28.05.2024

Usage des médias sociaux et des services de messagerie

Recommandations de la FMH

Nous déclinons toute responsabilité quant à l'exactitude juridique du présent document et aux dommages consécutifs directs ou indirects.

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Postfach · CH-3000 Bern 16 · Telefon +41 31 359 11 11 · info@fmh.ch · www.fmh.ch

Table des matières

LES RECOMMANDATIONS EN BREF

Médias sociaux

1. L'utilisation des médias sociaux à des fins professionnelles doit faire l'objet d'un examen critique tenant également compte des ressources nécessaires (temps, connaissances et budget).
2. Seules les informations nécessaires à l'activité professionnelle et utiles pour la patientèle, les proches, les collègues et les clients devraient être publiées sur les comptes professionnels dans les médias sociaux.
3. Il convient de s'abstenir de diffuser des déclarations ambiguës ou fausses, d'éviter d'utiliser les comptes professionnels dans les médias sociaux à des fins privées et de ne pas susciter des attentes injustifiées. (Exemple I)
4. Il est essentiel d'avoir à l'esprit que les différentes plateformes et les différents canaux présentent chacun des atouts et des risques spécifiques pour des objectifs de communication spécifiques.
5. Les comptes privés et professionnels sur les plateformes de médias sociaux doivent être gérés séparément.
6. Les demandes d'ajout de patients sur des comptes privés doivent être considérées avec la plus grande attention. (Exemple II)
7. En cas de commentaires négatifs sur les médias sociaux, il est recommandé de réagir de manière réfléchie afin de préserver son image et de contribuer à un débat public respectueux. (Exemple III)
8. Il convient de veiller à ne pas publier de contenus inappropriés sur les médias sociaux et à prévenir les collègues en cas de publications inappropriées de leur part. (Exemple IV)
9. Le partage d'informations et de données concernant les patients dans les médias sociaux doit se faire d'une manière qui ne permette en aucun cas de les identifier. (Exemple V)
10. Les droits accordés aux exploitants des médias sociaux sur les contenus publiés (photos, vidéos, graphiques, textes et informations) devraient être examinés avec le plus grand soin.
11. Il est recommandé d'effectuer régulièrement des recherches sur sa propre personne dans les médias sociaux pour vérifier si des publications pourraient avoir un impact sur sa réputation personnelle ou professionnelle.
12. La protection de l'accès aux comptes des médias sociaux est une mesure essentielle pour garantir la sécurité des informations personnelles.
13. Le réglage des paramètres de protection des données sur les réseaux sociaux est une mesure importante pour la protection de la sphère privée.
14. Il est conseillé de réagir de manière réfléchie aux contributions d'autres utilisatrices et utilisateurs sur les médias sociaux. Des réponses précipitées et irréfléchies peuvent conduire à des malentendus ou nuire à sa propre réputation.

Services de messagerie

15. L'utilisation des services de messagerie doit se faire dans le strict respect des dispositions légales et des règles déontologiques.
16. Il convient de définir quels services de messagerie seront utilisés pour communiquer avec les patients et de le communiquer clairement.
17. Les services de messagerie peuvent être utilisés pour la communication entre professionnels de santé, mais dans le strict respect des dispositions relatives à la protection des données.
18. En cas d'utilisation de services de messagerie, il convient de communiquer quels sont les contenus électroniques acceptés et les conditions de leur traitement.
19. Toute donnée sensible, personnelle et/ou médicale, doit être protégée de manière systématique et permanente par des technologies de chiffrement en cas de transmission au moyen de services de messagerie.
20. Lors de demandes de contact via des services de messagerie, il est recommandé de vérifier l'identité de la personne à l'origine de la demande et d'éviter de divulguer des informations personnelles sans avoir vérifié au préalable la fiabilité du contact.

Photos de patientes et patients

21. Afin de préserver les droits de la personnalité et la protection des données, le consentement est une priorité absolue lors de la publication de photos dites « avant-après ». (Exemple VI)
22. Avant d'utiliser des appareils dotés d'une fonction caméra, il convient de s'assurer que tous les systèmes d'enregistrement basés sur le cloud ainsi que la fonction GPS sont désactivés.
23. Il est impératif de supprimer ou de masquer tous les éléments permettant d'identifier les personnes sur les photos avant de les transmettre via un service de messagerie et de les publier sur les médias sociaux.
24. La publication d'images inversées (avec effet miroir) devrait être évitée, car cela peut conduire à des interprétations erronées et à des diagnostics incorrects.

Chapitre 1 : Introduction

Contexte et pertinence des médias sociaux et des services de messagerie dans l'exercice quotidien de la médecine

Les médias sociaux (en anglais *Social Media*), dont les plateformes telles que Facebook, X, LinkedIn et Instagram, ainsi que les services de messagerie sociale (messages directs) tels que WhatsApp, Threema et Telegram, présentent une grande utilité pour l'activité médicale, mais en modifient également de nombreux aspects. Parmi leurs atouts figurent la communication entre professionnels de santé, la promotion du travail en réseau et de la collaboration entre les professionnels de santé, le soutien à la formation prégraduée, postgraduée et continue, et le dialogue avec les patientes et patients. Les médias sociaux contribuent également à la diffusion d'informations et de connaissances pertinentes en matière de santé et soutiennent la mise en œuvre de mesures dans le domaine de la santé publique.

Bien que les médias sociaux et les services de messagerie soient parfois regroupés sous le terme de « réseaux sociaux », ils présentent d'importantes différences quant à leurs objectifs et à leurs fonctions.

1. **Forme et objectif de la communication**

- **Médias sociaux :** les plateformes telles que Facebook, Instagram et X sont principalement conçues pour partager des contenus en public ou au sein d'un réseau d'abonnés et pour échanger publiquement. L'accent est mis sur la diffusion d'informations, le divertissement, la présentation de soi et le débat public.
- **Services de messagerie :** les plateformes telles que WhatsApp, Threema et Telegram sont conçues en premier lieu pour la communication privée (éventuellement au sein de groupes). Elles permettent aux utilisatrices et utilisateurs d'échanger des messages, des photos, des vidéos et des fichiers de manière directe (et partiellement chiffrée). Le contenu n'est pas accessible publiquement.

2. **Sécurité et protection des données**

- **Médias sociaux :** en raison de la nature (semi-)publique des contributions, la sécurité et la protection des données posent régulièrement question. Même si les utilisatrices et utilisateurs peuvent personnaliser leurs paramètres de confidentialité, les informations sont en principe accessibles à un public plus large.
- **Services de messagerie :** de nombreuses applications de messagerie mettent l'accent sur la sécurité et la protection des données, notamment grâce au chiffrement de bout en bout, qui empêche les tiers d'accéder aux communications. Cet accent sur les conversations privées signifie que les données et les messages personnels sont mieux protégés, à condition que les paramètres de sécurité soient gérés de manière stricte.

3. **Modèles d'interaction et création de réseaux**

- Les **médias sociaux** permettent aux utilisatrices et utilisateurs de partager des contenus, de les commenter et d'interagir ainsi avec un large public. La création de réseaux est souvent moins personnelle, mais elle a une grande portée et une visibilité publique.
- Les **services de messagerie** servent à l'échange direct de messages entre des individus ou des groupes. L'interaction est généralement ciblée et personnelle, et la création de réseaux se fait à un niveau plus personnel et doit en principe respecter la sphère privée.

