Version brève

Comment gérer les médias sociaux – Recommandations pour les médecins

Avril 2016

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Elfenstrasse 18 · Postfach 300 · CH-3000 Bern 15 · Telefon +41 31 359 11 11 · Fax +41 31 359 11 12 · info@fmh.ch · www.fmh.ch

Les médias sociaux dans le quotidien professionnel des médecins

Les médias sociaux jouissent d'une popularité qui ne cesse d'augmenter. Leur diffusion est exponentielle. Le domaine de la santé ne déroge pas à la règle; ils lui offrent aussi de nouvelles chances et de nouvelles possibilités. En parallèle, leur utilisation place les médecins ainsi que les autres professionnels de santé face à des risques et problèmes spécifiques, et soulève de nouvelles questions: les médecins doivent-ils accepter les demandes d'ami de leurs patients sur Facebook? Sur les réseaux sociaux, peut-on conseiller les patients ou recommander un traitement ou des médicaments? Qu'en est-il du transfert de données confidentielles concernant un patient? De quoi faut-il tenir compte lorsqu'un cas est discuté ou que des commentaires sur un collègue sont postés sur les réseaux sociaux ou dans une communauté en ligne?

S'agissant de professionnalisme et de communication chez les médecins, les étudiants en médecine ou d'autres professionnels de santé, les exigences et les attentes élevées ne s'arrêtent pas à l'entrée de «l'espace public» des médias sociaux. Le Code de déontologie de la FMH définit les relations du médecin avec ses patients et ses collègues, et son comportement en public et vis-à-vis des partenaires de santé. La validité de ces règles est inchangée dans les médias sociaux et sur internet, mais elles doivent être bien interprétées et mises en œuvre dans l'environnement des nouveaux médias.

Les présentes recommandations de la FMH s'entendent comme une aide à l'orientation et visent à attirer l'attention des médecins et des étudiants en médecine sur les risques et les dangers inhérents aux médias sociaux et à les aider à adopter une gestion adéquate des médias sociaux dans le contexte particulier de leur profession.

L'élaboration de ces recommandations s'est appuyée sur les recommandations et les directives de différents pays et de différentes organisations médicales, tout en tenant compte des résultats d'études internationales sur la diffusion et l'utilisation des médias sociaux dans l'environnement professionnel des médecins. A l'étranger aussi, l'augmentation des cas avec des conséquences disciplinaires ou juridiques a souligné la nécessité d'établir des recommandations spécifiques aux professionnels de santé.

Les chances et les possibilités de nouvelles voies pour la prise en charge médicale mais aussi les attentes des patients de la génération des «digital natives» sont à confronter aux exigences de qualité et de sécurité des traitements médicaux et aux enjeux de la protection et de la sécurité des données. Il ne serait pas pertinent que les présentes recommandations émettent des interdictions catégoriques car il s'agit aussi de faire fructifier les possibilités offertes par les médias sociaux. Les limites d'une éventuelle consultation ou d'un traitement médical via les médias sociaux sont implicitement déterminées par une pratique correcte sur le plan professionnel. La question fondamentale qui se pose est donc la suivante: en situation concrète, que peut-on considérer comme une pratique diligente?

Médias sociaux: chances et risques

Par «médias sociaux» on entend les médias, plateformes et applications numériques basées sur le Web permettant d'un côté la communication et l'échange interactif d'informations et de contenus, et de l'autre, la collaboration et la connexion à des communautés publiques ou privées.

Les contenus, contributions ou images diffusés dans les médias sociaux ou sur internet sont rapidement accessibles à un nombre illimité et incontrôlable de personnes. Ils peuvent être copiés, enregistrés ou réutilisés. De ce fait, une déclaration et des images irréfléchies peuvent sévèrement ternir la renommée d'une personne ou d'une organisation en un temps très court. De plus, les données et informations publiées sur internet ou dans les médias sociaux sont pratiquement «indélébiles» c.-à-d. impossibles à faire disparaître.

La facilité de saisir une contribution mais aussi le prétendu anonymat de «l'espace public» des médias sociaux constituent un risque, celui de publier ou d'exprimer trop rapidement et imprudemment un avis peu nuancé. Il faut aussi être attentif au fait que des contributions problématiques ou des rumeurs peuvent être colportées de manière anonyme ou sous un faux nom ou un pseudonyme sans que l'identité du véritable auteur ne soit connue. Rappelons cependant que l'internet n'est pas un

espace de non-droit, contrairement aux idées reçues et largement diffusées. Lorsqu'il est possible de remonter à une diffusion illicite d'informations ou d'images et d'en identifier les auteurs, ces derniers courent le risque de sanctions juridiques similaires à celles encourues lors de déclarations illicites dans la presse écrite.

