PRATIQUES EXEMPLAIRES POUR L'UTILISATION CLINIQUE DE LA PHOTOGRAPHIE PAR TÉLÉPHONE OU AUTRES APPAREILS INTELLIGENTS

CONTEXTE

La photographie est un outil précieux pour les médecins en contexte clinique. Or, les téléphones intelligents, comme tout autre appareil en réseau, constituent un moyen pratique et efficace de prendre des photos et de les transmettre. Cependant, en raison du caractère privé de celles-ci, il importe que le stockage, la diffusion et la documentation des images cliniques se fassent de façon appropriée. La confidentialité des images doit être prise en considération, et leur diffusion sur des serveurs doit respecter la vie privée et les droits du patient. Principe important, on doit traiter comme un renseignement sur le patient toute information qui vient de lui; aussi les notions présentées ici s'appliquent-elles à tout document visuel de cet ordre qui puisse être capté ou transmis au moyen d'un appareil intelligent.

La photographie clinique peut servir à attester la forme et le fonctionnement d'un organe, à faire le suivi d'une affection et de la guérison d'une plaie, à planifier des interventions chirurgicales et à prendre une décision clinique. De plus, la photo clinique peut constituer pour le médecin un outil précieux de communication avec le patient et être utilisée à des fins de sensibilisation. Étant donné l'utilité indéniable de ce type de technologie, on ne saurait demander aux médecins, qui tentent d'offrir les meilleurs soins possible à leurs patients, de s'en passer.

Il existe déjà des technologies et des logiciels qui assurent la transmission, la communication et le stockage sécurisés des photos et vidéos cliniques, mais de nombreux appareils comportent des options de stockage et de diffusion non sécurisées qui, notamment, ne permettent pas la suppression définitive des fichiers, sans compter que les données téléversées sur des serveurs

i Heyns M†, Steve A‡, Dumestre DO‡, Fraulin FO‡, Yeung JK‡
† University of Calgary, Canada
‡ Section of Plastic Surgery, Department of Surgery, University of Calgary, Canada

externes se retrouvent bien souvent en territoire étranger. Bien des médecins ne sont pas à l'aise avec cette pratique pour des raisons de sécurité, de protection des renseignements personnels et de confidentialité, et à cause de l'incertitude entourant les réglementations régionales[1]. Par égard pour la protection des renseignements personnels et de la vie privée, il importe au plus haut point de limiter l'obtention et la diffusion non sécurisées ou non documentées de photographiques cliniques.

Pour faire le point sur l'état actuel de la réflexion dans ce domaine, Heyns et ses collaborateurs ont examiné l'accessibilité et l'exhaustivité des lignes directrices des ordres des médecins provinciaux et territoriaux[2]. Les thèmes jugés essentiels et explorés dans leur étude étaient le consentement, la transmission, le stockage, la vérification et la conservation, et les brèches de sécurité. Or, chaque ordre professionnel n'aborde que certains de ces thèmes, et les auteurs notent un manque d'information généralisé sur la question. Ils font valoir la nécessité d'établir un document normatif unique sur la prise de photographies cliniques à l'aide de téléphones intelligents et la transmission électronique de renseignements sur les patients[2].

Cette réflexion collective se doit d'être permanente : il importe que les médecins connaissent les réglementations fédérales et provinciales et sachent comment elles s'appliquent à eux. Les pratiques exemplaires proposées ici visent à informer les intervenants en santé de l'ampleur et de la gravité de la situation. Elles leur indiquent aussi comment protéger la vie privée des patients et la confidentialité de leurs renseignements dans l'utilisation de la photographie clinique pour améliorer les soins. Notons que le présent document ne concerne que l'utilisation médicale (clinique, didactique et pédagogique) de la photographie clinique et que, bien qu'il fasse état de nombreux principes fondamentaux de l'obligation de confidentialité et de respect de la vie privée, il ne constitue pas un règlement-cadre complet ou exécutoire. De plus, il est également recommandé que les médecins connaissent les principes de base de la photographie clinique, qui ne sont pas décrits ici.

L'Association médicale canadienne (AMC) suggère que les recommandations suivantes soient mises en œuvre, le plus complètement possible, pour le respect de ses *Principes de protection des renseignements personnels des patients* (Politique PD2018-02 de l'AMC). Il s'agit toutefois d'une liste incomplète; les médecins devraient se renseigner davantage au besoin afin d'acquérir une solide compréhension du domaine et de rester au fait de son évolution constante.

