28.05.2024

Zum Umgang mit sozialen Medien und Messenger-Diensten

Empfehlungen der FMH

In diesem Text wird aus Gründen der besseren Lesbarkeit die männliche Form genutzt; sie steht jedoch stellvertretend für alle Geschlechtsidentitäten.

Jede Haftung zur juristischen Korrektheit des Dokumentes sowie direkten oder indirekten Folgeschäden wird ausgeschlossen.

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

Inhaltsverzeichnis

ZUSAMMENFASSUNG DER EMPFEHLUNGEN

Soziale Medien

1. Eine kritische Prüfung des Einsatzes sozialer Medien zu beruflichen Zwecken ist unerlässlich. Für das Management und Monitoring müssen entsprechende Ressourcen wie Zeit, Know-how und Budget berücksichtigt werden.
2. Auf professionellen Accounts in sozialen Medien ist es ratsam, nur Informationen zu veröffentlichen, die für die Praxis, das Angebot und die ärztliche Tätigkeit notwendig sind und Patienten, Kollegen, Kunden und Angehörigen einen Mehrwert bieten.
3. Es ist auf die Verbreitung mehrdeutiger oder falscher Aussagen zu verzichten. Professionelle Accounts in sozialen Medien sollen nicht für die persönliche Selbstdarstellung verwendet werden oder ungerechtfertigte Erwartungen wecken. (Fallbeispiel I)
4. Es ist wesentlich, zu erkennen, dass verschiedene Plattformen und Kanäle jeweils spezifische Stärken und Risiken für bestimmte Kommunikationsziele bieten.
5. Private und berufliche Accounts auf Social-Media-Plattformen sind angemessen zu trennen.
6. Freundschaftsanfragen von Patienten auf privaten Accounts sollten mit Sorgfalt behandelt werden. (Fallbeispiel II)
7. Bei negativen Kommentaren in den sozialen Medien ist eine wohlüberlegte Reaktion empfehlenswert. Eine reflektierte Antwort kann zur Wahrung des Images und zum respektvollen Umgang im öffentlichen Diskurs beitragen. (Fallbeispiel III)
8. Es sollte darauf geachtet werden, auf sozialen Medien keine unangemessenen Inhalte zu posten und Kolleginnen und Kollegen behutsam auf nicht angemessenes Verhalten hinzuweisen. (Fallbeispiel IV)
9. Patientenbezogene Informationen und Daten sollten in sozialen Medien nur in einer Weise verwendet werden, die absolut keine Rückschlüsse auf die Identität der Personen zulässt. (Fallbeispiel V)
10. Es empfiehlt sich, sorgfältig zu evaluieren, welche Rechte an den von Ihnen publizierten Inhalten – dazu zählen Bilder, Videos, Grafiken, Texte und Informationen – Sie den Betreibern der sozialen Medien gewähren.
11. Es ist empfehlenswert, in regelmässigen Abständen eine Suche nach Beiträgen, die die eigene Person betreffen, auf sozialen Medien durchzuführen. Dabei sollte besonders auf Inhalte geachtet werden, die das persönliche oder berufliche Ansehen beeinflussen könnten.
12. Der Schutz des Zugangs zu Social-Media-Konten ist eine wesentliche Massnahme, um die Sicherheit persönlicher Informationen zu gewährleisten.
13. Die Anpassung von Datenschutzeinstellungen in sozialen Netzwerken ist eine wichtige Massnahme zum Schutz der Privatsphäre.
14. Im Kontext sozialer Medien ist es ratsam, auf Beiträge anderer Nutzer bedacht und überlegt zu reagieren. Schnelle, unüberlegte Antworten können zu Missverständnissen führen oder das eigene Ansehen schädigen.

Messenger-Dienste

15. Die Nutzung von Messenger-Diensten sollte unter strenger Beachtung der gesetzlichen Vorschriften und der berufsethischen Richtlinien erfolgen.
16. Es ist festzulegen, über welche Messenger-Dienste Kommunikation mit Patienten erfolgen soll. Diese Kanäle sind eindeutig zu kommunizieren.
17. Messenger-Dienste dürfen für die Kommunikation zwischen medizinischen Fachpersonen genutzt werden, jedoch unter strikter Einhaltung der Datenschutzbestimmungen.
18. Bei der Nutzung von Messenger-Diensten ist zu kommunizieren, welche elektronischen Inhalte akzeptiert und verwaltet werden und unter welchen Konditionen die Bearbeitung erfolgt.
19. Es ist essenziell, dass besonders schützenswerte Gesundheits- und Personendaten bei der digitalen Übertragung mit Messenger-Diensten durchgehend und konsequent durch Verschlüsselungstechnologien geschützt werden.
20. Bei der Entgegennahme von Kontaktanfragen über soziale Messenger-Dienste wird empfohlen, die Identität des Anfragenden zu verifizieren und die Preisgabe persönlicher Informationen ohne vorherige Überprüfung der Vertrauenswürdigkeit des Kontakts zu vermeiden.

Patientenbilder

21. Zur Wahrung der Persönlichkeitsrechte und des Datenschutzes hat die Patienteneinwilligung der abgebildeten Personen bei der Veröffentlichung von sogenannten Vorher-Nachher-Bildern oberste Priorität. (Fallbeispiel VI)
22. Bevor Geräte mit Kamerafunktion genutzt werden, ist sicherzustellen, dass alle cloudbasierten Backup-Systeme sowie die GPS-Funktion deaktiviert sind.
23. Vor der Verwendung von Messenger-Diensten und der Veröffentlichung auf sozialen Medien müssen zwingend alle potenziellen Identifizierungsmerkmale von Bildern entfernt oder unkenntlich gemacht werden.
24. Die spiegelverkehrte Darstellung von Bildaufnahmen ist zu vermeiden, da sie zu Missinterpretationen und zu Fehldiagnosen führen kann.

Kapitel 1: Einführung

Hintergrund und Relevanz der sozialen Medien und Messenger-Dienste im ärztlichen Alltag

Soziale Medien (engl. Social Media), darunter Plattformen wie Facebook, X, LinkedIn und Instagram, sowie soziale Messenger-Dienste (Direktnachrichten) wie WhatsApp, Threema oder Telegram, bereichern und modifizieren zahlreiche Aspekte der ärztlichen Tätigkeit. Dies umfasst die berufliche Kommunikation, die Förderung von Netzwerken und die Kooperation unter Fachkräften, die Aus-, Weiter- und Fortbildung sowie den Dialog mit Patienten. Ebenso tragen sie zur Verbreitung von gesundheitsrelevanten Informationen und Wissen bei und unterstützen die Durchführung von Massnahmen im Bereich Public Health.

Obwohl soziale Medien und Messenger-Dienste manchmal unter dem Begriff «soziale Netzwerke» subsummiert werden, weisen sie deutliche Unterschiede in ihren Zielsetzungen und Funktionen auf.

1. **Kommunikationsform und Zweck**

- **Soziale Medien**: Plattformen wie Facebook, Instagram und X sind hauptsächlich darauf ausgerichtet, Inhalte öffentlich oder innerhalb eines Netzwerks von Followern zu teilen und einen öffentlichen Austausch zu ermöglichen. Der Schwerpunkt liegt auf der Verbreitung von Informationen, Unterhaltung, Selbstpräsentation und öffentlichen Diskussion.
- **Messenger-Dienste**: Plattformen wie WhatsApp, Threema oder Telegram sind primär für die private (ggf. gruppenbasierte) Kommunikation konzipiert. Sie ermöglichen es Nutzern, Nachrichten, Fotos, Videos und Dateien auf eine direkte (und teilweise verschlüsselte) Weise auszutauschen. Die Inhalte sind nicht öffentlich zugänglich.

2. **Datenschutz und Sicherheit**

- **Soziale Medien:** Aufgrund der (halb-)öffentlichen Natur der Beiträge sind Datenschutz und Sicherheit häufige Bedenken. Obwohl Benutzer ihre Privatsphäre-Einstellungen anpassen können, sind die Informationen grundsätzlich für ein breiteres Publikum zugänglich.
- **Messenger-Dienste:** Viele Messenger-Apps betonen Sicherheit und Datenschutz, insbesondere durch Ende-zu-Ende-Verschlüsselung, die verhindert, dass Dritte auf die Kommunikation zugreifen können. Die Fokussierung auf private Konversationen bedeutet, dass persönliche Daten und Nachrichten besser geschützt sind, solange die Sicherheitseinstellungen strikt gehandhabt werden.

3. **Interaktionsmuster und Netzwerkbildung**

- **Soziale Medien** ermöglichen es Nutzern, Inhalte zu teilen, zu kommentieren und auf diese Weise mit einem grossen Publikum zu interagieren. Die Netzwerkbildung ist oft weniger persönlich, aber dafür weitreichend und öffentlich sichtbar.