En principe, les médias sociaux disposent aussi de différentes mesures de sécurité organisationnelles et techniques permettant d'empêcher ou de réduire fortement l'accès à des données personnelles ou privées. Cependant, même des paramètres restrictifs ne permettent pas toujours d'exclure avec une certitude absolue l'accès à des données et informations protégées, et d'éviter leur utilisation abusive. En outre, l'échange de messages et de documents via les médias sociaux est rarement sécurisé et protégé. En fonction de la teneur des conditions générales (CG), les contenus peuvent être réutilisés ou transmis par les exploitants des médias sociaux. De plus, beaucoup de plateformes se laissent la possibilité de modifier à tout moment leurs CG.

Dans les médias sociaux et sur internet, la protection de la sphère privée peut être compromise non seulement par l'accès direct à des données et à des informations protégées mais également par la conjonction et la connexion de données et d'informations issues de plusieurs sources et diffusées à des périodes différentes. Dans ce contexte, il est important de rappeler les technologies et les méthodes du «Big Data». En effet, diverses individus ou organisations criminelles, les services secrets mais aussi un grand nombre d'entreprises privées (p. ex. industrie, commerce, banques, assurances, etc.) manifestent un vif intérêt pour l'utilisation des résultats ainsi obtenus.

De plus, un nombre croissant d'entreprises et d'organisations, p. ex. les compagnies d'assurance ou d'autres prestataires commerciaux, recherchent des données et des informations personnelles et établissent des profils de clients différenciés. Les patients, collègues de travail, partenaires ou employeurs potentiels et chercheurs de têtes mais aussi les groupements criminels recherchent de plus en plus d'informations personnelles et professionnelles concernant les médecins sur internet et dans les médias sociaux. Dès lors, une présence ou des contributions inadéquates, des formulations imprudentes ou encore des informations trop intimes sur soi peuvent non seulement porter préjudice dans l'environnement professionnel mais aussi pour des relations à venir ou la carrière professionnelle. Le Préposé fédéral à la protection des données et à la transparence recommande de ce fait de «se demander avant toute publication si on souhaiterait être confronté à cette information lors d'un entretien d'embauche – même dix ans plus tard.»

Dans ce contexte, il serait également pertinent que les médecins qui emploient des étudiants en médecine, des professionnels de santé ou des auxiliaires les rendent attentifs aux risques spécifiques des médias sociaux dans le contexte médical et qu'ils en réglementent l'utilisation.

Gestion des médias sociaux dans l'environnement professionnel

Fondamentalement, les médecins, les étudiants en médecine et les autres professionnels de santé sont aussi très attentifs aux exigences élevées posées à leur comportement professionnel dans les médias sociaux et sur internet. En particulier,

- ils respectent, dans ces médias aussi, la confidentialité des informations se rapportant aux patients et le secret médical;
- ils se comportent, dans ces médias aussi, de manière correcte et professionnelle vis-à-vis de leurs patients et de leurs collègues et maintiennent ainsi la confiance dont jouit le corps médical.

La FMH recommande de réglementer la gestion des médias sociaux et de l'internet dans l'environnement professionnel avec les employés.

Recommandation 1: confidentialité des informations se rapportant aux patients

La FMH recommande:

- de faire preuve de beaucoup de retenue dans les médias sociaux lorsqu'il s'agit d'utiliser des informations et des images se rapportant à un patient et, dans la mesure du possible, de demander l'accord préalable du patient;
- en particulier pour des photos ou vidéos de patients, de ne pas utiliser d'appareils qui pourraient servir en privé (téléphone portable privé pour la documentation photo d'un patient);
- de modifier ou d'éviter les indications personnelles et les informations détaillées comme les initiales du patient, sa date de naissance, sa profession, son lieu de résidence, etc. dans les contributions (p. ex. descriptions de cas, présentations, etc.) et documents (p. ex. radio, scanner, IRM, ECG, etc.);
- si possible, de n'indiquer dans les contributions que des informations de trois domaines médicaux au maximum (p. ex. sexe, maladie, traitement, etc.) car elles suffisent généralement pour une description de cas anonyme;
- de veiller aux informations concernant une image, qui sont également sauvegardées avec l'image (ce qu'on appelle les métadonnées);
- de veiller aux points mentionnés dans la présente également pour les présentations lors de congrès, sessions de formation, etc., car elles sont souvent publiées sur internet;
- de n'utiliser que des groupes fermés sur des plateformes professionnelles et protégées lorsqu'il s'agit d'échanger entre collègues des informations médicales se rapportant à un patient (p. ex. discussion de cas, consilium, etc.) dans les médias sociaux.