Le Code de déontologie de la FMH « règle le comportement du médecin envers ses patients, ses confrères, les autres partenaires de la santé publique et la société ». Les règles de conduite et de déontologie établies conservent toute leur validité dans le cadre de l'utilisation des médias sociaux et des services de messagerie. Outre les bases légales nationales et cantonales générales et spécifiques à la profession, de nombreux établissements ont édicté des directives internes sur la communication et sur l'utilisation des réseaux sociaux, qu'il convient aussi de respecter. Il est recommandé aux médecins qui emploient des étudiants en médecine ou d'autres spécialistes (personnel de santé ou auxiliaire) de sensibiliser leur personnel aux risques spécifiques des médias sociaux et des services de messagerie dans le milieu médical et de réglementer leur utilisation.

Les présentes recommandations de la FMH sur l'usage des médias sociaux et des services de messagerie ont pour but d'aider les médecins à interpréter et à appliquer correctement le Code de déontologie de la FMH et de les soutenir dans l'instruction de leur personnel.

Défis liés à l'utilisation des médias sociaux et des services de messagerie

Un comportement imprudent ou des contributions irréfléchies sur internet peuvent avoir des conséquences bien plus problématiques que lors d'une conversation, d'un exposé ou dans des médias imprimés. Ces actions peuvent porter atteinte à la sphère privée et à l'intégrité personnelle des médecins comme des patientes et des patients, affecter la relation médecin-patient ou les relations avec les collègues. En outre, elles peuvent avoir des conséquences juridiques.

Les cybercriminels exploitent de manière ciblée la popularité des réseaux sociaux, par exemple pour commettre des délits tels que l'usurpation d'identité, l'utilisation abusive de données privées rendues publiques, les attaques par hameçonnage, le harcèlement et la publication, intentionnellement ou par négligence, de secrets d'affaires.

L'information, la communication et la collaboration via les médias sociaux et les services de messagerie soulèvent différentes questions quant à leurs possibilités et à leurs limites. Cela concerne notamment :

- **Secret médical et protection des données :** comment les médecins peuvent-ils protéger les données de leurs patientes et patients en cas d'utilisation des médias sociaux ? Quelles informations a-t-on le droit de transmettre via les services de messagerie ?
- **Communication et relations professionnelles :** les médecins doivent-ils refuser les demandes d'ajout de patients sur Facebook ? À quoi faut-il prêter attention lors de discussions de cas ou de commentaires concernant des collègues sur les réseaux sociaux ?
- **Information, communication et publicité :** quelles sont les règles à respecter lorsqu'un cabinet médical souhaite annoncer son ouverture ou communiquer publiquement au sujet de mesures de prévention ?
- **Photos de patientes et patients :** comment procéder lors de prises de vue pendant le traitement médical et quelles images peut-on publier dans les médias sociaux ?

Démarche de la FMH et champ d'application

Les présentes recommandations ont pour but de guider et d'accompagner le corps médical en signalant les risques et en mettant l'accent sur le bon usage et sur l'utilisation prudente des médias sociaux et des services de messagerie dans l'activité médicale quotidienne.

Elles traitent de la protection des données, des relations professionnelles, de l'information, de la communication et de la publicité. Le chapitre 2 est consacré aux médias sociaux, le chapitre 3 aux services de messagerie et le chapitre 4 aux photos de patientes et patients. Pour faciliter la compréhension, les points particulièrement délicats et les risques spécifiques à l'utilisation des médias sociaux et des services de messagerie dans l'environnement médical sont illustrés par des exemples pratiques.

Pour élaborer ses recommandations, la FMH s'est basée sur les expériences, recommandations et directives de différents pays et organisations médicales. Elle n'a pas tenu compte des détails techniques, des instructions concrètes ou des spécifications de fournisseurs, d'applications, etc. Les sociétés cantonales de médecine peuvent également émettre des directives et des recommandations dans ce domaine afin de tenir compte des spécificités régionales.

Chapitre 2 : Médias sociaux

Les plateformes telles que Facebook, Instagram, LinkedIn, YouTube et X se concentrent principalement sur le partage de contenus, soit publiquement, soit au sein d'un réseau d'abonnés, afin de favoriser un large échange. Elles ont pour but de diffuser des informations et d'alimenter les débats publics, en mettant l'accent sur la transmission d'informations et, de plus en plus, sur le divertissement. Les dynamiques d'interaction sur ces plateformes sont conçues pour s'adresser à un large public et établir des liens entre les individus ayant des intérêts similaires et entre les utilisateurs et les institutions publiques, mais aussi pour permettre un débat scientifique au sein de la société.
Compte tenu de la nature au moins partiellement publique des contributions, le secret médical ainsi que la sécurité et la protection des données représentent un véritable défi. Malgré la possibilité de personnaliser les paramètres de confidentialité, les informations partagées restent en principe visibles pour un large public.

Information, communication, publicité

Le Code de déontologie de la FMH encourage la participation active des médecins dans les débats publics, y compris la collaboration avec la presse écrite, audiovisuelle et les médias numériques. La publicité et l'information dans les médias sociaux sont soumises aux mêmes règles que celles qui se rapportent aux médias traditionnels : dans leur activité professionnelle, les médecins se gardent de recourir à une publicité non objective, mensongère ou qui pourrait nuire à la réputation de la profession médicale[1]. Les détails à ce sujet, notamment la mise à disposition d'informations appropriées au public visé, sont réglés à l'annexe 2 du Code de déontologie « Directives pour l'information et la publicité ».

Les sociétés cantonales de médecine sont aussi habilitées à définir des règles spécifiques concernant les modalités, par exemple le canal et le format, des informations autorisées. La FMH recommande à ses membres de prendre contact avec leur société cantonale afin de clarifier ces points.

Recommandation 1 : L'utilisation des médias sociaux à des fins professionnelles doit faire l'objet d'un examen critique tenant également compte des ressources nécessaires (temps, connaissances et budget).

Explication : la prudence est de mise lors du partage de contenus par l'intermédiaire des médias sociaux. Il est conseillé de se familiariser avec les différentes possibilités afin de prendre une décision éclairée sur le contenu et le format adaptés pour la publication d'informations concernant son activité médicale et son cabinet médical. Le contenu doit avant tout être de qualité. Il est important de réfléchir aux canaux utilisés, de développer soigneusement le contenu, de répondre aux commentaires en temps utile et de respecter le secret médical et les directives sur la protection des données. Ces activités nécessitent un investissement en temps ainsi que des connaissances spécifiques.

Recommandation 2 : Seules les informations nécessaires à l'activité professionnelle et utiles pour la patientèle, les proches, les collègues et les clients devraient être publiées sur les comptes professionnels dans les médias sociaux.