- **Messenger-Dienste** dienen dem unmittelbaren Nachrichtenaustausch zwischen Einzelpersonen oder Gruppen. Die Interaktion ist in der Regel zielgerichtet und persönlich, und die Netzwerkbildung erfolgt auf einer eher persönlichen Ebene uns soll prinzipiell die Privatsphäre wahren.

Die Standesordnung der FMH «regelt die Beziehungen des Arztes zu seinen Patienten und seinen Kollegen, das Verhalten in der Öffentlichkeit und gegenüber den Partnern im Gesundheitswesen». Die etablierten Verhaltens- und Berufsregeln behalten ihre volle Gültigkeit auch bei der Verwendung von sozialen Medien und Messenger-Diensten. Neben den zu beachtenden allgemeinen und berufsspezifischen nationalen und kantonalen Rechtsgrundlagen wurden in verschiedenen Einrichtungen institutsinterne Vorgaben zur Kommunikation sowie zum Umgang mit sozialen Netzwerken erarbeitet. Ärzten, welche als Arbeitgeber Medizinstudierende oder andere Gesundheitsfach- oder Hilfspersonen beschäftigen, wird empfohlen, die Mitarbeitenden auf die spezifischen Risiken von sozialen Medien und Messenger-Diensten im medizinischen Umfeld zu sensibilisieren und deren Handhabung zu regeln.

Zur Unterstützung der Ärzteschaft in der korrekten Interpretation und Umsetzung der Standesordnung der FMH sowie der Schulung der Mitarbeitenden, erarbeitete die FMH Empfehlungen zum Umgang mit sozialen Medien und Messenger-Diensten.

Herausforderungen bei der Nutzung sozialer Medien und Messenger-Diensten

Unvorsichtiges Verhalten oder unüberlegte Beiträge im Internet können sich um ein Vielfaches problematischer auswirken als in einem Gespräch, in einem Vortrag oder in gedruckten Medien. Sie können die Privatsphäre und persönliche Integrität von Arzt und Patient verletzen, die Arzt-Patienten-Beziehung oder das Verhältnis zu Kollegen beeinträchtigen. Darüber hinaus können entsprechende Handlungen rechtliche Konsequenzen zur Folge haben.

Cyber-Kriminelle nutzen die Popularität sozialer Netzwerke gezielt aus, beispielsweise für Delikte wie Identitätsdiebstahl, den Missbrauch von öffentlich gemachten privaten Daten, Phishing-Angriffe, Mobbing sowie die fahrlässige oder absichtliche Veröffentlichung von Betriebsgeheimnissen.

Bei der Information, Kommunikation und Kollaboration über soziale Medien und Messenger-Dienste stellen sich verschiedene Fragen nach den Möglichkeiten und Grenzen. Dazu gehören beispielsweise:

- **Arztgeheimnis & Datenschutz**: Wie können Ärzte Patientendaten bei der Nutzung von sozialen Medien schützen? Welche Informationen dürfen über Messenger-Dienste versandt werden?
- **Professionelle Beziehung und Kommunikation**: Sollen Ärzte Freundschaftsanfragen von Patienten auf Facebook zurückweisen? Was ist zu beachten, wenn in sozialen Netzwerken Fallbesprechungen durchgeführt oder Kommentare über Kollegen abgegeben werden?
- **Information, Kommunikation und Werbung**: Welche Regeln gilt es zu beachten, wenn eine Arztpraxis über ihre Eröffnung informiert oder öffentlich Aufklärung über Präventionsmassnahmen leistet?
- **Umgang mit Patientenbildern**: Wie erfolgt der sorgfältige Umgang mit Bildaufnahmen während der medizinischen Behandlung und welche Bilder dürfen in den sozialen Medien erscheinen?

Beitrag der FMH und Abgrenzung

Die vorliegenden Empfehlungen zum Umgang mit sozialen Medien und Messenger-Diensten dienen der Ärzteschaft als Orientierung und Hilfestellung, indem sie auf Risiken aufmerksam machen, auf die sinnvolle Nutzung Bezug nehmen und beim sorgfältigen Umgang mit sozialen Medien und Messenger-Diensten im ärztlichen Alltag unterstützen.

In den Kapiteln 2-4 werden ausgewählte Aspekte aus den Bereichen Datenschutz, professionelle Beziehung und Information, Kommunikation und Werbung erläutert und konkrete Empfehlungen ausgesprochen. Kapitel 2 setzt das Augenmerk auf soziale Medien, Kapitel 3 auf Messenger-Dienste und Kapitel 4 widmet sich den Patientenbildern. Zum besseren Verständnis werden kritische Themen und Risiken im Zusammenhang mit sozialen Medien und Messenger-Diensten im ärztlichen Berufsumfeld anhand praxisnaher Fallbeispiele mit empfohlenen Verhaltensweisen veranschaulicht.

Als Grundlage für die Ausarbeitung der Empfehlungen der FMH wurden Erfahrungen, Empfehlungen und Richtlinien aus unterschiedlichen Ländern und medizinischen Organisationen beigezogen. Die Empfehlungen der FMH enthalten keine detaillierten technischen Informationen, konkrete Anleitungen oder Bewertungen bestimmter Anbieter, Anwendungen etc. Kantonale Ärzteorganisationen können auch Richtlinien und Empfehlungen in diesem Bereich erlassen, um die spezifischen regionalen Einzelheiten zu berücksichtigen.

Kapitel 2: Soziale Medien

Plattformen wie Facebook, Instagram, LinkedIn, YouTube und X konzentrieren sich primär auf das Teilen von Inhalten entweder öffentlich oder innerhalb eines definierten Netzwerks von Followern, um einen breiten kommunikativen Austausch zu fördern. Sie zielen darauf ab, Informationen zu verbreiten und öffentliche Diskurse zu stimulieren, wobei Informationsvermittlung und zunehmend auch Unterhaltung im Vordergrund stehen. Die Interaktionsdynamiken auf diesen Plattformen sind darauf ausgelegt, ein weitreichendes Publikum anzusprechen und Verbindungen zwischen Individuen mit ähnlichen Interessen sowie zwischen Nutzern und öffentlichen Institutionen zu etablieren; auch um einen fachlichen und sozialen Dialog zu ermöglichen.
Angesichts der zumindest teilöffentlichen Natur der Beiträge stellen Arztgeheimnis, Datenschutz und Datensicherheit regelmässig Herausforderungen dar. Trotz der Möglichkeit für Benutzer, ihre Privatsphäre-Einstellungen zu konfigurieren, bleiben die geteilten Informationen prinzipiell für eine umfassende Rezipientenschaft einsehbar.

Information, Kommunikation, Werbung

Die Standesordnung der FMH spricht sich für eine aktive Beteiligung von Ärzten an öffentlichen Diskursen aus, was die Mitwirkung in Presse, Radio, Fernsehen sowie digitalen Medien einschliesst. Werbung und Information im Kontext sozialer Medien unterliegen dabei denselben Richtlinien wie in den traditionellen Medien. Ärzte sind angehalten, Werbung zu unterlassen, die als unsachlich gilt, auf unzutreffenden Behauptungen fusst oder das Ansehen des ärztlichen Berufsstands potenziell schädigt[1]. Anhang 2 der Standesordnung, die Richtlinien «Information und Werbung», führt diesbezüglich detaillierte Bestimmungen aus, vor allem hinsichtlich der angemessenen Bereitstellung von Informationen für die anvisierte Zielgruppe bzw. das Publikum.

Weiterhin ist zu berücksichtigen, dass den kantonalen Ärztegesellschaften die Befugnis eingeräumt wird, spezifische Regelungen hinsichtlich der Modalitäten – beispielsweise Kanal und Format – der gestatteten Informationen festzulegen. Die FMH legt ihren Mitgliedern nahe, zur Klärung dieser Angelegenheiten proaktiv den Kontakt zu ihrer zuständigen kantonalen Ärztegesellschaft zu suchen.

Empfehlung 1: Eine kritische Prüfung des Einsatzes sozialer Medien zu beruflichen Zwecken ist unerlässlich. Für das Management und Monitoring müssen entsprechende Ressourcen wie Zeit, Know-how und Budget berücksichtigt werden.

