* [http://www.legisquebec.gouv.qc.ca/fr/showdoc/cs/P-39.1#se:10].

GOUVERNEMENT DU QUÉBEC. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels — Chapitre A-2.1.* [http://legisquebec.gouv.qc.ca/fr/ShowDoc/cs/A-2.1#se:63_1].