Explication : sur les réseaux sociaux, les contenus se propagent rapidement et peuvent rester visibles de manière permanente pour un nombre indéterminé et incontrôlé de personnes. Le Code de déontologie de la FMH autorise les médecins à publier leurs qualifications professionnelles et les informations nécessaires à leurs patients et à leurs collègues en faisant usage de réserve et de modestie (cf. art. 20 du Code de déontologie). Il est permis de partager des informations relevant de l'activité médicale (informations scientifiques, prévention) et de l'offre de prestations (cabinet, infrastructure, horaires, possibilités de contact et équipe), et de les modifier. Outre le site internet du cabinet, les médias sociaux peuvent aussi servir de plateforme pour échanger ces informations. Ils offrent également aux professionnels de santé la possibilité de fournir des renseignements sur la prévention des maladies, les options thérapeutiques et la recherche médicale actuelle, contribuant ainsi à la sensibilisation à la santé et à l'éducation médicale. Conformément aux dispositions de l'annexe 2 du Code de déontologie de la FMH concernant les informations autorisées et la publicité non autorisée, les contributions dans les médias sociaux doivent être formulées de manière objective, choisies avec soin, apporter une valeur ajoutée à la patientèle, aux proches ou aux clients et soutenir la prise de décision médicale. Enfin, les médias sociaux peuvent être utilisés pour les échanges entre professionnels de santé, par exemple sur des projets de recherche en cours ou des congrès.

[1] Art. 20, al. 2, Code de déontologie de la FMH

Recommandation 3 : Il convient de s'abstenir de diffuser des déclarations ambiguës ou fausses, d'éviter d'utiliser les comptes professionnels dans les médias sociaux à des fins privées et de ne pas susciter des attentes injustifiées.

Explication : dans le contexte médical, les médecins ont un rôle d'expert qui exige de leur part une communication responsable dans les médias sociaux. Il est impératif qu'ils ne s'expriment que sur des sujets sur lesquels ils disposent des compétences spécifiques requises et ne diffusent pas d'informations fausses ou ambiguës. Les contenus doivent toujours être présentés dans leur contexte et, le cas échéant, être accompagnés de renvois à des informations complémentaires afin de permettre aux non-spécialistes d'approfondir le sujet de manière adéquate. Les comptes professionnels doivent servir en priorité à communiquer des informations utiles pour la patientèle, et non à se mettre en avant. Enfin, les médecins ne doivent pas se servir des recommandations ou des commentaires de patients pour leur propre communication.

Exemple I : Publications problématiques dans les médias sociaux

Contexte
Le Dr Meier est orthopédiste et s'est spécialisé dans les problèmes de genou. Il gère un compte LinkedIn contenant de nombreuses informations, images et publications. Outre des photos du cabinet médical et de la salle d'opération, il a publié une photo de lui avec un footballeur célèbre, accompagnée du commentaire suivant : « Si vous aussi, vous voulez vous remettre au jeu rapidement en cas de problèmes de genou, venez me voir ! » En réalité, le Dr Meier n'a pas opéré le célèbre footballeur. Suite à sa publication, plusieurs membres de LinkedIn rédigent des commentaires et posent des questions sur leurs problèmes de genou. Plusieurs personnes donnent même leur nom et leur lieu de résidence.

Problème
La publication de photos du cabinet et de la salle d'opération aux côtés d'un selfie avec un footballeur connu et de la présentation de prestations et d'avis médicaux fait penser à tort que le Dr Meier a opéré ce footballeur et est donc considérée comme une mesure publicitaire illicite. Si des informations générales sur les douleurs articulaires peuvent être informatives, les conseils médicaux individuels pourraient être interprétés comme des recommandations thérapeutiques spécifiques et violer le secret médical et la sphère privée.

Solution alternative
Sur son profil LinkedIn, le Dr Meier présente des informations sur les pathologies du genou, les options chirurgicales et les résultats thérapeutiques. Dans la section « Infos » de son profil, il informe les utilisatrices et utilisateurs des règles de protection des données et de la problématique de la divulgation de données personnelles dans les commentaires publics. Enfin, il explique que la consultation en ligne n'est pas autorisée et indique ses coordonnées en vue d'une consultation dans son cabinet.

Recommandation 4 : Il est essentiel d'avoir à l'esprit que les différentes plateformes et les différents canaux présentent chacun des atouts et des risques spécifiques pour des objectifs de communication spécifiques.

Explication : les canaux des médias sociaux varient selon leur objectif, la communauté visée et le type de communication. Certaines plateformes comme Facebook, YouTube ou Instagram se prêtent plutôt à la transmission d'informations visuelles à la patientèle, tandis que d'autres, comme LinkedIn, servent principalement à la communication écrite entre professionnels. Il est important de se pencher sur les types de communication spécifiques et les modes de présentation propres à chaque format, comme l'image, le texte, la vidéo et les événements en direct.

Recommandation 5 : Les comptes privés et professionnels sur les plateformes de médias sociaux doivent être gérés séparément.

Explication : selon le Code de déontologie de la FMH, l'activité privée doit être clairement séparée de l'activité professionnelle, particulièrement en ce qui concerne la communication directe avec les patientes et patients. Les médias sociaux peuvent servir à la fois à l'échange privé avec les amis et à l'échange professionnel avec les collègues. Une séparation des comptes est donc recommandée, afin de pouvoir décider spécifiquement des contenus qui seront publiés à titre privé ou rendus accessibles au grand public à titre professionnel ou au nom d'un cabinet ou d'une organisation. Ces contenus doivent dans tous les cas respecter le Code de déontologie de la FMH. Les plateformes de médias sociaux ne sont en principe pas des moyens appropriés pour la communication médecin-patient.

Relation médecin-patient

Recommandation 6 : Les demandes d'ajout de patients sur des comptes privés doivent être considérées avec la plus grande attention.

Explication : la FMH recommande aux médecins de limiter l'accès à leurs comptes privés aux personnes de leur entourage personnel. En permettant à leur patientèle d'accéder à leur profil personnel sur les plateformes des médias sociaux, les médecins leur permettent également d'accéder à un pan de leur vie privée, ce qui n'est d'ordinaire pas le cas dans une relation médecin-patient. Exercer la profession de médecin avec soin et diligence implique également de respecter les limites professionnelles afin de protéger sa propre sphère privée et celle de ses patientes et patients. Si cette règle n'est pas respectée, des limites pourraient être facilement franchies, ce qui aurait un impact négatif sur la relation médecin-patient. Dans les médias sociaux, le seuil d'inhibition a tendance à être plus bas, ce qui peut non seulement nuire à la relation médecin-patient, mais aussi conduire à des ruptures de confidentialité et à d'autres conséquences d'ordre déontologique.

Exemple II : Vidéo privée sur Facebook

Contexte
Le Dr Stettler, médecin du sport, reçoit une demande d'ajout de S. Müller sur son compte privé Facebook. Cette personne ayant un voilier en photo de profil, le Dr Stettler pense qu'il s'agit d'un collègue du club de voile et accepte la demande. Ce n'est que plus tard qu'il réalise que S. Müller est en réalité un patient. Celui-ci lui demande une copie des derniers résultats de laboratoire et tombe sur une vidéo privée du Dr Stettler, qui le montre légèrement alcoolisé, en train de faire la fête. Lors de la consultation suivante, S. Müller se montre distant, la relation médecin-patient est tendue et le rapport de confiance est altéré. Après plusieurs consultations, S. Müller finit par changer de médecin.