PRINCIPALES RECOMMANDATIONS

1. CONSENTEMENT

- Il y a lieu d'obtenir, préférablement à l'avance, le consentement éclairé du patient à la prise d'images avec un appareil mobile, et ce, à chaque rencontre et en lui en expliquant clairement l'utilisation prévue (utilisation clinique, recherche, sensibilisation, publication, etc.). Le patient devrait aussi être informé qu'il peut demander une copie de l'image ou sa destruction.

- Le fait qu'un patient ait consenti à la transmission électronique d'une image ne relève pas le médecin de son obligation d'en protéger la confidentialité ni n'annule les autres exigences légales et réglementaires.
- Il importe de garder une trace d'un consentement, même verbal. L'acquisition et la consignation du consentement d'un patient à la prise et à la diffusion de photos médicales pourraient être associées à un devoir rigoureux de reddition de comptes, étant donné les préoccupations de protection des renseignements personnels et de la vie privée inhérentes à l'utilisation de cette technologie. On préconise l'obtention d'un consentement écrit et signé.
- L'obtention du consentement devrait être considéré comme indispensable dès qu'une photo montre un patient, même si elle ne permet pas de le reconnaître directement, en raison du potentiel d'information liée ou d'atteinte à la vie privée. Il y a lieu de faire preuve de circonspection dans la définition de ce qu'est une photo non identificatoire. Certaines technologies actuelles telles que la reconnaissance faciale et l'appariement de formes (marques cutanées, structure corporelle, etc.) ont la capacité de porter atteinte à la vie privée d'un patient, surtout en combinaison avec des renseignements identificatoires.
- L'envoi d'un message texte ou d'un courriel non sécurisé ne devrait avoir lieu que si le recours à une méthode sécurisée est impossible. Le cas échéant, le consentement du patient devrait obligatoirement être explicite, et ce, même si la transmission est effectuée par le patient.

2. TRANSMISSION

- La transmission des images et renseignements concernant un patient devrait être chiffrée selon les normes les plus rigoureuses et les plus récentes (à savoir, au moment d'écrire ces lignes, le chiffrement de bout en bout) et ne passer que par des serveurs sécurisés soumis aux lois canadiennes. Dans le cas contraire, un consentement explicite et éclairé du patient est requis en raison des préoccupations relatives à la protection des renseignements personnels et de l'incertitude quant aux normes s'appliquant aux autres territoires. En règle générale, les services de communication gratuits par Internet et les accès Internet publics ne sont pas sécurisés, et les serveurs correspondants se trouvent souvent hors du territoire canadien.
- Il faut chercher à utiliser le mode de transmission le plus sûr possible. Pour des raisons de sécurité, on ne devrait jamais trouver de renseignements d'identification dans l'image ou la vidéo, dans le nom du fichier ni dans le message qui les accompagne.
- L'expéditeur devrait toujours vérifier la liste des destinataires pour s'assurer qu'elle est justifiable et ne comporte pas d'erreurs et, si possible, obtenir un accusé de réception.

3. STOCKAGE

- Pour des raisons de sécurité, le stockage d'images et de données sur un appareil intelligent devrait se limiter au strict nécessaire.
- Les photos cliniques ainsi que les messages connexes et tout autre renseignement se rapportant au patient devraient se trouver dans un espace de stockage complètement

séparé des données personnelles sur l'appareil. Pour cela, on peut utiliser une application qui crée un dossier sécurisé et protégé par mot de passe.

- Tous les renseignements stockés (dans la mémoire interne ou sur un nuage) doivent être efficacement chiffrés et protégés par mot de passe. Les mesures de sécurité ne doivent pas se limiter au simple verrouillage par mot de passe de l'appareil mobile.
- Il y a lieu de chercher à dissocier les images des renseignements identificatoires lorsque celles-ci sont exportées d'un serveur sécurisé. Il n'y a lieu de téléverser des photos ou vidéos sur des plateformes n'offrant pas d'option de suppression sûre que s'il n'existe aucune autre option, et avec le consentement du patient. Il faudrait aussi désactiver la sauvegarde automatique des photos sur les serveurs infonuagiques non sécurisés. Enfin, il importe d'évaluer et d'atténuer le risque que représentent les autres options de copie de sauvegarde ou de synchronisation qui pourraient faire appel à des serveurs non sécurisés.
- Le stockage infonuagique devrait se faire sur un serveur canadien certifié SOC 2, sauf si le patient consent de façon explicite et éclairée à une autre option, car la confidentialité ne peut être garantie sur les serveurs d'autres territoires.

