DME ET MESURES DE SÉCURITÉ

Vous avez fait le grand virage et êtes passé aux dossiers médicaux électroniques (DME) ? Il faut maintenant vous poser les bonnes questions sur le recours aux technologies de l'information dans votre pratique : est-elle respectueuse de vos obligations quant à la protection de la confidentialité des renseignements personnels et du secret professionnel ? Votre utilisation et votre gestion sont-elles efficaces et sûres ? L'une des premières choses à mettre en place lors du passage du papier à l'informatique est une politique de sécurité au sein de votre clinique. L'avez-vous fait ?

Christiane Larouche

OBLIGATIONS DU MÉDECIN ET TECHNOLOGIES DE L'INFORMATION

Le règlement du Collège des médecins du Québec sur les dossiers, les lieux d'exercice et la cessation d'exercice d'un médecin permet le recours à l'informatique dans la gestion des dossiers médicaux, à condition de respecter la confidentialité des renseignements et les règles relatives à l'accès aux documents et à la protection des renseignements[1]. Les modalités du règlement concernant la constitution, la tenue, la détention et le maintien des dossiers médicaux sont d'ailleurs les mêmes pour les dossiers médicaux papier et électroniques. Toutefois, le règlement prévoit spécifiquement que le médecin qui emploie un support informatique doit de plus :

- employer une signature numérique ;
- utiliser un répertoire distinct de tous les autres ;
- protéger l'accès aux données, notamment à l'aide d'une clé de sécurité et de l'authentification des utilisateurs ;
- avoir recours à un logiciel de gestion de documents conçu de façon à ce que les données déjà inscrites ne puissent être effacées, ni remplacées ni altérées ;
- utiliser un logiciel permettant l'impression des données ;
- conserver, dans un autre lieu, une copie de sécurité cryptée des données ainsi recueillies[2].

Les systèmes de DME homologués au Québec tiennent compte de certaines de ces exigences techniques. Cependant, le médecin doit également prendre des mesures de sécurité concrètes pour assurer la confidentialité et la protection de la gestion des accès pour satisfaire à ses obligations. Rappelons qu'en vertu du *Code de déontologie des médecins*, le médecin doit prendre des moyens raisonnables à l'égard des personnes avec lesquelles il collabore[3]. Mais comment transposer les réalités bien connues de la gestion des dossiers papier à l'ère du numérique ? Dans un monde de papier, le contrôle de l'information a lieu par un contrôle physique des dossiers et des lieux. Dans un monde numérique, les mesures de contrôle prennent d'autres formes. Le Collège donne peu d'information pour guider les médecins sur ce sujet comme l'a fait, par exemple, le Barreau du Québec pour ses membres. Il faut donc se référer aux écrits émanant d'autres organisations, dont l'Association canadienne de protection médicale qui fournit quelques recommandations[4]. Certaines associations ou organisations médicales ont, par ailleurs, créé des guides et des outils dont les médecins peuvent s'inspirer dans leur milieu[5-8]. Nous placerons des liens vers ces outils sur la section du site Internet de la FMOQ consacrée au Programme québécois d'adoption des dossiers médicaux électroniques (PQADME).

POLITIQUE DE SÉCURITÉ

L'adoption d'une politique de sécurité a pour but de fixer des exigences encadrant l'usage de son réseau informatique ainsi que des mesures de sécurité pour en assurer la protection. Elle doit de plus établir les responsabilités des diverses personnes œuvrant au sein de la clinique : médecin responsable de la sécurité, ensemble des membres du personnel médical et administratif, fournisseurs de DME et spécialiste en soutien technique, le cas échéant.

Une politique de sécurité fait foi de l'engagement des médecins de la clinique de protéger les renseignements personnels de leurs patients. Elle permet de normaliser les processus et de réduire au minimum les risques médicolégaux associés aux technologies de l'information. La protection de la confidentialité, de l'intégrité et de l'accessibilité de l'information doit en être l'assise.

Un médecin responsable au sein de la clinique devrait idéalement en assurer la mise en œuvre et assumer les responsabilités suivantes :

- s'assurer que la politique de sécurité de la clinique est connue de tous les membres du personnel, qu'ils la comprennent et qu'ils la respectent ;

Me Christiane Larouche, avocate, travaille au Service juridique de la Fédération des médecins omnipraticiens du Québec.