Problème
La relation médecin-patient entre S. Müller et le Dr Stettler, jusqu'alors professionnelle, a été influencée négativement par l'aperçu que S. Müller a eu de la vie privée de son médecin. Le contenu de la vidéo ne correspondait pas à l'image et aux attentes que S. Müller avait envers le Dr Stettler, ce qui lui a fait perdre confiance.

Solution alternative
Le Dr Stettler gère, en plus de son compte privé, un compte Facebook professionnel pour son cabinet orthopédique. Grâce à une vérification consciencieuse des demandes d'ajout sur son compte privé, il se souvient de son patient S. Müller. Il l'informe, via un moyen de communication chiffré, que pour des raisons de discrétion, il n'accepte pas les demandes d'ajout de patients sur son compte privé et le renvoie gentiment à son compte professionnel public.

Recommandation 7 : En cas de commentaires négatifs sur les médias sociaux, il est recommandé de réagir de manière réfléchie afin de préserver son image et de contribuer à un débat public respectueux.

Explication : préserver sa réputation dans l'espace public revêt également une grande importance pour les médecins. Des évaluations injustifiées ou négatives peuvent avoir des conséquences émotionnelles, voire existentielles. Les évaluations négatives infondées représentent aussi un problème non négligeable pour la communauté médicale. Elles génèrent souvent des situations juridiques complexes, en particulier s'agissant des réglementations spécifiques à la profession telles que le secret professionnel. De plus, il est difficile pour les médecins de prendre position face à des évaluations rédigées de manière anonyme. En outre, sans l'accord de la patiente ou du patient ou une levée officielle du secret médical par l'autorité de surveillance cantonale, y répondre constituerait une rupture du secret médical. Les « Recommandations de la FMH concernant la gestion des évaluations en ligne » ont pour but de renseigner les médecins quant à leurs possibilités de recours légaux, et de leur offrir une aide concrète.

Exemple III : Mauvaise évaluation Google

Contexte
La Dre Gruber est spécialiste en médecine interne générale et médecin de famille. En plus du site internet de son cabinet et d'un compte Facebook, elle gère également un profil d'entreprise Google sur lequel les personnes peuvent donner publiquement des avis sur la Dre Gruber et son cabinet. Elle reçoit l'avis suivant : « Non seulement j'ai attendu longtemps, mais en plus je n'ai pas eu de réponse à mes questions. La Dre Gruber n'a rien pu dire sur mes douleurs abdominales, si ce n'est qu'elle ne savait pas de quoi il s'agissait et qu'elle devait m'adresser à l'hôpital cantonal pour une coloscopie. Une vraie perte de temps. » (une étoile) La Dre Gruber se souvient du cas et sait, malgré l'anonymat de la personne à l'origine de l'évaluation, qui a écrit cette évaluation. Elle répond directement sur son profil d'entreprise Google avec le message suivant : « Madame, merci pour votre réaction. Malheureusement, en tant que médecin de famille, je n'ai pas les moyens d'examiner votre cas de manière approfondie. Vos symptômes n'indiquent pas nécessairement une maladie grave, mais je ne pouvais pas non plus l'exclure. Dans des cas comme le vôtre, il est important de se faire examiner par une personne spécialisée en chirurgie viscérale. »

Problème
Dans sa réponse, la Dre Gruber aborde les antécédents médicaux de la patiente. Elle viole ainsi le secret médical, car les avis Google sont publics. En outre, en mentionnant le sexe de la patiente, elle fournit une information susceptible de permettre son identification.

Solution alternative
La Dre Gruber prend position de manière neutre et sans fournir aucun détail sur les antécédents de la patiente : « Bonjour, merci beaucoup pour votre réaction. Il est courant que les cabinets de médecins de famille doivent orienter les patients vers des spécialistes pour mieux cibler le diagnostic. Je regrette que vous ayez pu l'interpréter comme une absence de réponse à vos questions. Cela ne reflète en aucun cas nos valeurs. En raison du secret médical, je ne peux pas me pencher ici en détail sur votre cas. Je vous invite à prendre contact avec nous par téléphone. »

Relation médecin-médecin

Recommandation 8 : Il convient de veiller à ne pas publier de contenus inappropriés sur les médias sociaux et à prévenir les collègues en cas de publications inappropriées de leur part.

Explication : des allégations inappropriées, offensantes ou fausses dans des publications concernant des collègues ou dans des commentaires sur leurs publications peuvent nuire à long terme à la réputation de la profession médicale. Les dispositions de l'article 23 du Code de déontologie concernant la collégialité et les critiques inadmissibles s'appliquent également à l'espace public numérique des médias sociaux. Les médecins sont donc tenus d'entretenir entre eux des rapports confraternels, empreints d'honnêteté et de courtoisie, y compris sur les plateformes sociales, et d'éviter tout comportement susceptible de discréditer une ou un collègue sans juste motif. Dans la communication avec des tiers, y compris avec les autorités, les médecins font preuve de retenue et d'objectivité concernant les mesures médicales prises par des collègues.

Exemple IV : Déclarations publiques sur le comportement de collègues

Contexte
Le Dr Müller, chef de clinique, publie sur son compte public LinkedIn le commentaire suivant concernant un collègue des urgences :
Cher collègue P. du Service des urgences,
Je vous remercie d'avoir mal interprété les douleurs abdominales de Mme R. B., 1.1.1932, comme relevant d'une constipation et de lui avoir administré des laxatifs. Je suis sûr que la patiente vous est également reconnaissante pour la perforation intestinale qui s'en est suivie, avec choc septique et défaillance multiorganique. Elle a besoin d'un foie frais maintenant. Avec votre excellent savoir-faire médical, je suis sûr que vous l'aiderez à trouver un nouvel organe !
Meilleurs messages, Dr Müller, chef de clinique, USI

Problème
Les propos du Dr Müller sur son collègue contreviennent aux règles du Code de déontologie de la FMH et peuvent avoir des conséquences civiles et pénales. Une telle publication sur LinkedIn est accessible au public et pourrait être interprétée comme portant atteinte à la réputation ou être diffamatoire. En outre, les informations publiées, associées aux données d'autres plateformes, pourraient permettre de tirer des conclusions sur le médecin concerné et l'identité de la patiente.

Solution alternative
Le Dr Müller envoie à son collègue du Service des urgences, via son courriel clinique chiffré, un rapport factuel sur le diagnostic et l'évolution de Mme R. B., dans le sens d'un feed-back professionnel. Le Dr P. réalise son erreur d'interprétation et prend position à ce sujet. Dans une analyse de cas commune, ils recherchent les causes de l'interprétation et du traitement erronés du Dr P. Sur une plateforme interne de discussion de cas cliniques, ils discutent de ce cas inhabituel mais instructif avec leurs collègues et les médecins en formation, tout en garantissant l'anonymat des personnes impliquées et de la patiente en omettant les noms, les initiales et les dates.

Secret médical et protection des données

Recommandation 9 : Le partage d'informations et de données concernant les patients dans les médias sociaux doit se faire d'une manière qui ne permette en aucun cas de les identifier.