4. VÉRIFICATION ET CONSERVATION

- Établir une piste de vérification constitue une pratique exemplaire médicale importante pour des raisons de transparence. Les renseignements importants en cause ici sont l'information médicale et générale sur le patient; la nature et le contenu du consentement donné; l'information connexe à la photo (date, circonstances, photographe); et tout autre fait digne de mention, comme les demandes de suppression ou les autorisations de visionnement accordées.
- Seuls devraient pouvoir accéder aux données stockées le médecin ou l'intervenant en soins de santé autorisés, et ce, dans le but prévu et selon le consentement donné. Les dossiers devraient être stockés de façon à permettre l'impression et le transfert du contenu, au besoin.
- Les fichiers originaux devraient être conservés et ne jamais être écrasés.
- Toutes les images et tous les messages connexes peuvent être considérés comme faisant partie du dossier clinique du patient et conservés pendant au moins 10 ans, ou 10 ans après l'âge de la majorité dans le cas d'un patient mineur. Lorsque c'est possible, les renseignements sur le patient (y compris les photos et les historiques de messages entre professionnels de la santé) devraient être conservés et joints à son dossier médical. La réglementation sur la conservation des dossiers cliniques peut varier d'une province à l'autre, et d'autres règlements peuvent s'appliquer, selon l'entité – par exemple, pour les dossiers fédéraux, la durée de conservation est de 90 ans après la date de naissance.
- Il peut être interdit de supprimer une image ayant joué un rôle déterminant dans une décision clinique ou à laquelle s'applique une exigence de conservation fédérale, provinciale ou d'une autre autorité.

5. BRÈCHES DE SÉCURITÉ

- Toute brèche de sécurité devrait être examinée et prise au sérieux. Tous les efforts raisonnables doivent être faits pour prévenir les brèches de sécurité. On parle de brèche de sécurité quand des renseignements personnels, des communications ou des photos de patients sont volés, perdus ou divulgués par erreur. Il peut s'agir de la perte ou du vol d'un appareil mobile, d'un message texte envoyé à un mauvais numéro ou d'un courriel envoyé à un destinataire erroné, ou encore du fait de montrer accidentellement une photo clinique se trouvant dans un album personnel sur le téléphone.
- À noter que des renseignements non identificatoires combinés à d'autres informations (p. ex. un message texte ou une image comportant des éléments identificatoires) peuvent permettre de déterminer l'identité d'une personne avec précision.
- À l'heure actuelle, les applications personnelles qu'on peut télécharger sur un appareil intelligent peuvent collecter et transmettre des renseignements; étant donné l'évolution rapide de cette technologie et les questions de sécurité inhérentes qu'elle pose, une vigilance constante s'impose. Dans ce contexte, il y a lieu d'employer des applications spécialement conçues pour transmettre des données médicales et protéger les renseignements sur les patients.
- La fonction de nettoyage à distance (reformatage de l'appareil) est un atout et peut aider à limiter les brèches de sécurité. Toutefois, un tiers non autorisé pourrait avoir le temps d'accéder aux données avant le reformatage.
- La perte d'un téléphone intelligent, s'il est efficacement chiffré et ne contient aucune photo clinique, ne constitue pas nécessairement une brèche de sécurité.
- En cas de brèche, les patients potentiellement touchés doivent être avisés dès que possible. L'Association canadienne de protection médicale, l'organisation ou l'hôpital, et l'organisme provincial d'attribution de permis doivent aussi être informés immédiatement. La réglementation sur la déclaration des brèches de sécurité peut varier d'une province à l'autre.

Approuvé par le Conseil d'administration de l'AMC en mars 2018

Références

[1] Chan, N. et coll. Should 'smart phones' be used for patient photography? *Plastic Surgery*. 2016; vol. 24, nº 1, p. 32–34.
[2] Heyns, M. et coll. Canadian Guidelines on Smartphone Clinical Photography. Non publié.