- faire signer un engagement de confidentialité par le personnel et s'assurer de son respect ;
- déterminer qui bénéficiera de droits d'accès ;
- fournir la description des meilleures pratiques de sécurité ;
- effectuer des vérifications périodiques du respect des mesures de sécurité, y compris une vérification du registre des accès aux DME ;
- s'assurer que les ententes contractuelles de la clinique avec des tiers comportent des exigences de sécurité visant le respect des renseignements personnels.

MESURES DE SÉCURITÉ

Les médecins doivent s'assurer que des mesures de sécurité protègent leur réseau informatique. Ce réseau est formé d'ordinateurs, de périphériques, comme des imprimantes, des numériseurs, des serveurs, des routeurs et des modems, reliés ou non à des réseaux sans fil, et de logiciels. Les médecins, souvent peu familiers avec la technologie, auraient fortement intérêt à se faire aider dans cette tâche par des centres de services autorisés par le ministère de la Santé et des Services sociaux (voir la section du site Internet de la FMOQ sur le PQADME) ou par d'autres professionnels compétents en informatique. Une entente de services devrait alors intervenir pour prévoir les conditions de manipulation, d'utilisation, de stockage et de disponibilité de l'information. Il est également très important que cette entente contienne un engagement de confidentialité pour protéger adéquatement les informations confidentielles.

Nous vous proposons des exemples de mesures de sécurité figurant au nombre des pratiques recommandées.

IMPRIMANTES, PHOTOCOPIEURS, NUMÉRISEURS ET TÉLÉCOPIEURS

- Placer les équipements dans des lieux sécurisés accessibles uniquement au personnel.
- Prendre les documents imprimés sans délai.
- Vérifier les numéros de télécopieur avant de transmettre des documents.
- Ne laisser aucun original dans la photocopieuse ou le télécopieur avant de quitter les lieux.

ORDINATEURS FIXES ET PORTABLES

- Chaque utilisateur doit entrer un mot de passe pour commencer une session de travail.
- Les mots de passe devraient être changés minimalement tous les quatre-vingt-dix jours. Un bon mot de passe comporte un minimum de huit caractères avec une majuscule, une minuscule, un chiffre et un symbole.
- Chaque ordinateur doit être protégé par un antivirus mis à jour régulièrement.
- Les logiciels et les systèmes d'exploitation doivent également être mis à jour régulièrement.
- Les données enregistrées sur un ordinateur portable ou sur des supports amovibles doivent être chiffrées.
- L'installation de logiciels non autorisés sur les ordinateurs utilisés pour le travail doit être interdite.
- Les portables devraient être attachés lorsqu'ils sont employés dans la clinique.
- Il ne faut jamais laisser de portable dans une voiture.
- Il ne faut jamais laisser de portable sans surveillance dans un lieu public ou en voyage.
- Il faut être prudent lorsque vous travaillez avec un portable pour protéger la confidentialité des dossiers qui apparaissent à l'écran.

RÉSEAU

- Si vous utilisez un réseau sans fil, à la clinique ou à votre domicile, modifiez le code d'administrateur par défaut du routeur sans fil et le mot de passe, mettez en place une méthode par chiffrement (cryptage) des données qui transitent sur le réseau et configurez le routeur pour qu'il accepte uniquement les communications en provenance de votre réseau.
- Assurez-vous que les médecins qui travaillent à distance disposent d'une connexion RPV (réseau privé virtuel) protégeant leur session de travail.

COPIE DE SAUVEGARDE

- Faites des copies de sauvegarde une de vos priorités.
- La sauvegarde de l'ensemble des fichiers doit être effectuée quotidiennement sur un support indépendant conservé dans un autre lieu afin de pouvoir être récupéré en cas de désastre.
- Testez vos copies de sauvegarde régulièrement.
- Si les sauvegardes sont faites sur un CD, assurez-vous que les fichiers qui s'y trouvent sont en format cryptés.
- Si les sauvegardes ont lieu sur des clés USB, assurez-vous que les données sont enregistrées en format crypté également.