Erklärung zu Empfehlung 1: Beim Teilen von Inhalten über soziale Medien ist grundsätzlich Vorsicht geboten. Es ist ratsam, sich mit den verschiedenen Möglichkeiten vertraut zu machen, um eine fundierte Entscheidung darüber zu treffen, welche Inhalte und Formate im Rahmen eines öffentlichen Auftritts von Fachpersonen oder Praxen angemessen sind. Inhalte sollten von hoher Qualität sein. Es ist wichtig, den Einsatz von Social-Media-Kanälen zu bedenken – dazu gehören unter anderem die sorgfältige Entwicklung von Inhalten, das zeitnahe Reagieren auf Kommentare und das Einhalten des Arztgeheimnisses und von Datenschutzrichtlinien. Diese Aktivitäten erfordern ein Zeitinvestment sowie spezifisches Fachwissen.

Empfehlung 2: Auf professionellen Accounts in sozialen Medien ist es ratsam, nur Informationen zu veröffentlichen, die für die Praxis, das Angebot und die ärztliche Tätigkeit notwendig sind und Patienten, Kollegen, Kunden und Angehörigen einen Mehrwert bieten.

Erklärung zur Empfehlung 2:
In sozialen Netzwerken verbreiten sich Inhalte rasch und können dauerhaft für eine unbestimmte und unkontrollierte Anzahl von Personen sichtbar bleiben. Die Standesordnung der FMH gestattet Ärzten, ihre fachlichen Qualifikationen und notwendige Informationen für Patienten und Kollegen in zurückhaltender Form zu teilen (siehe Art. 20 Abs. 1 StaO). Erlaubt ist die Bekanntmachung von relevanten Informationen über medizinische Themen, Prävention, Angebot, Praxisablauf, Infrastruktur, Öffnungszeiten, Kontaktmöglichkeiten und das Team sowie Änderungen derselben. Neben der Praxis-Website dienen soziale Medien als Plattform, um diese Informationen auszutauschen. Sie bieten Gesundheitsfachpersonen die Möglichkeit, über Krankheitsprävention, Behandlungsoptionen und aktuelle medizinische Forschung zu informieren und damit zum Gesundheitsbewusstsein und zur medizinischen Aufklärung beizutragen. Gemäss den Regelungen in Anhang 2 der FMH-Standesordnung zu zulässigen Informationen und unzulässiger Werbung sollten Beiträge in sozialen Medien objektiv formuliert, mit Bedacht gewählt, für Patienten, Kunden oder Angehörigen mehrwertbringend und darauf ausgerichtet sein, die medizinische Entscheidungsfindung zu unterstützen. Ferner können soziale

[1] Art. 12 Abs. 2 StaO

Medien für den fachlichen Austausch zwischen Gesundheitsfachpersonen, beispielsweise über aktuelle Forschung oder Kongresse, genutzt werden.

Empfehlung 3: Es ist auf die Verbreitung mehrdeutiger oder falscher Aussagen zu verzichten. Professionelle Accounts in sozialen Medien sollen nicht für die persönliche Selbstdarstellung verwendet werden oder ungerechtfertigte Erwartungen wecken.

Erklärung zu Empfehlung 3: Im medizinischen Kontext obliegt Ärzten eine Expertenrolle, die eine verantwortungsbewusste Kommunikation in den sozialen Medien erfordert. Es ist geboten, sich ausschliesslich zu Themen zu äussern, bei denen entsprechende fachliche Kompetenzen vorliegen und keine falschen oder missverständlichen Informationen zu verbreiten. Inhalte sollten stets im erforderlichen Kontext dargestellt und gegebenenfalls mit Verweisen auf weiterführende Informationen versehen werden, um auch Laien eine angemessene Einordnung zu ermöglichen. Professionelle Accounts sollten vorrangig der Bereitstellung wertstiftender Kommunikation aus Patienten- und Kundensicht dienen, und nicht der Selbstdarstellung. Der Arzt darf keine Empfehlungen oder Kommentare von Patienten für seine Kommunikation benutzen.

Fallbeispiel I: Problematische Auftritte und Beiträge in sozialen Medien

Ausgangslage
Dr. med. Meier ist Orthopäde und hat sich auf Knieprobleme spezialisiert. Er betreibt ein LinkedIn-Profil mit zahlreichen Informationen, Bildern und Beiträgen. Nebst Bildern aus der Arztpraxis und dem Operationssaal hat er ein gemeinsames Foto mit einem prominenten Fussballer und folgendem Begleitkommentar gepostet: «Wenn auch Sie bei Knieproblemen rasch wieder im Spiel sein wollen, kommen Sie besser zu mir.». In Wirklichkeit hat Dr. Meier den bekannten Fussballer nicht operiert. In der Folge verfassen verschiedene LinkedIn-User Kommentare und stellen Fragen zu ihren Knieproblemen. Mehrere Patienten nennen dabei Namen und Wohnort.

Problematik
Die Darstellung von Praxis- und Operationsbildern, ein Portrait neben einem bekannten Fussballer sowie die Präsentation von Leistungen und medizinischen Stellungnahmen erweckt irrtümlich den Anschein einer Behandlung durch Dr. Meier und gilt als unzulässige Werbemassnahme. Allgemeine Informationen zu Gelenkbeschwerden können informativ sein, doch individuelle medizinische Ratschläge könnten als spezifische Therapieempfehlungen interpretiert werden und das Berufsgeheimnis sowie die Privatsphäre verletzen.

Alternative zu Fallbeispiel
Auf seinem LinkedIn-Profil präsentiert Dr. Meier Informationen zu Knieerkrankungen, chirurgischen Behandlungsoptionen und mögliche Behandlungsergebnisse. In der Informationsbox des LinkedIn-Profils werden Nutzer über Datenschutzbestimmungen aufgeklärt und auf die Problematik der Offenlegung persönlicher Daten in öffentlichen Kommentaren hingewiesen. Weiterhin klärt sie über die Unzulässigkeit der Online-Beratung auf und bietet Kontaktmöglichkeiten für direkte Anfragen in der Praxis an.

Empfehlung 4: Es ist wesentlich, zu erkennen, dass verschiedene Plattformen und Kanäle jeweils spezifische Stärken und Risiken für bestimmte Kommunikationsziele bieten.

Erklärung zu Empfehlung 4: Social-Media-Kanäle variieren in Zweck, Community und Kommunikationsart. Einige Plattformen wie Facebook, YouTube oder Instagram eignen sich zur Vermittlung visueller Informationen an Patienten. Andere, wie LinkedIn, dienen vornehmlich der schriftlichen Kommunikation unter Fachpersonen. Es ist wichtig, sich mit den spezifischen Kommunikationsarten und den formatspezifischen Darstellungsweisen wie beispielsweise Bild, Text, Video, der Live-Event auseinanderzusetzen.

Empfehlung 5: Private und berufliche Accounts auf Social-Media-Plattformen sind angemessen zu trennen.

Erklärung zur Empfehlung 5: Gemäss der Standesordnung der FMH ist eine klare Trennung zwischen privater und beruflicher Tätigkeit geboten, insbesondere in der direkten Kommunikation mit Patienten. Soziale Medien dienen dem privaten Austausch mit Freunden sowie dem professionellen Austausch mit Kollegen aus der Fachschaft. Eine Trennung der Accounts wird empfohlen, um bewusst zu entscheiden, welche Inhalte als Fachperson oder als Vertreter einer Praxis oder Organisation für die Allgemeinheit zugänglich gemacht werden. Diese Inhalte sollten mit der Standesordnung der FMH übereinstimmen. Social-Media-Plattformen sind grundsätzlich keine geeigneten Mittel für die Arzt-Patient-Kommunikation.

Arzt-Patient-Beziehung

Empfehlung 6: Freundschaftsanfragen von Patienten auf privaten Accounts sollten mit Sorgfalt behandelt werden.

Erklärung zur Empfehlung 6: Die FMH empfiehlt allen Ärzten, den Zugriff auf private Accounts grundsätzlich auf Personen aus dem persönlichen Umfeld einzuschränken. Gewähren Ärzte ihren Patienten Zugang zu ihrem persönlichen Profil einer Social-Media-Plattform, erhalten diese Einblicke in das Privatleben des Arztes, wie dies im üblichen Arzt-Patienten-Verhältnis nicht der Fall wäre. Zur sorgfältigen und gewissenhaften Berufsausübung eines Arztes gehört auch die Einhaltung professioneller Grenzen zum Schutz der eigenen Privatsphäre und jener der Patienten. Wird dies missachtet, könnten leicht Grenzen überschritten werden, die das Arzt-Patienten-Verhältnis gegenseitig nachteilig beeinflussen. In den sozialen Medien ist die Hemmschwelle für Grenzüberschreitungen tendenziell geringer, was nicht nur das Arzt-Patient-Verhältnis beeinträchtigen, sondern auch zu Brüchen der Vertraulichkeit und zu weiteren berufsrechtlichen Konsequenzen führen kann.

