DIX MYTHES SUR LA PROTECTION DES DONNÉES DES DME

Christiane Larouche

Les incidents de sécurité et les cyberattaques touchent de plus en plus de personnes et d'entreprises. Les DME de vos patients ne sont pas à l'abri. Bien au contraire, les données personnelles sur la santé font partie des données particulièrement convoitées et les plus susceptibles de faire l'objet d'une intrusion.

Une saine gestion des risques par les professionnels et les organisations dans le domaine de la santé est devenue un enjeu prioritaire. En raison de leur nature, les données des DME exigent un haut degré de protection, tant sur le plan physique et administratif qu'informatique et technologique.

Les connaissances et les compétences des professionnels de la santé en informatique et en technologie de l'information devront sans nul doute être rehaussées. Trop nombreux sont ceux qui ne se sentent pas concernés par les menaces ou qui se fient aveuglément à des tiers pour assumer leurs obligations.

À la lumière de dix mythes ayant cours sur la protection des données des DME de vos patients, nous vous invitons à tester vos connaissances.

MYTHE 1

L'UTILISATION D'UN DME CERTIFIÉ GARANTIT LA SÉCURITÉ DES DONNÉES

La certification d'un DME par le ministère de la Santé et des Services sociaux atteste de sa conformité à certains critères d'évaluation de qualité et de sécurité relativement à son interopérabilité (ou à son intégration) avec les actifs informationnels du secteur de la santé et des services sociaux[1]. La certification pourra ainsi orienter le choix d'un DME vers des solutions de qualité. Cependant, pour assurer la sécurité et la confidentialité des données de ses patients, le médecin doit obtenir des garanties contractuelles de son fournisseur de DME ou de services de soutien informatique. Il doit également adopter les meilleures pratiques pour protéger la confidentialité et la sécurité des DME de ses patients.

MYTHE 2

LE MÉDECIN N'EST PAS EN MESURE D'ASSURER LA SÉCURITÉ DES DME

Le médecin doit prendre les mesures requises pour assurer la sécurité des DME de ses patients afin de respecter ses obligations légales et déontologiques, même si ce n'est pas nécessairement facile pour lui[2,3,4]. La sécurité des DME englobe différents aspects dont le médecin devra tenir compte sur les plans physique (gestion des équipements informatiques, etc.), administratif (gestion du personnel ou des fournisseurs de services de soutien en technologie de l'information) et technologique ou informatique (solution de DME, d'hébergement des données; utilisation et accès aux données, etc.).

Bien que le médecin puisse déléguer certaines responsabilités à des fournisseurs de services, il demeure ultimement responsable devant son ordre professionnel[3,4]. Les contrats avec les fournisseurs doivent donc inclure des exigences que le médecin doit respecter, notamment les exigences informatiques en GMF.

Le médecin peut contribuer à instaurer une culture favorisant la sécurité des données personnelles dans sa clinique. Les mesures de protection sur le plan administratif incluent notamment la clarification des rôles et des responsabilités de chacun, l'adoption de politiques et des meilleures pratiques, une saine gestion des risques d'atteinte à la sécurité, y compris la gestion des incidents, leur déclaration, les plans de relève en cas de désastre, les évaluations internes des risques, etc.

MYTHE 3

L'ANALYSE DES RISQUES DE SÉCURITÉ EST REQUISE UNIQUEMENT EN ÉTABLISSEMENT OU EN GMF

L'analyse des risques de sécurité des DME doit être faite autant au sein des établissements publics que des cliniques médicales pour assurer le respect des lois sur la protection des renseignements personnels. De plus, les exigences informatiques imposées par le Programme GMF sont identiques pour les points de service en établissements publics ou privés[5].

MYTHE 4

L'ANALYSE DES RISQUES DE SÉCURITÉ EST REQUISE UNIQUEMENT LORS DE LA MISE EN ŒUVRE DES DME

L'analyse des risques de sécurité doit être faite non seulement lors de la mise en œuvre d'un DME, mais aussi lorsque se produit un incident ou un changement au système de DME et des applications associées. De plus, des évaluations

Me Christiane Larouche, avocate, travaille au sein de la Direction de la Planification et de la régionalisation à la Fédération des médecins omnipraticiens du Québec.

ponctuelles des équipements et du journal des accès aux DME devraient avoir lieu régulièrement pour s'assurer que seuls les intervenants autorisés ont accès aux DME aux fins requises dans le cadre de leur fonction.

MYTHE 5

L'UTILISATION D'UNE LISTE DE CONTRÔLE EST SUFFISANTE POUR ÉVALUER LES RISQUES

Les listes de contrôle (*checklist*) pour évaluer les risques dans son milieu peuvent être utiles et facilement accessibles[6, 7]. De telles listes ne permettent toutefois pas de réaliser une analyse de risque de sécurité systématique ou de documenter une analyse des risques antérieure.