Explication : le partage de textes et d'images sur les médias sociaux comporte le risque que des données personnelles soient rendues publiques par inadvertance. Il est donc important de supprimer ou de modifier toutes les données personnelles (p. ex. initiales, date de naissance, profession, domicile) lors du partage d'informations concernant les patients dans les médias sociaux. Une simple anonymisation ou pseudonymisation n'est souvent pas suffisante, car il est

possible de rétablir l'identité d'une personne en combinant ces données avec des informations provenant d'autres sources telles que des blogs, des forums ou des sites internet. Afin de garantir une description anonyme du cas, le nombre de catégories d'informations partagées (p. ex. sexe, maladie, traitement) devrait également être réduit au strict minimum.

Exemple V : Article de blog sur un cas rare

Contexte
La Dre Feller, cheffe de clinique, exerce la médecine intensive dans un hôpital cantonal. Elle s'occupe du cas rare d'une patiente atteinte de tétanos. Sur son profil LinkedIn accessible au public, la Dre Feller relate périodiquement l'évolution de la maladie de sa patiente P. L., 46 ans, afin de partager son expérience avec ses collègues. En même temps, elle respecte le secret médical et ne mentionne ni le nom de sa patiente ni l'hôpital dans lequel elle est prise en charge. Cependant, elle publie une photo prise avec son téléphone portable sur laquelle on voit la patiente de dos, présentant une courbature typique des muscles du dos. Le visage de la patiente n'est pas visible, mais ses cheveux le sont. Inquiet, un collègue de travail de la patiente souhaite savoir dans quel hôpital elle se trouve. Lors de ses recherches sur internet, il tombe sur un rapport concernant la réorganisation des urgences de l'hôpital en question, dans lequel le nom de la cheffe de clinique, la Dre Feller, est mentionné. Il tombe sur ce même nom dans une autre publication LinkedIn commentée par une connaissance. En combinant les informations du rapport et de la publication LinkedIn, et en connaissant l'âge de sa collègue de travail, ses initiales et sa couleur de cheveux, il apprend des informations confidentielles sur Mme Petra Lässer et son tétanos.

Problème
La combinaison d'informations illustrée dans cet exemple annule l'anonymat souhaité par la cheffe de clinique ; la protection des données n'est donc plus garantie, ce qui constitue une rupture du secret médical.

Solution alternative
Si la Dre Feller ne publie pas les initiales, l'âge et la photo de la patiente ou si elle les modifie (p. ex. patiente A. A., âge moyen), la patiente ne peut pas être identifiée par son collègue de travail. Même avec la description du cas par un confrère sur un blog ou un réseau professionnel accessible exclusivement aux étudiants en médecine et aux médecins (p. ex. Doctornet), il ne serait ainsi pas possible d'identifier la patiente.

Recommandation 10 : Les droits accordés aux exploitants des médias sociaux sur les contenus publiés (photos, vidéos, graphiques, textes et informations) devraient être examinés avec le plus grand soin.

Explication : les conditions générales d'utilisation des médias sociaux peuvent stipuler des droits étendus sur l'utilisation des données. Un examen peu attentif et une acceptation hâtive des conditions générales peuvent avoir pour conséquence l'octroi de consentements qui rendent également les données accessibles à des tiers dans un tout autre contexte. Les conditions et les paramètres de confidentialité sont également susceptibles d'être modifiés et doivent donc être vérifiés régulièrement. Il faut en outre garder à l'esprit que les données sur les réseaux sociaux sont souvent moins bien protégées que dans le cadre de l'e-banking, par exemple. Il n'est jamais possible d'exclure entièrement que des données soient rendues accessibles à des tiers en dehors des accords contractuels, que ce soit par des moteurs de recherche, des attaques informatiques ou des failles de sécurité chez les exploitants des plateformes.

Recommandation 11 : Il est recommandé d'effectuer régulièrement des recherches sur sa propre personne dans les médias sociaux pour vérifier si des publications pourraient avoir un impact sur sa réputation personnelle ou professionnelle.

Explication : il arrive de plus en plus souvent que des patients, des collègues, des partenaires ou des employeurs (actuels ou futurs) recherchent des informations personnelles et professionnelles sur internet et dans les médias sociaux. Les publications et contributions peu flatteuses, un langage inapproprié ou des informations partagées avec une franchise excessive peuvent avoir des répercussions négatives sur l'environnement professionnel, sur les futures relations médecin-médecin et médecin-patient, ainsi que sur la carrière professionnelle. En outre, les personnes et les groupes impliqués dans des activités criminelles peuvent recourir aux informations personnelles pour mener des cyberattaques ciblées (attaques d'ingénierie sociale[2]).

En cas de découverte de contenus inappropriés ou problématiques sur les réseaux sociaux, il convient de demander à l'exploitant de la plateforme de les supprimer. Le règlement européen sur la protection des données et la loi suisse sur la protection des données garantissent le droit à l'effacement des données à caractère personnel. Ce processus peut cependant nécessiter du temps et des efforts, d'autant plus que de nombreuses plateformes (p. ex. Google ou Facebook) ne proposent pas de service client facilement accessible. Les « Recommandations de la FMH concernant la gestion des évaluations en ligne » ont pour but de renseigner les médecins quant à leurs possibilités de recours légaux, et de leur offrir une aide concrète.

[2] https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-private/aktuelle-themen/social-engineering.html

Recommandation 12 : La protection de l'accès aux comptes des médias sociaux est une mesure essentielle pour garantir la sécurité des informations personnelles.

Explication : il est indispensable de protéger scrupuleusement son identité dans les médias sociaux. Un moyen efficace pour ce faire est d'utiliser un mot de passe unique pour chaque plateforme. Un mot de passe fort se compose d'une combinaison de lettres, de chiffres et de caractères spéciaux et est suffisamment long pour ne pas être facilement deviné ou cassé par des outils automatisés. En outre, il est recommandé d'activer l'authentification à deux facteurs chaque fois que cela est possible. Pour des recommandations concrètes en matière de mots de passe et d'autres conseils sur la sécurisation de la présence en ligne, il est possible de consulter les « Exigences minimales pour la sécurité informatique des cabinets médicaux ».

Recommandation 13 : Le réglage des paramètres de protection des données sur les réseaux sociaux est une mesure importante pour la protection de la sphère privée.

Explication : il est conseillé de configurer soigneusement les paramètres de confidentialité des comptes personnels et professionnels dans les médias sociaux. Les paramètres par défaut doivent être examinés de manière critique, car ils permettent de contrôler quelles informations sont partagées et avec qui. Différentes options permettent de contrôler la visibilité des données personnelles, des publications et des listes de contacts. Les comptes personnels doivent être paramétrés sur « privé », afin que les publications, les images, les commentaires, la liste des contacts, etc., ne soient pas accessibles publiquement. Les paramètres des fonctions de commentaire et de marquage devraient être définis de manière restrictive afin de pouvoir contrôler chaque commentaire, marquage et mention avant publication. Il faudrait également vérifier régulièrement si les paramètres choisis correspondent encore au niveau de protection souhaité et procéder à des ajustements lorsque les fonctionnalités des plateformes ou les exigences personnelles en matière de protection de la sphère privée évoluent.

Recommandation 14 : Il est conseillé de réagir de manière réfléchie aux contributions d'autres utilisatrices et utilisateurs sur les médias sociaux. Des réponses rapides et irréfléchies peuvent conduire à des malentendus ou nuire à sa propre réputation.