Fallbeispiel II: Privates Facebook-Video

Ausgangslage
Dr. med. Stettler, Sportmediziner, erhält auf seinem privaten Facebook-Account eine Freundschaftsanfrage von S. Müller. Das Profilfoto zeigt ein Segelboot, weshalb Dr. Stettler vermutet, es handle sich um einen Kollegen aus dem Segelclub und die Anfrage annimmt. Erst später realisiert Dr. Stettler, dass S. Müller ein Patient ist. Dieser erkundigt sich nach einer Kopie der letzten Laborresultate und sieht ein privates Video von Dr. Stettler. Das Video zeigt ihn, leicht alkoholisiert, an einer Party. In der nachfolgenden Sprechstunde gibt sich S. Müller zurückhaltend, die Arzt-Patient-Beziehung ist angespannt und das Vertrauensverhältnis beeinträchtigt. Nach weiteren Konsultationen wechselt S. Müller den Arzt.

Problematik
Die bisher professionelle Arzt-Patienten-Beziehung zwischen S. Müller und Dr. Stettler wurde durch den Einblick von Herrn Müller in das private Leben seines Arztes negativ beeinflusst. Der Inhalt des Videos entsprach nicht dem Bild und den Erwartungen, welche S. Müller gegenüber Dr. Stettler hatte, wodurch er das Vertrauen in seinen Arzt verlor.

Alternative zu Fallbeispiel
Dr. Stettler führt nebst dem privaten auch einen beruflichen Facebook-Account für seine orthopädische Praxis. Nach einer vorsichtigen Überprüfung der Freundschaftsanfragen für seinen privaten Account erinnert sich Dr. Stettler an seinen Patienten S. Müller. Er informiert ihn über einen verschlüsselten Kommunikationsweg, dass er aus Diskretionsgründen grundsätzlich keine privaten Online-Freundschaften mit Patienten eingehen würde und verweist ihn freundlich auf seinen öffentlichen beruflichen Facebook-Account.

Empfehlung 7: Bei negativen Kommentaren in den sozialen Medien ist eine wohlüberlegte Reaktion empfehlenswert. Eine reflektierte Antwort kann zur Wahrung des Images und zum respektvollen Umgang im öffentlichen Diskurs beitragen.

Erklärung zur Empfehlung 7: Die Wahrung der Reputation eines Arztes ist auch im öffentlichen Raum von hoher Bedeutung. Unberechtigte oder negative Online-Bewertungen können für Ärzte emotionale und sogar existenzielle Folgen nach sich ziehen. Kritische, fachlich nicht fundierte Online-Bewertungen stellen für die medizinische Fachwelt ein signifikantes Problem dar. Sie führen oft zu komplexen rechtlichen Herausforderungen, insbesondere im Kontext berufsspezifischer Regelungen wie der Schweigepflicht, und erschweren es Ärzten, sich gegenüber anonym verfassten Bewertungen zu äussern. Ohne die Zustimmung des Patienten oder eine offizielle Entbindung von der ärztlichen Schweigepflicht durch die kantonale Aufsichtsbehörde würde eine Gegendarstellung einen Bruch des Arztgeheimnisses darstellen. Die Empfehlungen der FMH für den Umgang mit Online-Bewertungen klären Ärzte über die rechtlichen Möglichkeiten auf und bieten konkrete zusätzliche Hilfestellungen.

Fallbeispiel III: Schlechte Google-Bewertung

Ausgangslage
Dr. med. Gruber ist Internistin und Hausärztin. Sie betreibt neben ihrer Praxis-Website und einem Facebook-Account ein Google-Unternehmensprofil, auf welchem Personen öffentlich Rezensionen für Dr. Gruber und ihre Praxis abgeben können. Sie erhält folgende negative Google-Rezension: «Nach sehr langer Wartezeit wurde ich auch noch inkompetent behandelt. Zu meinen Bauchschmerzen konnte Dr. Gruber nichts sagen, ausser dass sie nicht weiss, was es ist und mich ans Kantonsspital für eine Darmspiegelung verweisen müsse. Eine reine Zeitverschwendung.» (einen Stern). Dr. Gruber kann sich an den Fall erinnern und weiss trotz anonymisiertem Benutzernamen, welche Patientin diese Bewertung geschrieben hat. Sie antwortet direkt im Google-Unternehmensprofil mit folgender Nachricht: «Liebe Patientin, vielen Dank für Ihre Rückmeldung. Leider stehen mir als Hausärztin nicht die Mittel zur Verfügung, Ihre Situation abschliessend zu beurteilen. Ihre Symptome deuten zwar nicht zwingend auf eine schwerwiegende Krankheit hin, ich konnte dies jedoch auch nicht ausschliessen. In Fällen wie Ihrem ist es wichtig, dass Sie sich von einer auf Viszeralchirurgie spezialisierten Person untersuchen lassen.»

Problematik
In ihrer Antwort geht Dr. Gruber auf die Krankengeschichte der Patientin ein. Sie verletzt damit das Arztgeheimnis, denn Beiträge in Google-Rezensionen sind öffentlich und für alle frei einsehbar. Auch nennt sie das Geschlecht der Patientin, was ein Identifizierungsmerkmal ist.

Alternative zu Fallbeispiel
Dr. Gruber nimmt neutral und ohne weitere Informationen zur Krankheitsgeschichte der Patientin Stellung mit folgender Antwort: «Guten Tag, vielen Dank für Ihre Rückmeldung. Es ist üblich, dass wir als Hausarztpraxis Patienten an Fachspezialisten weiterleiten. Es ist bedauerlich, dass Sie die Behandlung als nicht kompetent empfunden haben. Dies widerspiegelt in keinem Falle unsere Werte. Aufgrund des Patientenschutzes werden wir hier nicht auf die medizinischen Details eingehen. Nehmen Sie gerne telefonisch Kontakt mit uns auf.»

Arzt-Arzt-Beziehung

Empfehlung 8: Es sollte darauf geachtet werden, auf sozialen Medien keine unangemessenen Inhalte zu posten und Kollegen behutsam auf nicht angemessenes Verhalten hinzuweisen.

Erklärung zur Empfehlung 8: Unangemessene, beleidigende oder falsche Behauptungen in Beiträgen über Kollegen sowie Kommentare zu deren Veröffentlichungen, können dem Ruf des ärztlichen Berufsstandes langfristig Schaden zufügen. Die Bestimmungen des Artikels 23 StaO bezüglich des kollegialen Verhaltens und der Vermeidung unzulässiger Kritik unter Ärzten gelten auch im digitalen öffentlichen Raum der sozialen Medien. Ärzte sind demnach angehalten, auch auf sozialen Plattformen kollegiale Beziehungen zu wahren, die sich durch Aufrichtigkeit und Respekt auszeichnen, sowie jegliches Verhalten zu meiden, das die Ehre eines Kollegen ohne gerechtfertigten Grund verletzen könnte. In der Kommunikation über Dritte inkl. Behörde sollte stets eine sachliche und objektive Haltung bezüglich medizinischer Massnahmen von Kollegen bewahrt werden.

Fallbeispiel IV: Öffentliche Äusserungen zum Verhalten von Kollegen

Ausgangslage
Oberarzt Dr. med. Müller postet auf seinem öffentlichen LinkedIn-Account folgenden Kommentar gegenüber einem Kollegen vom Notfall:
Sehr geehrter Herr Kollege P. von der Notfallstation
Besten Dank für die fehlerhafte Interpretation der Bauchschmerzen von Frau R.B.,1.1.1932 als Obstipation sowie für ihre Behandlung mit Laxantien. Ich bin mir sicher, dass die Patientin für die anschliessende Darmperforation mit septischem Schock und Multiorganversagen dankbar ist. Sie braucht jetzt eine frische Leber. Mit ihrem hervorragenden ärztlichen Know-how bin ich mir sicher, dass Sie ihr dabei helfen werden, ein neues Organ zu bekommen!
Beste Grüsse, Dr. med. Müller, OA IPS

Problematik
Dr. Müllers Äusserungen über einen Kollegen stehen im Konflikt mit den Richtlinien der FMH-Standesordnung und können zivilrechtliche sowie strafrechtliche Folgen nach sich ziehen. Ein solcher Beitrag auf LinkedIn ist öffentlich zugänglich und könnte als rufschädigend oder als Verleumdung interpretiert werden. Zudem ermöglichen die veröffentlichten Informationen in Verbindung mit Daten von anderen Plattformen eventuell Rückschlüsse auf den betroffenen Arzt und die Identität der Patientin.