ENVIRONNEMENT DE TRAVAIL

- Les portes des bureaux doivent être verrouillées.
- Le ou les serveurs doivent être installés dans un environnement verrouillé.
- Les postes de travail doivent être éteints à la fin de la journée et les écrans de veille doivent être sécurisés.
- Tous les supports contenant des données, comme les clés USB, les CD, etc., doivent être conservés sous clé dans un lieu à l'abri du feu.

DESTRUCTION DES DOCUMENTS

- Les données enregistrées sur des disques durs doivent être supprimées par l'exécution d'un script en plusieurs passes. Les disques durs défectueux doivent être détruits physiquement au déchiquetage.
- Les dossiers papier que vous détruirez pour passer en mode numérique devront l'être conformément à vos obligations déontologiques.
- Videz la mémoire de vos photocopieurs ou numériseurs. Ces appareils utilisent un disque dur branché sur le réseau de la clinique et pourraient donc être accessibles par Internet.

PROCESSUS DE GESTION DES DÉPARTS

- Prévoyez des mesures de sécurité pour gérer le départ d'un médecin ou d'un membre du personnel de votre clinique.
- Désactivez temporairement, puis de façon permanente le compte de cette personne.
- Désactivez les accès au réseau privé virtuel.
- Remplacez tous les mots de passe.

INCIDENT DE SÉCURITÉ

- Mettez en place une procédure pour que les incidents de sécurité soient signalés et analysés par le responsable de la sécurité au sein de la clinique.

SINISTRE

- Établissez un plan d'action dans l'éventualité d'un sinistre, comme la perte de données, pour assurer la continuité des activités de la clinique.

CONCLUSION

L'adoption de mesures de sécurité appropriées pour l'utilisation des technologies de l'information dans votre pratique est incontournable. Elle exige de nouvelles connaissances, mais vous procure l'occasion de revoir la protection des renseignements personnels dans votre clinique et de former votre personnel en conséquence. //

BIBLIOGRAPHIE

1. Québec. *Règlement sur les dossiers, les lieux d'exercice et la cessation d'exercice d'un médecin*. Chapitre M-9, r. 20.3, article 3, à jour au 1er décembre 2013. Québec : Éditeur officiel du Québec.
2. *Idem*., article 9.
3. Québec. *Code de déontologie des médecins*. RRQ. chapitre M-9, r. 17, article 8, à jour au 1er février 2014.
4. Association canadienne de protection médicale. *Comment minimiser les risques médico-légaux découlant de la technologie.* Ottawa : L'Association ; 2008.
5. OntarioMD. Electronic Medical Records – Transition Support Program: Privacy and Security Guide and Workbook. Version 1.2. Toronto : OntarioMD. Site Internet : *https://www.ontariomd.ca/idc/groups/public/documents/omd_file_content_item/omd011945.pdf* (Date de consultation : janvier 2014).
6. CyberSanté Ontario. *Guide sur la sécurité de l'information pour le secteur des soins de santé pour les petits cabinets médicaux.* Toronto : CyberSanté Ontario ; 2010. Site Internet : *www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecGuide_SmallOffices_FR.pdf* (Date de consultation : janvier 2014).
7. British Columbia Medical Association. *Sample office privacy policy*. Vancouver : L'Association ; 2009. Site Internet : *https://www.bcma.org/files/Sample_office_privacy_policy_from_CMA_Privacy_Wizard.pdf* (Date de consultation : janvier 2014).
8. Manitoba e-Health. *Sample Privacy Policy*. Winnipeg : Le Programme. Site Internet : *www.manitoba-ehealth.ca/commPhysicians/files/Privacy_sample.pdf* (Date de consultation : janvier 2014).

ERRATUM

Une erreur s'est glissée dans le Dossier spécial PQADME du mois d'octobre 2013 intitulé : « Le PQADME, une occasion à saisir ! ». À la page 33, dans la dernière colonne du tableau *Frais admissibles et remboursement dans le cadre du PQADME*, de la section *GMF-UMF et GMF-CLSC en CSSS*, on devrait lire 5000 $ à la 5e ligne (Frais d'implantation) et 2000 $ à la 6e ligne (Acquisition et exploitation des licences).