Explication : les activités telles que les commentaires, les likes et les partages/reposts effectués avec un compte public ou privé peuvent également être visibles par des utilisatrices et utilisateurs avec lesquels il n'existe aucun lien direct. Il est donc conseillé de contribuer de manière réfléchie et consciente au débat public, y compris sur son profil personnel.

Chapitre 3 : Services de messagerie

Les services de messagerie sont des plateformes numériques qui permettent un échange en temps réel de messages entre personnes ou au sein d'un groupe spécifique. Ces services sont principalement axés sur une interaction ciblée et privée, garantissant la confidentialité des communications. Ils offrent la possibilité de transmettre des messages ainsi que des contenus multimédias tels que des photos, des vidéos et des documents par voie directe et en partie chiffrée, les contenus n'étant pas visibles en dehors du cercle de communication concerné. Nombre de ces applications mettent un accent particulier sur les aspects de sécurité et sur la protection des données de leurs utilisatrices et utilisateurs, notamment par la mise en œuvre du chiffrement de bout en bout, qui minimise le risque d'accès non autorisé par des tiers. Dans le milieu médical, la communication par l'intermédiaire de plateformes numériques doit être conforme aux standards relatifs aux consultations de télémédecine.

En Suisse, il n'existe pas de recommandations uniformes sur les conditions d'une utilisation conforme à la protection des données du service de messagerie WhatsApp, de loin le plus utilisé. Les présentes recommandations s'inspirent des conditions posées par une autorité allemande de protection des données et des recommandations concernant les paramètres de sécurité publiées par l'Office fédéral allemand de la sécurité des technologies de l'information (BSI). La FMH recommande aux médecins de n'utiliser les services de messagerie que pour l'administratif et après avoir obtenu le consentement de la patiente ou du patient. Toute communication par l'intermédiaire de services de messagerie est également soumise à l'obligation de documentation et doit à ce titre être inscrite dans le dossier médical.

Information, communication, publicité

Recommandation 15 : L'utilisation des services de messagerie doit se faire dans le strict respect des dispositions légales et des règles déontologiques.

Explication : bien que les services de messagerie permettent une communication rapide et efficace, ils doivent néanmoins respecter les dispositions relatives au secret médical ainsi que les directives en matière de protection des données, notamment la loi fédérale sur la protection des données (LPD) et l'ordonnance sur la protection des données (OPDo). Leur utilisation pour communiquer avec la patientèle, les proches et les clients dans le cadre de l'activité médicale doit donc se faire après mûre réflexion, dans le respect des dispositions relatives au secret médical et uniquement avec le consentement explicite des patientes et des patients (déclaration de consentement de la FMH).

Relation médecin-patient

Recommandation 16 : Il convient de définir quels services de messagerie seront utilisés pour communiquer avec les patients et de le communiquer clairement.

Explication : il convient d'examiner de manière critique dans quelle mesure les services de messagerie peuvent être utilisés comme moyens de communication d'appoint dans la pratique médicale, en tenant compte en particulier du secret médical et de la protection des données. Il est recommandé d'informer les patientes et patients concernant les canaux de communication autorisés. Ces informations doivent leur être clairement communiquées lors de la signature du formulaire de consentement et d'entretiens personnels, sur le site internet du cabinet ou dans les médias sociaux. Les demandes de contact ne devraient être traitées que si elles ont lieu sur ces canaux prédéfinis. En règle générale, les cabinets médicaux utilisent un système de courriers électroniques chiffrés pour l'échange de données sensibles concernant la patientèle. L'utilisation de services de messagerie pour la relation médecin-patient n'est donc recommandée que pour gérer l'administratif telles que les prises de rendez-vous. Pour tout autre type de données, la FMH préconise l'utilisation de courriels chiffrés.

Relation médecin-médecin

Recommandation 17 : Les services de messagerie peuvent être utilisés pour la communication entre professionnels de santé, mais dans le strict respect du secret médical et des dispositions relatives à la protection des données.

Explication : lors de la communication par l'intermédiaire de services de messagerie, toutes les dispositions applicables en matière de protection des données doivent être prises en compte, et en particulier le secret médical et la protection des données des patients. Rappelons que le secret médical s'applique aussi entre professionnels de santé lorsque ceux-ci ne sont pas impliqués dans le traitement de la patiente ou du patient concerné. Il est essentiel d'utiliser un service qui offre un chiffrement de bout en bout afin de garantir en tout temps la confidentialité et l'intégrité des informations communiquées. Avant d'utiliser ces outils, il convient de définir des directives claires concernant leur usage et de préciser notamment le type d'informations pouvant être transmises et les responsabilités des utilisatrices et utilisateurs.

Protection des données

Recommandation 18 : En cas d'utilisation de services de messagerie pour la communication médecin-patient, il convient de préciser quels sont les contenus électroniques acceptés et les conditions de leur traitement.

Explication : afin de minimiser le risque de transmission de contenus non sollicités par les patients, il est utile de définir et de communiquer précisément quels types de contenus électroniques sont acceptés, par exemple images, vidéos, documents, échographies, clichés IRM ou radiographies, et par quels moyens de communication les échanger. En outre, il convient d'indiquer de manière transparente à quel endroit les contenus sont stockés et traités et quels sont les délais de réponse auxquels les patients peuvent s'attendre. Pour les demandes via Messenger, il peut être utile de configurer une réponse automatique avec ces informations. Certaines applications, comme WhatsApp, offrent la possibilité de configurer des confirmations de lecture.

Recommandation 19 : Toute donnée sensible, personnelle et/ou médicale, doit être protégée de manière systématique et permanente par des technologies de chiffrement en cas de transmission au moyen des services de messagerie[3].

Explication : les documents contenant des données personnelles sensibles (p. ex. certificats d'incapacité de travail) sont susceptibles d'être falsifiés en cas de transmission non sécurisée. De même, des données telles que le nom du médecin qui a délivré le certificat, la signature, etc., pourraient être consultées par des tiers.

La FMH recommande donc de protéger de manière systématique et permanente toute donnée sensible, personnelle et/ou médicale, par des technologies de chiffrement lors d'échanges électroniques. Dès qu'il s'agit de données de patients, le secret médical doit également être respecté. L'échange de messages non chiffrés (via des services de courriers électroniques ou des réseaux sociaux non chiffrés) ne permet pas de garantir la confidentialité et le respect du secret médical. Or la violation des dispositions relatives à la protection des données peut avoir des conséquences pénales. Le chiffrement garantit qu'en cas d'accès physique de tiers aux supports de stockage, les données ne peuvent pas être lues ou comprises sans la clé de chiffrement.

Si le message ne contient aucune donnée concernant la patiente ou le patient (p. ex. simple demande de rendez-vous), et qu'il n'est donc pas possible de l'identifier, le message peut également être envoyé de manière non chiffrée. Pour cela, il faut toutefois obtenir au préalable le consentement écrit de la patiente ou du patient. Si les patients écrivent un message de leur propre initiative, nous recommandons de ne pas inclure dans la réponse d'autres données personnelles que celles qu'ils ont eux-mêmes mentionnées dans leur message.