MYTHE 6

SEUL UN FOURNISSEUR DE SERVICES EN INFORMATIQUE EST QUALIFIÉ POUR ÉVALUER LES RISQUES

Il est possible d'évaluer les risques à l'aide des outils d'autoassistance. Cependant, une analyse de risque approfondie et professionnelle qui résistera à un examen de conformité nécessite des connaissances poussées pouvant être obtenues auprès des services d'un professionnel externe expérimenté.

MYTHE 7

EN CABINET, LE MÉDECIN PEUT CONFIER LA SÉCURITÉ DES DME À DES FOURNISSEURS DE SERVICES

C'est le médecin qui doit s'assurer de la protection de la confidentialité et de la sécurité des DME. Certaines responsabilités spécifiques peuvent toutefois être confiées à des fournisseurs de services, qu'il s'agisse d'un fournisseur de DME ou d'un fournisseur de services de soutien informatique. Dans chaque cas, un contrat doit attester des obligations du fournisseur. Votre fournisseur de DME peut être en mesure de fournir des informations, de l'assistance et une formation sur les aspects de confidentialité et de sécurité de son DME.

MYTHE 8

IL FAUT UTILISER DES MÉTHODES RECONNUES POUR ÉVALUER LES RISQUES DE SÉCURITÉ

Il n'y a pas qu'une seule façon d'évaluer les risques de sécurité. Certaines organisations canadiennes ont publié des documents ou offrent des formations en ligne sur les exigences et les éléments à considérer en matière d'analyse des risques de sécurité[8]. Ces informations peuvent être utiles pour mettre en œuvre les mesures de protection les plus efficaces et les plus appropriées pour sécuriser les DME.

MYTHE 9

UNE ANALYSE DE LA SÉCURITÉ DES DONNÉES DES DME PORTE SUR LE LOGICIEL DE DME

Passez en revue tous les appareils électroniques qui stockent, capturent ou modifient des informations de santé protégées électroniquement. Incluez votre matériel, vos logiciels et le logiciel de votre DME et des applications qui s'y greffent, ainsi que les appareils pouvant accéder à vos données (par exemple, votre tablette électronique, le téléphone portable de votre responsable de cabinet). N'oubliez pas que les numériseurs stockent également des données.

MYTHE 10

UNE ANALYSE DES RISQUES DOIT ÊTRE FAITE CHAQUE ANNÉE

L'analyse complète des risques de sécurité doit être faite lors de l'adoption d'un DME ou d'un changement de DME. Par la suite, chaque année, dès que des modifications sont apportées à votre pratique ou à vos systèmes électroniques, vous devriez revoir et mettre à jour votre analyse des risques en y apportant les modifications requises selon les nouveaux risques constatés. //

BIBLIOGRAPHIE

1. Le ministère de la Santé et des Services sociaux. *Technologies de l'information—Internet—Familles de services : Certification et homologation*. Québec : le Ministère ; 2016. .
2. LégisQuébec. *Code de déontologie des médecins*. Chapitre M-9, r. 17. Québec : Publications du Québec ; 2014.
3. LégisQuébec. *Règlement sur les dossiers, les lieux d'exercice et la cessation d'exercice d'un médecin*. Chapitre M-9, r.20.3. Québec : Publications du Québec ; 2019.
4. LégisQuébec. *Loi sur la protection des renseignements personnels dans le secteur privé*. Chapitre P-39.1. Québec : Publications du Québec ; 2019.
5. Équipe suprarégionale GMF MSSS. *Exigences informatiques GMF version : 6.2*. Québec : le ministère de la Santé et des Services sociaux ; 2017.
6. Commissariat à la protection de la vie privée du Canada, Office of the Information and Privacy Commissioner for BC (OIPC), Office of the Information and Privacy Commissioner of Alberta. *Securing personal information: A self-assessment tool for organizations*. Gatineau, Vancouver, Edmonton : le Commissariat, le Bureau de l'information de la Colombie-Britannique, le Bureau de l'information de l'Alberta ; 2012. 32 p.
7. Alberta Medical Association. *Privacy and security self assessment*. Edmonton : l'Association.
8. Doctors of BC (BCMA), College of Physicians and Surgeons of BC (College), Office of the Information and Privacy Commissioner for BC (OIPC). *BC Physician Privacy Toolkit A guide for physicians in private practice*. 3e éd. Vancouver : l'Association, le Collège et le Bureau ; 2017. 70 p.
9. Inforoute Santé du Canada. *Enjeux et exigences de protection des renseignements personnels et de sécurité des solutions de santé numérique*. Montréal : l'Inforoute ; 2014.