Alternative zu Fallbeispiel
Dr. Müller schickt dem Kollegen von der Notfallstation über seine verschlüsselte Klinik-E-Mail einen sachlichen Bericht zu Diagnose und Verlauf von Frau R.B. im Sinne eines professionellen Feedbacks. Dr. P. realisiert seine fehlerhafte Einschätzung und nimmt dazu Stellung. In einer gemeinsamen Fallanalyse ergründen sie die Ursachen der initial fehlerhaften Bewertung und Behandlung durch Dr. P. Auf einer internen Plattform für klinische Fallbesprechungen diskutieren sie den ungewöhnlichen, doch instruktiven Fall mit ihren Assistenzärzten und Kollegen, wobei sie die Anonymität der beteiligten Personen sowie der Patientin durch Weglassen von Namen, Initialen und Zeitangaben sicherstellen.

Arztgeheimnis und Datenschutz

Empfehlung 9: Patientenbezogene Informationen und Daten sollten in sozialen Medien nur in einer Weise verwendet werden, die absolut keine Rückschlüsse auf die Identität der Personen zulässt.

Erklärung zur Empfehlung 9: Beim Teilen von Texten und Bildern über soziale Medien besteht das Risiko, dass persönliche Daten versehentlich öffentlich gemacht werden. Daher ist es wichtig, bei der Nutzung von Patienteninformationen in sozialen Medien alle persönlichen Daten (z.B. Initialen, Geburtsdatum, Beruf, Wohnort) zu entfernen oder zu verändern. Eine einfache Anonymisierung oder Pseudonymisierung reicht oft nicht aus, da die Möglichkeit besteht, dass

durch die Kombination von Daten mit Informationen aus anderen Quellen wie Blogs, Foren oder Webseiten die Identität einer Person wiederhergestellt wird. Um eine anonymisierte Fallbeschreibung zu gewährleisten, sollte auch die Menge der geteilten Informationskategorien (z.B. Geschlecht, Erkrankung, Behandlung) auf das Nötigste reduziert werden.

Fallbeispiel V: Blog-Beitrag über einen seltenen Fall

Ausgangslage
Oberärztin Dr. med. Feller arbeitet an einem Kantonsspital in der Intensivmedizin. Sie betreut den seltenen Fall einer Patientin mit Tetanus. Auf ihrem öffentlich zugänglichen LinkedIn-Profil berichtet Dr. Feller periodisch über den Krankheitsverlauf ihrer 46-jährigen Patientin P. L., um Kollegen an der Erfahrung teilhaben zu lassen. Gleichzeitig respektiert sie das ärztliche Berufsgeheimnis und erwähnt weder den Namen ihrer Patientin noch das behandelnde Spital. Allerdings postet Dr. Feller eine Aufnahme von ihrem Handy, auf welchem die Patientin mit typischem Krampf der Rückenmuskulatur von hinten zu sehen ist. Das Gesicht der Patientin ist nicht erkennbar, jedoch ihre Haare. Ein besorgter Arbeitskollege der Patientin will sich im Internet über das Spital informieren, in welchem diese hospitalisiert ist. Bei seiner Internet-Recherche stösst er auf einen Bericht über den neuorganisierten Notfall des Spitals, in welchem der Name der Oberärztin Dr. Feller erwähnt wird. Derselbe Name fällt dem Arbeitskollegen auch in einem LinkedIn-Beitrag, welcher eine Bekannte kommentiert, auf. Durch die Verbindung der Informationen aus dem Online-Bericht und dem LinkedIn-Post sowie in Kenntnis von Alter, Name und Haarfarbe seiner Kollegin erfährt der Arbeitskollege vertrauliche Informationen über Frau Petra Lässer und ihre Tetanus-Erkrankung.

Problematik
Die Kombination der Informationen im Fallbeispiel hebt die intendierte Anonymisierung der leitenden Ärztin auf. Dies führt zur Aufhebung des gewährleisteten Datenschutzes und stellt einen Bruch des ärztlichen Berufsgeheimnisses dar.

Alternative zu Fallbeispiel
Lässt Dr. Feller die Initialen, die Altersangabe sowie die Bildaufnahme der Patientin weg oder verändert diese (z.B. Patientin A. A., mittleren Alters), kann die Patientin durch den Arbeitskollegen nicht identifiziert werden. Auch mit der Fallbeschreibung durch einen Kollegen in einem ausschliesslich für Medizinstudierende und Ärzte zugänglichen Blog oder professionellem Netzwerk (z.B. Doctornet) ist eine Identifikation so nicht möglich.

Empfehlung 10: Es empfiehlt sich, sorgfältig zu evaluieren, welche Rechte an den von Ihnen publizierten Inhalten – dazu zählen Bilder, Videos, Grafiken, Texte und Informationen – Sie den Betreibern der sozialen Medien gewähren.

Erklärung zur Empfehlung 10: In den Allgemeinen Geschäftsbedingungen (AGB) sozialer Medien können umfangreiche Nutzungsrechte der Daten festgeschrieben sein. Eine nicht sorgfältig durchgeführte Prüfung und vorschnelle Akzeptanz der AGB können zur Folge haben, dass Zustimmungen erteilt werden, welche die Daten auch Dritten in einem ganz anderen Kontext zugänglich machen. Die Bedingungen und Privatsphäre-Einstellungen sind Veränderungen unterworfen und bedürfen daher einer regelmässigen Überprüfung. Es ist zu berücksichtigen, dass Daten auf sozialen Netzwerken weniger geschützt sein können als beispielsweise beim E-Banking. Es besteht immer die Möglichkeit, dass Daten ausserhalb der vertraglichen Vereinbarungen Dritten zugänglich gemacht werden, sei es durch Suchmaschinen, Hackerangriffe oder Sicherheitslücken bei den Plattformbetreibern.

Empfehlung 11 Es ist empfehlenswert, in regelmässigen Abständen eine Suche nach Beiträgen, welche die eigene Person betreffen, auf sozialen Medien durchzuführen. Dabei sollte besonders auf Inhalte geachtet werden, die das persönliche oder berufliche Ansehen beeinflussen könnten.

Erklärung zur Empfehlung 11: Im Internet und auf sozialen Medien suchen Patienten, Berufskollegen, Partner, aktuelle oder zukünftige Arbeitgeber vermehrt nach persönlichen und beruflichen Informationen. Unangemessene Darstellungen und Beiträge, nachlässige Ausdrucksweisen oder übermässig freimütig geteilte Informationen können sich negativ auf das berufliche Umfeld, zukünftige Arzt-Arzt- und Arzt-Patient-Verhältnisse, sowie die berufliche Laufbahn auswirken. Kriminelle Personen und Gruppierungen nutzen persönliche Informationen, um gezielt Cyberangriffe durchzuführen (Social-Engineering-Angriffe[2]).

Bei Auffinden unpassender oder problematischer Inhalte auf sozialen Netzwerken ist es angezeigt, den Plattformbetreiber um Entfernung zu ersuchen. Die Europäische Datenschutz-Grundverordnung sowie das Schweizerische Datenschutzgesetz gewähren das Recht auf Löschung personenbezogener Daten. Zu beachten ist, dass der Löschvorgang Zeit und Mühe erfordern kann, insbesondere da viele Plattformen (z.B. Google oder Facebook) keinen leicht zugänglichen Kundenservice bieten. Die Empfehlungen der FMH für den Umgang mit Online-Bewertungen klären Ärzte über die rechtlichen Möglichkeiten auf und bieten konkrete zusätzliche Hilfestellungen.

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

Empfehlung 12: Der Schutz des Zugangs zu Social-Media-Konten ist eine wesentliche Massnahme, um die Sicherheit persönlicher Informationen zu gewährleisten.

Erklärung zur Empfehlung 12: Es ist unerlässlich, in den sozialen Medien die eigene Online-Identität sorgfältig zu schützen. Ein effektiver Weg, dies zu tun, ist die Verwendung einzigartiger Passwörter für jede Plattform. Ein starkes Passwort besteht aus einer Kombination von Buchstaben, Zahlen und Sonderzeichen und ist lang genug, um nicht leicht erraten oder durch automatisierte Tools geknackt zu werden. Darüber hinaus ist es empfehlenswert, wo immer möglich eine Zwei-Faktor-Authentifizierung zu aktivieren. Für konkrete Anforderungen an sichere Passwörter und weitere Tipps zur Absicherung der Online-Präsenz, kann der IT-Grundschutz für Praxisärztinnen und Praxisärzte beigezogen werden.

Empfehlung 13: Die Anpassung von Datenschutzeinstellungen in sozialen Netzwerken ist eine wichtige Massnahme zum Schutz der Privatsphäre.