[3] WhatsApp : utilise par défaut le chiffrement de bout en bout pour les messages et les appels.
Signal : offre un chiffrement strict de bout en bout pour toutes les communications.
Telegram : offre un chiffrement de bout en bout dans les « chats secrets », ce qui n'est pas le cas par défaut pour les chats normaux.
iMessage : offre un chiffrement de bout en bout, mais uniquement entre appareils Apple.
Viber : offre un chiffrement de bout en bout pour les messages texte, les appels vocaux et les appels vidéo.
Threema : accorde une grande importance à la sécurité et à la protection des données et au chiffrement de bout en bout de tous les messages et appels.

Recommandation 20 : Lors de demandes de contact via des services de messagerie, il est recommandé de vérifier l'identité de la personne à l'origine de la demande et d'éviter de divulguer des informations personnelles sans avoir vérifié au préalable la fiabilité du contact.

Explication : il convient de faire preuve d'une grande prudence lors du recours à des services de messagerie pour la communication avec des collègues. Ces services ne permettent pas toujours de garantir à 100 % l'identité et l'authenticité des personnes à l'origine des demandes, qu'il s'agisse de patients demandant par exemple des résultats de laboratoire ou de médecins et d'autres professionnels de santé. Dans le cas où des tiers se feraient passer pour les patients d'un cabinet médical ou pour des médecins traitants sur les réseaux sociaux, le secret médical pourrait être violé par la transmission de données relatives aux patients. Pour minimiser ces risques, l'identité de ces personnes, y compris des professionnels de santé, devrait être systématiquement vérifiée. Une méthode consiste à utiliser des services spécialisés tels que Health Info Net SA (HIN), qui propose à ses membres un système de vérification de l'identité[4]. En outre, les professionnels de santé peuvent prouver leur identité par des documents officiels tels que la carte de professionnel délivrée par la direction cantonale de la santé ou l'Office fédéral de la santé publique, responsables de l'enregistrement et de l'octroi des autorisations au personnel médical. Pour certaines professions du secteur de la santé, il existe également des registres comme le Registre des professions médicales.

[4] Référence en matière de sécurité simple dans le système de santé (hin.ch)

Chapitre 4 : Photos de patientes et patients

L'imagerie médicale joue un rôle important dans le diagnostic et le traitement, en particulier dans les spécialités comme la dermatologie et la chirurgie plastique. Les prises de vue sont utilisées non seulement pour informer les patients concernant les procédures, les traitements et le suivi, mais aussi à des fins d'enseignement, de recherche et de publication. Elles sont également importantes pour obtenir un deuxième avis de la part de collègues ou de personnes de conseil.

Les recommandations ci-après sur l'utilisation des images médicales dans les médias sociaux et les services de messagerie supposent que les patients ont été au préalable informés de l'utilisation des prises de vue les concernant et que leur consentement à la prise de vue a été recueilli. Elles mettent l'accent sur les mesures préventives pour une prise de vue consciencieuse et sur la dé-identification ultérieure plutôt que sur l'effacement des données personnelles. En ce qui concerne l'utilisation consciencieuse des photos de patients, il convient également de consulter les « Recommandations relatives à la protection des données ».

Recommandation 21 : Afin de préserver les droits de la personnalité et la protection des données, le consentement est une priorité absolue lors de la publication de photos dites « avant-après ».

Explication : la publication de photos « avant-après » sur les services de messagerie et les médias sociaux est uniquement autorisée lorsque ces images ont un lien direct avec une intervention médicalement indiquée. Les images publiées doivent servir à informer ainsi qu'à documenter et à illustrer le succès de l'intervention, et ne doivent pas être utilisées à des fins principalement publicitaires. En outre, il convient d'obtenir le consentement explicite et éclairé des personnes représentées, le respect des droits de la personnalité et de la protection des données étant une priorité absolue. Il convient également de s'assurer que la publication n'entraîne pas une violation de la sphère privée ou ne dénigre pas d'une quelconque manière les personnes représentées. La publication de photos « avant-après » pour des interventions de nature purement esthétique n'est pas autorisée. Ces images ne contiennent pas d'informations nécessaires et pourraient inciter des personnes à subir des interventions médicales dont elles n'ont objectivement pas besoin.

Exemple VI : Dilemme éthique et juridique concernant l'utilisation des smartphones personnels pour photographier les patients

Contexte
Une patiente de 45 ans est adressée à un chirurgien plasticien pour une abdominoplastie après avoir perdu 80 kg suite à une petite gastrectomie. Elle se plaint d'un excès de peau sur tout le corps, qui la gêne dans sa vie sociale et quotidienne. Après avoir étudié son cas, le chirurgien décide de procéder à plusieurs interventions, en commençant par une abdominoplastie. Il lui explique en quoi consiste l'intervention et recueille son consentement. Lors de la visite préopératoire, le chirurgien lui demande l'autorisation de prendre une photo d'elle à des fins médicales. Ce qu'elle refuse, ne souhaitant pas se dénuder face au photographe de l'hôpital. Dans la salle d'opération et avant le début de l'intervention, le chirurgien réitère sa demande en lui expliquant qu'il souhaiterait comparer les images avec les clichés postopératoires. La patiente hésite, mais finit par accepter. Le chirurgien lui couvre ses parties génitales et prend des photos avec son propre smartphone. Un mois plus tard, une patiente anxieuse se présente à la clinique pour la même intervention. Le chirurgien lui explique en quoi consiste l'intervention et répond à ses questions. Pour la rassurer, il lui montre les photos pré- et postopératoires de sa précédente patiente, prises avec son propre smartphone. La nouvelle patiente accepte l'intervention.

Problème
Les smartphones personnels ne devraient pas être utilisés pour des photos à des fins médicales. Cela est susceptible d'entraîner notamment une violation de la confidentialité et de la sphère privée des patients.

Solution alternative
Si une image doit impérativement être utilisée pour la communication entre professionnels de santé, il faut obtenir au préalable un consentement écrit, après avoir expliqué l'objectif et les risques aux personnes avec lesquelles la photo est partagée. La photo doit être effacée après la consultation et le processus documenté dans le dossier de la patiente ou du patient.

Recommandation 22 : Avant d'utiliser des appareils dotés d'une fonction caméra, il convient de s'assurer que tous les systèmes d'enregistrement basés sur le cloud ainsi que la fonction GPS sont désactivés.

Explication : les appareils dotés d'une caméra sont souvent équipés d'un récepteur pour le système de positionnement mondial (GPS), qui peut enregistrer l'emplacement exact au moment de la prise de vue. La précision de ces données de localisation peut parfois être de moins de quelques mètres. Lors de la prise de vue, notamment dans un contexte médical, ces données GPS peuvent être utilisées pour identifier les patients. Il est également important de prêter attention aux informations supplémentaires enregistrées automatiquement lors de la prise de vue, les métadonnées. Ces métadonnées se présentent couramment sous la forme de données EXIF (Exchangeable Image File Format), qui sont créées et enregistrées en même temps que l'image. Les données EXIF standards comprennent généralement des

informations sur la marque de l'appareil photo, le numéro de série, la vitesse d'obturation, la distance focale, le mode de compression et les paramètres d'ouverture. Les données EXIF peuvent également inclure la date, l'heure et l'emplacement de la prise de vue.