Recommandation 2: la relation médecin-patient

La FMH recommande:

- de veiller au caractère professionnel de la relation médecin-patient également dans la communication via les médias sociaux et, dans la mesure du possible, de séparer les relations médecin-patient des relations privées;
- sur Facebook ou d'autres médias sociaux, de créer un compte à usage purement professionnel pour le cabinet ou l'hôpital, distinct d'un compte privé, avec exclusivement des informations professionnelles, et de ne communiquer avec les patients que via de tels comptes;
- de refuser autant que possible «les demandes d'ami» sur un compte privé lorsqu'elles proviennent de patients;
- d'avoir toujours présent à l'esprit les limites d'une consultation et d'un traitement via des médias en ligne;
- de traiter les informations médicales concernant les patients obtenues par courriel ou via les médias sociaux de la même manière que les autres informations de patients obtenues par oral ou par courrier;
- de mentionner, à l'intention des patients, les risques en lien avec l'utilisation des médias sociaux.

Recommandation 3: comportement dans l'environnement de travail

La FMH recommande:

- de veiller au fait que les dispositions du Code de déontologie de la FMH concernant la collégialité et les critiques inadmissibles sont également applicables dans les médias sociaux et sur internet;

- de veiller à une communication professionnelle objective et respectueuse, et à l'objectivité de contributions à l'endroit de collègues;
- d'attirer l'attention sur le comportement problématique, si possible personnellement, des collègues médecins, des étudiants en médecine ou d'autres professionnels de santé ayant un comportement inapproprié dans les médias sociaux;
- de prendre la décision réfléchie de savoir à quels collègues de travail ou personnes de l'environnement professionnel accorder l'accès à un domaine privé et protégé des médias sociaux.

Recommandation 4: présences et contributions professionnelles, privées ou publiques

La FMH recommande:

- de faire preuve de retenue et d'objectivité dans la manière de publier des informations, commentaires et images aussi bien professionnels que privés dans les médias sociaux. Les règles fondamentales d'un comportement professionnel, en particulier l'interdiction de publicité réputée non objective, mensongère ou qui nuit à la réputation de la profession de médecin, doivent également être respectées dans les médias sociaux;
- de rédiger les contributions assorties de contenus médicaux dans les médias sociaux et sur internet de manière correcte, actualisée, objective, professionnelle et compréhensible. On recommande à l'auteur de mentionner sa spécialisation et sa qualification, l'intention poursuivie, les sources, la date de la dernière actualisation et les informations nécessaires pour une prise de contact et, par ailleurs, de prendre en compte les objectifs et le public cible des médias sociaux et plateformes utilisés, de déclarer ses éventuels conflits d'intérêts (financiers, idéels, etc.) et, enfin, de donner la priorité au sujet traité et non à la personne du médecin;
- de ne pas donner de recommandations concrètes et de remarques sur un traitement, ou le cas échéant, uniquement à des personnes connues personnellement.
- à titre de mesure de protection, de rechercher et de vérifier régulièrement sur internet les contributions sur sa propre personne.

Recommandation 5: protection et sécurité des données

La FMH recommande:

- de limiter, si possible à des groupes ou à des individus définis, les paramètres de protection de la sphère privée et l'accès aux contenus sur les médias sociaux, et de sélectionner le niveau de confidentialité le plus élevé;
- d'appliquer aussi dans les médias sociaux les mesures organisationnelles et techniques générales de protection et de sécurité des données (p. ex. contrôle d'accès aux appareils et aux comptes, mot de passe sécurisé, changé périodiquement et conservé en lieu sûr, etc.). En particulier, il est recommandé de protéger et de sécuriser les appareils mobiles, comme les smartphones ou les tablettes, contenant des informations de patients ou un accès à des dossiers médicaux informatisés (perte, vol), de ne pas y installer d'applications qui accèdent aux données locales (compte Facebook ou similaire), et de vérifier périodiquement les possibilités et les limites des paramètres pour la protection de la sphère privée;
- d'échanger les informations médicales confidentielles uniquement via des connexions sécurisées ou des documents cryptés;
- de toujours veiller à l'identité du destinataire lors de l'échange d'informations confidentielles (p. ex. adresse électronique connue).