Erklärung zur Empfehlung 13: Es ist ratsam, die Datenschutzeinstellungen auf persönlichen und professionellen Sozialen Medien sorgfältig zu konfigurieren. Standardeinstellungen sollten kritisch geprüft werden, denn dadurch lässt sich steuern, welche Informationen mit wem geteilt werden. Verschiedene Optionen ermöglichen es, die Sichtbarkeit von persönlichen Daten, Beitragsfreigaben und Freundeslisten zu kontrollieren. Persönliche Accounts sollten auf «privat» eingestellt sein, damit Beiträge, Bilder, Kommentare, Freundesliste etc. nicht von der Öffentlichkeit einsehbar sind. Einstellungen zur Kommentar- und Markierungsfunktion können restriktiv eingestellt werden und gewährleisten so, dass Kommentare, Markierungen und Erwähnungen individuell geprüft werden müssen, bevor Sie öffentlich sichtbar sind. Nutzer sollten regelmässig überprüfen, ob die gewählten Einstellungen noch dem gewünschten Schutzniveau entsprechen, und Anpassungen vornehmen, wenn sich die Funktionalitäten der Plattformen oder die persönlichen Anforderungen an die Privatsphäre ändern.

Empfehlung 14: Im Kontext sozialer Medien ist es ratsam, auf Beiträge anderer Nutzer bedacht und überlegt zu reagieren. Schnelle, unüberlegte Antworten können zu Missverständnissen führen oder das eigene Ansehen schädigen.

Erklärung zur Empfehlung 14: Aktivitäten wie Kommentare, Likes und Shares/Reposts, die mit einem öffentlichen oder privaten Account durchgeführt werden, sind möglicherweise auch für Nutzer sichtbar, die keine direkten Verbindungen aufweisen. Es ist ratsam, sich überlegt und bewusst am öffentlichen Diskurs zu beteiligen, selbst wenn es um Aktivitäten im persönlichen Profil geht.

Kapitel 3: Messenger-Dienste

Messenger-Dienste sind digitale Plattformen, die einen unmittelbaren Austausch von Nachrichten zwischen Einzelpersonen oder innerhalb einer spezifischen Gruppe ermöglichen. Diese Dienste sind primär auf eine zielorientierte und private Interaktion ausgerichtet und sollen die Vertraulichkeit der Kommunikation gewährleisten. Sie bieten die Möglichkeit, Nachrichten sowie multimediale Inhalte wie Fotos, Videos und Dokumente auf direktem und zum Teil verschlüsseltem Wege zu übermitteln, wobei die Inhalte ausserhalb des jeweiligen Kommunikationskreises nicht einsehbar sind. Viele dieser Anwendungen legen ein besonderes Augenmerk auf Sicherheitsaspekte und den Datenschutz ihrer Nutzer, insbesondere durch die Implementierung von Ende-zu-Ende-Verschlüsselung, welche das Risiko unbefugter Zugriffe durch Dritte minimiert. Gegebenenfalls muss die Kommunikation über digitale Plattformen den Standards der Telemedizinischen Konsultationen entsprechen.

In der Schweiz gibt es keine einheitlichen Empfehlungen, unter welchen Bedingungen der weitaus am häufigsten genutzte Messenger Dienst "WhatsApp" datenschutzkonform genutzt werden kann. Eine deutsche Datenschutzbehörde führt Bedingungen dafür auf. Zusätzlich veröffentlichte das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen betreffend Sicherheitseinstellungen. Die FMH empfiehlt die Nutzung von Messenger-Diensten mit Patienten im ärztlichen Alltag nur für administrative Anliegen und nach erfolgter Einwilligung des Patienten. Eine Kommunikation über Messenger-Dienste kann auch in Bezug auf die Dokumentationspflicht relevant sein und wäre gegebenenfalls in die KG entsprechend einzutragen.

Information, Kommunikation, Werbung

Empfehlung 15: Die Nutzung von Messenger-Diensten sollte unter strenger Beachtung der gesetzlichen Vorschriften und der berufsethischen Richtlinien erfolgen.

Erklärung zu Empfehlung 15: Obwohl Messenger-Dienste eine schnelle und effiziente Kommunikation ermöglichen, müssen dabei die Bestimmungen zum Arztgeheimnis sowie die strengen Datenschutzrichtlinien, insbesondere das Bundesgesetz über den Datenschutz (DSG) und die Verordnung zum Bundesgesetz über den Datenschutz (DSV), eingehalten werden. In der medizinischen Praxis ist der Einsatz von Messenger-Diensten zur Kommunikation mit Patienten, Angehörigen und Kunden daher mit Vorsicht handzuhaben. Zudem sind die Bestimmungen zur ärztlichen Schweigepflicht gegenüber Dritten einzuhalten. Eine ausdrückliche Einwilligung der Patienten zur Nutzung dieser Kommunikationswege muss vorliegen (Einwilligungserklärung FMH).

Arzt-Patient-Beziehung

Empfehlung 16: Es ist festzulegen, über welche Messenger-Dienste Kommunikation mit Patienten erfolgen soll. Diese Kanäle sind eindeutig zu kommunizieren.

Erklärung zur Empfehlung 16: Es ist kritisch zu prüfen, inwieweit Messenger-Dienste als unterstützende Kommunikationsmittel in der medizinischen Praxis eingesetzt werden können, unter besonderer Berücksichtigung des Arztgeheimnisses und des Datenschutzes. Es wird empfohlen, dass die Patienten über die zugelassenen Kommunikationskanäle informiert werden. Diese Informationen sollten ihnen klar und deutlich durch die Unterzeichnung der Einwilligungserklärung, persönliche Gespräche, die Praxiswebsite oder Social-Media-Kanäle vermittelt werden. Kontaktanfragen sollten konsequent nur über diese festgelegten Kanäle bearbeitet werden. In der Regel verwenden Arztpraxen ein verschlüsseltes E-Mail-System für den Austausch sensibler Patientendaten. Die Nutzung von Messenger-Diensten für die Arzt-Patient-Beziehung wird daher nur für administrative Anliegen wie zum Beispiel Terminvereinbarungen empfohlen. Für den restlichen Datenaustausch empfiehlt die FMH die Nutzung des bestehenden Systems und der Datenaustausch über verschlüsselte E-Mail.

Arzt-Arzt-Beziehung

Empfehlung 17: Messenger-Dienste dürfen für die Kommunikation zwischen medizinischen Fachpersonen genutzt werden, jedoch unter Einhaltung des Arztgeheimnisses und der Datenschutzbestimmungen.

Erklärung zu Empfehlung 17: Bei der Kommunikation mit Messenger-Diensten müssen alle relevanten Datenschutzbestimmungen berücksichtigt werden. Dazu zählen insbesondere die Einhaltung des Arztgeheimnisses und der Schutz von Patientendaten. Es ist daran zu erinnern, dass das Arztgeheimnis auch zwischen medizinischen Fachpersonen gilt, wenn diese nicht in der Behandlung des Patienten involviert sind. Essenziell ist die Verwendung von Diensten, die eine Ende-zu-Ende-Verschlüsselung bieten. Die Vertraulichkeit und Integrität der Informationen müssen jederzeit gewährleistet sein. Vor der Nutzung sollten klar definierte Richtlinien für den Umgang mit diesen Kommunikationswerkzeugen etabliert werden, die auch die Art der übermittelbaren Informationen und die Verantwortlichkeiten der Nutzer umfassen.

Datenschutz

Empfehlung 18: Bei der Nutzung von Messenger-Diensten zwischen Arzt-Patient ist zu kommunizieren, welche elektronischen Inhalte akzeptiert und verwaltet werden und unter welchen Konditionen die Bearbeitung erfolgt.

Erklärung zur Empfehlung 18: Um das Risiko zu minimieren, dass unaufgefordert Inhalte von Patienten übermittelt werden, ist es zielführend, genau zu definieren und zu kommunizieren, welche Arten von elektronischen Inhalten über welche Kommunikationswege akzeptiert werden, beispielsweise Bilder, Videos, Dokumente, Ultraschall-, MRI-Bilder oder Röntgenaufnahmen. Ferner ist transparent zu machen, an welchem Ort die Inhalte gespeichert und verarbeitet werden und welche Antwortzeiten seitens der Patienten zu erwarten sind. Bei Anfragen via Messenger kann es zweckmässig sein, eine Standardnachricht festzulegen, die automatisch versendet wird und die genannten Informationen beinhaltet. Einige Anwendungen, wie zum Beispiel WhatsApp, bieten die Möglichkeit, Lesebestätigungen zu konfigurieren.