La combinaison de l'horodatage de la photo (date et heure) avec la localisation (coordonnées GPS) peut permettre de remonter à une personne et a donc le potentiel de devenir un élément d'identification précis. Du point de vue de la protection des données, il convient donc de faire preuve de prudence. Avant d'utiliser des prises de vue dans le domaine médical, il faut s'assurer qu'aucune donnée personnelle sensible n'est révélée par les données EXIF ou d'autres métadonnées. Il est recommandé de supprimer ou d'anonymiser toutes les métadonnées qui pourraient permettre d'identifier les personnes représentées sur les images avant de les traiter, de les stocker ou de les publier.

Recommandation 23 : Il est impératif de supprimer ou de masquer tous les éléments permettant d'identifier les personnes sur les photos avant de les transmettre via un service de messagerie et de les publier sur les médias sociaux.

Explication : avant de publier des images, tout élément susceptible de permettre l'identification de la personne doit être supprimé ou masqué, afin de garantir la protection de la sphère privée et le respect des dispositions légales relatives à la protection des données. Lors de la prise de vue, il convient de s'assurer qu'aucun objet en arrière-plan ne permette de tirer des conclusions sur l'identité de la personne photographiée. Les vêtements peu communs, les bijoux et les accessoires tels que les lunettes doivent être retirés. De même, il faut veiller à ce que les éléments particuliers tels que les tatouages, les grains de beauté ou les cicatrices ne soient pas visibles. Ces éléments peuvent être masqués soit en les omettant délibérément lors du cadrage, en les recouvrant de vêtements neutres ou en retouchant la photo ultérieurement.

Recommandation 24 : La publication d'images inversées (effet miroir) devrait être évitée, car cela peut conduire à des interprétations erronées et à des diagnostics incorrects.

Explication : afin de garantir l'exactitude du diagnostic, il faut s'assurer que les images ne soient pas inversées au moment de leur transmission via les services de messagerie et les médias sociaux. De même, il convient de faire preuve d'une grande prudence lors de l'établissement d'un diagnostic sur la base d'images prises notamment avec des caméras frontales de terminaux mobiles. Nombre de ces appareils sont dotés d'une fonction d'inversion d'image par défaut, ce qui fait que certains éléments (p. ex. éruption cutanée) peuvent apparaître du mauvais côté. Pour éviter de potentielles erreurs de diagnostic, il convient de désactiver cette fonction. En outre, il est conseillé d'apposer des marques clairement identifiables afin de désigner sans ambiguïté le côté du corps concerné. Lors de la prise d'un selfie, par exemple, il est possible de lever la main du côté où se trouve l'élément à documenter. D'autres solutions sont envisageables, l'essentiel étant d'exclure toute ambiguïté pour l'observateur et de garantir une évaluation médicale correcte[5].

[5] https://jamanetwork.com/journals/jamaneurology/article-abstract/2810959#:~:text=Differing%20conventions%20of%20photographic%20representation,avoided%20the%20left%2Dright%20confusion

Bibliographie

Handreichung der Bundesärztekammer – Ärztinnen und Ärzte in sozialen Medien

Social-Media und Social-Messaging im Spital – Ethische und Rechtliche Leitlinien (Jusletter)

Making and using visual and audio recordings of patients (General Medical Council)

Anonymizing facial images to improve patient privacy

Clinical photography and our responsibilities

Experiences of Health Care Providers Using a Mobile Medical Photography Application

Medical Photography

Medical Photography using mobile devices (Zoltie et al., 2022)

Patients, pictures, and privacy: Managing clinical photographs in the smartphone era

Recommendations für Better Adoption of Medical Photography as a Clinical Tool

Glossaire

Anonymisation	L'anonymisation de données vise à supprimer tout lien avec la personne concernée. Les données anonymisées ne peuvent plus être reliées à un individu en particulier, ou seulement de manière très limitée, et réduisent ainsi le risque lié à l'utilisation des données pour cette personne[1].
Attaque d'ingénierie sociale	Les attaques d'ingénierie sociale utilisent la tromperie et la manipulation pour exploiter les faiblesses humaines et obtenir l'accès à des informations ou des systèmes sensibles.
Cybercriminels	Les cybercriminels sont des personnes ou des groupes qui se livrent à des activités illégales dans l'espace numérique, telles que le piratage, la fraude, l'usurpation d'identité ou la diffusion de logiciels malveillants, dans le but de réaliser des gains financiers ou de causer des dommages.
Data at rest	La notion de *Data at rest* fait référence aux données stockées, p. ex. sur un disque dur, une clé USB ou un serveur, et non activement transmises.
Data in transit	La notion de *Data in transit* fait référence aux données en cours de transfert d'un endroit à un autre, p. ex. lors de l'envoi d'un courriel.
Données EXIF	Les données EXIF sont des métadonnées stockées dans les images numériques et qui peuvent contenir des informations telles que la date de la prise de vue, le modèle de l'appareil, les paramètres d'exposition et l'emplacement.
GPS	Le système GPS, pour « Global Positioning System », est un système de navigation par satellite qui permet de déterminer la position exacte des objets à la surface de la Terre.
Partages	Sur les médias sociaux, les partages font référence à l'action de partager une publication, une vidéo ou un message créé par une personne ou une entreprise avec d'autres utilisateurs. Cela peut contribuer à augmenter la portée du contenu et à le rendre accessible à un public plus large.
Pseudonymisation	Par pseudonymisation, on entend le remplacement des données directement identifiantes de façon à ce que les données qui en résultent ne puissent pas être reliées à l'individu concerné par une personne malveillante ou seulement au prix d'efforts disproportionnés. L'identité de l'individu peut être rétablie uniquement à l'aide d'informations supplémentaires (p. ex. clé de chiffrement)[2].
Reposts	Un « repost » fait référence à la republication d'une publication ou d'un contenu qui existe déjà sur une plateforme de médias sociaux, mais qui est partagé par un autre utilisateur.
Secure Sockets Layers (SSL)	Secure Sockets Layer (SSL) est un protocole de chiffrement obsolète, similaire au protocole TLS (cf. ci-dessous), utilisé pour assurer la sécurité des données lors de leur transmission sur internet.
Selfie	Un selfie est une photo prise par la personne elle-même, généralement à l'aide d'un smartphone, en dirigeant l'appareil photo vers elle-même.
Téléconsultation	Une téléconsultation est une consultation ou un traitement médical qui a lieu par téléphone, appel vidéo ou par un autre moyen de communication

	numérique entre un médecin et un patient, sans qu'ils aient à se rencontrer en personne.
Transport Layer Security (TLS)	Transport Layer Security (TLS) est un protocole de chiffrement utilisé pour assurer la sécurité des données lors de leur transmission sur internet.

[1] Verfahren zur Anonymisierung und Pseudonymisierung von Daten | SpringerLink
[2] Verfahren zur Anonymisierung und Pseudonymisierung von Daten | SpringerLink

Impressum
Edition : FMH – Fédération des médecins suisses, Berne
Cette brochure a été développée par Lumina Health à la demande de la FMH.
Publication : juillet 2024
www.fmh.ch