Empfehlung 19: Es ist essenziell, dass besonders schützenswerte Gesundheits- und Personendaten bei der digitalen Übertragung mit Messenger-Diensten durchgehend und konsequent durch Verschlüsselungstechnologien geschützt werden.[3]

Erklärung zur Empfehlung 19: Ungesicherte übermittelte Dokumente, wie z.B. Arbeitsunfähigkeitszeugnisse, enthalten besonders schützenswerte Personendaten und vereinfachen bspw. die Fälschung solcher Dokumente. Auch könnten Merkmale wie Name des ausstellenden Arztes, Unterschrift etc. von Dritten eingesehen werden.

Die FMH empfiehlt, dass besonders schützenswerte Gesundheits- und Personendaten bei der digitalen Übertragung stets durch Verschlüsselung geschützt sind. Sobald es um Patientendaten geht, geht es auch um die Wahrung des ärztlichen Berufsgeheimnisses. Der unverschlüsselte Nachrichtenverkehr (via unverschlüsselte E-Mail oder unverschlüsselte soziale Netzwerke) kann die Vertraulichkeit und die Einhaltung der ärztlichen Schweigepflicht nicht gewährleisten, und die Verletzung von datenschutzrechtlichen Vorgaben kann strafrechtliche Konsequenzen nach sich ziehen. Durch die Verschlüsselung wird sichergestellt, dass bei physischem Zugriff von Dritten auf die Speichermedien, die Daten ohne den richtigen Schlüssel nicht gelesen oder verstanden werden können.

Wenn keine patientenbezogenen Daten aus der Nachricht ersichtlich sind, sprich keine Rückverfolgbarkeit möglich ist, darf diese auch unverschlüsselt verschickt werden, zum Beispiel für administrative Anliegen. Dazu muss jedoch vorgängig die schriftliche Einwilligung des Patienten eingeholt werden. Wenn die Patientinnen und Patienten von sich aus eine Nachricht schreiben, empfehlen wir, keine zusätzlichen als die selbstoffenbarten Personendaten in die Antwort zu integrieren.

[3] WhatsApp: Verwendet standardmässig Ende-zu-Ende-Verschlüsselung für Nachrichten und Anrufe.
Signal: Bietet strikte Ende-zu-Ende-Verschlüsselung für alle Kommunikationen.
Telegram: Bietet Ende-zu-Ende-Verschlüsselung in den sogenannten "Secret Chats", während normale Chats nicht standardmässig Ende-zu-Ende-verschlüsselt sind.
iMessage: Bietet Ende-zu-Ende-Verschlüsselung, aber nur zwischen Apple-Geräten.
Viber: Bietet Ende-zu-Ende-Verschlüsselung für Textnachrichten, Sprach- und Videoanrufe.
Threema: Legt grossen Wert auf Sicherheit und Datenschutz und Ende-zu-Ende-Verschlüsselung für alle Nachrichten und Anrufe.

Empfehlung 20: Bei der Entgegennahme von Kontaktanfragen über soziale Messenger-Dienste wird empfohlen, die Identität des Anfragenden zu verifizieren und die Preisgabe persönlicher Informationen ohne vorherige Überprüfung der Vertrauenswürdigkeit des Kontakts zu vermeiden.

Erklärung zur Empfehlung 20: Im Rahmen der Nutzung von Messenger-Diensten für die Kommunikation im Gesundheitswesen ist besondere Vorsicht geboten. Die Identifikation sowie die Authentizität von Personen, die Anfragen stellen – sei es Patienten, die beispielsweise nach Laborresultaten fragen, oder Ärzte sowie andere Gesundheitsfachpersonen –, kann über diese Dienste nicht immer zweifelsfrei gewährleistet werden. Im Falle, dass sich Dritte in sozialen Netzwerken fälschlicherweise als Patienten einer Praxis oder als behandelnde Ärzte ausgeben, könnte durch die Weitergabe von Patientendaten das ärztliche Berufsgeheimnis verletzt werden. Um derartige Risiken zu minimieren, sollte die Identität von Gesundheitsfachpersonen überprüft werden. Eine Methode ist die Verwendung von spezialisierten Diensten wie der Health Info Net AG (HIN), die eine Identitätsprüfung für ihre Mitglieder anbietet.[4] Des Weiteren können Gesundheitsfachpersonen ihre Identität durch offizielle Dokumente wie einen Ausweis der kantonalen Gesundheitsdirektion oder des Bundesamts für Gesundheit, die für die Registrierung und Lizenzierung von medizinischem Personal zuständig sind, nachweisen. Für spezifische Berufe im Gesundheitswesen gibt es zusätzliche Register wie das Medizinalberuferegister.

[4] Massstab für einfache Sicherheit im Schweizer Gesundheitswesen (hin.ch)

Kapitel 4: Umgang mit Patientenbildern

Medizinische Bildaufnahmen spielen eine wichtige Rolle bei der Diagnose und Behandlung, insbesondere in visuell orientierten Fachgebieten wie der Dermatologie und Plastischen Chirurgie. Solche Aufnahmen werden nicht nur zur Patienteninformation über Prozesse, Behandlungen und Nachsorge verwendet, sondern auch für Lehrzwecke, in der Forschung und für Publikationen. Sie sind ebenfalls von Bedeutung, um Zweitmeinungen von Kollegen oder Beratern einzuholen. (Al Balushi, 2019)

Als Voraussetzung für die nachfolgenden Empfehlungen zur Handhabung medizinischer Bildaufnahmen in sozialen Medien und Messenger-Diensten ist die umfassende Aufklärung der Patienten über die Verwendung ihrer Bilder und deren ausdrückliche Einwilligung zur Bildaufnahme zu betrachten. Diese Empfehlungen fokussieren sich mehr auf präventive Massnahmen zur sorgfältigen Bildaufnahme sowie die nachträgliche De-Identifizierung, weniger zur Löschung personenbezogener Daten. Im Zusammenhang mit dem sorgfältigen Umgang mit Patientenbildern sind auch die Empfehlungen zum Datenschutz zu berücksichtigen.

Empfehlung 21: Zur Wahrung der Persönlichkeitsrechte und des Datenschutzes hat die Patienteneinwilligung der abgebildeten Personen bei der Veröffentlichung von sogenannten Vorher-Nachher-Bildern oberste Priorität.

Erklärung zu Empfehlung 21: Die Veröffentlichung von Vorher-Nachher-Bildern in Messenger-Diensten und auf sozialen Medien ist ausschliesslich zulässig, wenn diese einen direkten Bezug zu einem medizinisch indizierten Eingriff aufweisen. Die Bilder müssen im Kontext der Aufklärung, Dokumentation oder Illustration des Behandlungserfolges eines solchen Eingriffs stehen und dürfen nicht primär zu Werbezwecken eingesetzt werden. Zudem ist die explizite und informierte Einwilligung der abgebildeten Personen für die Veröffentlichung einzuholen, wobei die Wahrung der Persönlichkeitsrechte und des Datenschutzes oberste Priorität hat. Es ist sicherzustellen, dass die Veröffentlichung nicht zu einer Verletzung der Privatsphäre führt oder die abgebildeten Personen in irgendeiner Weise herabwürdigt. Die Veröffentlichung von Vorher-Nachher-Bildern von Eingriffen, welche eine rein ästhetische Motivation haben, sind nicht zugelassen. Sie enthalten keine notwendigen Informationen und könnten Patienten zu medizinischen Eingriffen verleiten, derer sie objektiv nicht bedürfen.

Fallbeispiel VI: Ethisches und rechtliches Dilemma bei der Verwendung privater Smartphones zum Fotografieren von Patienten (Al Balushi, 2019)

Ausgangslage
Eine 45-jährige Patientin wurde für eine Bauchdeckenstraffung an einen Plastischen Chirurgen überwiesen, nachdem sie nach einer kleinen Gastrektomie im ersten Jahr nach der Operation 80 kg abgenommen hatte. Sie klagte über Hautüberschüsse am ganzen Körper, die sie im sozialen Bereich und im täglichen Leben beeinträchtigten. Ihr Chirurg untersuchte ihren Fall und entschied sich für mehrere Eingriffe, beginnend mit einer Bauchdeckenstraffung. Der Chirurg erklärte ihr den Eingriff, und die Patientin willigte ein. Bei der präoperativen Visite bat der Chirurg um die Erlaubnis, ein medizinisches Foto von ihr machen zu dürfen. Sie lehnte ab, weil sie sich dem männlichen Krankenhausfotografen gegenüber entblössen müsste. Im Operationssaal und vor Beginn der Operation wiederholte der Chirurg die Bitte um Fotos, die er zum Vergleich mit den postoperativen Aufnahmen machen sollte. Die Patientin zögerte, willigte dann aber ein. Er bedeckte ihren Genitalbereich und machte Fotos mit seinem eigenen Smartphone. Einen Monat später stellte sich eine ängstliche Patientin in der Klinik des Chirurgen für den gleichen Eingriff vor. Der Chirurg erklärte ihr den Eingriff und beantwortete ihre Fragen. Um ihr die Angst zu nehmen, zeigte er ihr die prä- und postoperativen Fotos seiner vorherigen Patientin von seinem eigenen Smartphone. Die neue Patientin willigte in den Eingriff ein.

Problematik
Private Smartphones sollten nicht für medizinische Fotos verwendet werden. Aspekte wie die Vertraulichkeit und Privatsphäre der Patienten könnten verletzt werden.

Alternative
Wenn ihre Verwendung für die Kommunikation mit Fachpersonen essenziell ist, sollte der Arzt eine schriftliche Einwilligung einholen, nachdem er den Personen, mit denen das Foto geteilt wird, den Zweck sowie die Risiken erläutert hat. Das Foto muss nach der Konsultation gelöscht und der Prozess in der Patientenakte dokumentiert werden.

Empfehlung 22: Bevor Geräte mit Kamerafunktion genutzt werden, ist sicherzustellen, dass alle cloudbasierten Backup-Systeme sowie die GPS-Funktion deaktiviert sind.

Erklärung zur Empfehlung 22: Kameraausgestattete Geräte sind häufig mit einem Empfänger für das Global Positioning System (GPS) versehen, welcher den exakten Standort im Moment der Aufnahme festhalten kann. Die Präzision dieser Standortdaten kann unter bestimmten Umständen bis auf wenige Meter genau sein. Bei der Aufnahme von Bildern, insbesondere in einem medizinischen Kontext, können diese GPS-Daten zur Bildung von spezifischen Patientenidentifikatoren genutzt werden. Zudem ist es wichtig, auf die bei der Bildaufnahme zusätzlich automatisch gespeicherten

Informationen zu achten – die sogenannten Metadaten. Das Exchangeable Image File Format (EXIF) ist eine häufig vorkommende Form solcher Metadaten, die zusammen mit dem Bild erstellt und gespeichert werden. Standard-EXIF-Daten umfassen in der Regel Angaben zur Kameramarke, Seriennummer, Verschlusszeit, Brennweite, Komprimierungsmodus und Blendeneinstellungen. Des Weiteren können EXIF-Daten das Datum, die Uhrzeit und den Standort der Aufnahme beinhalten.

Die Kombination aus Zeitstempel des Fotos hinsichtlich des Tages und der Uhrzeit mit der Standorterfassung über GPS-Koordinaten kann zu einer Erstellung von präzisen Patientenidentifikatoren führen. Aus datenschutzrechtlicher Sicht ist daher eine umsichtige Handhabung dieser Metadaten geboten. Vor der Verwendung von Aufnahmen im medizinischen Bereich ist sicherzustellen, dass keine sensiblen Patientendaten durch EXIF-Daten oder andere Metadaten offenbart werden. Es empfiehlt sich, alle Metadaten, die Rückschlüsse auf die Identität der abgebildeten Personen ermöglichen könnten, aus den Bildern zu entfernen oder zu anonymisieren, bevor diese weiterverarbeitet, gespeichert oder veröffentlicht werden. (Nettrour et al., 2018)

Empfehlung 23: Vor der Verwendung von Messenger-Diensten und der Veröffentlichung auf sozialen Medien müssen zwingend alle potenziellen Identifizierungsmerkmale von Bildern entfernt oder unkenntlich gemacht werden.

Erklärung zur Empfehlung 23: Es ist von essenzieller Bedeutung, dass vor der Veröffentlichung von Bildern alle Identifizierungsmerkale entfernt oder unkenntlich gemacht werden. Dies dient dem Schutz der Privatsphäre und der Einhaltung datenschutzrechtlicher Bestimmungen. Es ist darauf zu achten, dass bei der Anfertigung von Fotografien keine Gegenstände im Hintergrund erkennbar sind, die Rückschlüsse auf die Identität der abgebildeten Person zulassen könnten. Auffällige Kleidungsstücke, Schmuck und Accessoires wie Brillen sollten entfernt werden. Ebenso ist darauf zu achten, dass potenzielle Identifizierungsmerkmale wie Tattoos, Muttermale oder Narben nicht erkennbar sind. Diese können entweder durch bewusstes Weglassen im Bildausschnitt, Abdeckung mit neutraler Kleidung oder nachträgliche Bearbeitung des Fotos unkenntlich gemacht werden, um die Privatsphäre zu wahren und datenschutzrechtliche Bestimmungen einzuhalten.

Empfehlung 24: Die spiegelverkehrte Darstellung von Bildaufnahmen ist zu vermeiden, da sie zu Missinterpretationen und zu Fehldiagnosen führen kann.

Erklärung zur Empfehlung 24: Um die Korrektheit medizinischer Diagnosen zu wahren, ist es unerlässlich, bei der Übermittlung von Bildaufnahmen über Messenger-Dienste und soziale Medien darauf zu achten, dass keine Spiegelung der Bilder stattfindet. Bei der Diagnosestellung auf Basis von Bildaufnahmen, die insbesondere mit Frontkameras von mobilen Endgeräten aufgenommen werden, ist besondere Vorsicht geboten. Aufgrund der standardmässigen Spiegelbildfunktion vieler dieser Geräte kann es zu einer Verwechslung der Seiten kommen, was etwa bei einem Hautausschlag dazu führen kann, dass dieser auf der Aufnahme scheinbar auf der gegenüberliegenden Seite des Gesichts erscheint. Um solche Irrtümer zu vermeiden, sollte die Spiegelbildfunktion deaktiviert werden. Zusätzlich ist es ratsam, klar identifizierbare Markierungen vorzunehmen, um die betroffene Körperhälfte eindeutig zu kennzeichnen. So kann beispielsweise bei einer Selfie-Aufnahme die Hand der Seite, auf der sich das zu dokumentierende Merkmal befindet, mit in das Bild gehoben werden. Alternativ können auch andere eindeutige Markierungen verwendet werden, um jegliche Ambiguität für den Betrachter auszuschliessen und eine korrekte medizinische Bewertung zu gewährleisten.[5]

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

Literatur

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

Glossar

Anonymisierung	Anonymisierung ermöglicht es, den Personenbezug von Daten zu entfernen. Anonymisierte Daten können nicht mehr oder nur sehr eingeschränkt auf einzelne Personen bezogen werden und senken damit das Risiko, das sich bei der Verwendung der Daten für diese Personen ergibt.[1]
Cyberkriminelle	Cyberkriminelle sind Personen oder Gruppen, die illegale Aktivitäten im digitalen Raum durchführen, wie zum Beispiel Hacking, Betrug, Identitätsdiebstahl oder die Verbreitung von Schadsoftware, um finanzielle Gewinne zu erzielen oder Schaden anzurichten.
Data at rest	Data at rest bezieht sich auf Daten, die gespeichert und nicht aktiv übertragen werden, wie zum Beispiel auf einer Festplatte, einem USB-Stick oder einem Server.
Data in transit	Data in transit bezieht sich auf Daten, die gerade von einem Ort zum anderen übertragen werden, beispielsweise beim Senden einer E-Mail.
EXIF-Daten	EXIF-Daten sind Metadaten, die in digitalen Bildern gespeichert sind und Informationen wie Aufnahmedatum, Kameramodell, Belichtungseinstellungen und Standort enthalten können.
GPS	GPS steht für "Global Positioning System" und ist ein satellitengestütztes Navigationssystem, das es ermöglicht, die genaue Position von Objekten auf der Erdoberfläche zu bestimmen.
Pseudonymisierung	Unter Pseudonymisierung wird das Ersetzen direkter Identifikationsmerkmale von Datenpunkten in einer Weise verstanden, die dazu führt, dass die resultierenden Daten von einem Angreifer nicht oder nur mit unverhältnismässigem Aufwand wieder auf eine konkrete Person bezogen werden können. Eine Wiederherstellung des Personenbezugs soll lediglich durch Hinzuziehen von zusätzlichen Informationen (zum Beispiel einem kryptografischen Schlüssel) möglich sein.[2]
reposts	Ein "Repost" bezieht sich auf die erneute Veröffentlichung eines Beitrags oder Inhalts, der bereits auf einer Social-Media-Plattform vorhanden ist, aber von einem anderen Benutzer geteilt wird.
Selfie	Ein Selfie ist ein selbstgemachtes Foto, normalerweise mit einem Smartphone, bei dem die Person die Kamera auf sich selbst richtet.
Secur Sockets Layers (SSL)	Secure Sockets Layer (SSL) ist ein veraltetes Verschlüsselungsprotokoll, das ähnlich wie TLS verwendet wird, um die Sicherheit von Daten während der Übertragung über das Internet zu gewährleisten.
shares	In Bezug auf Social Media beziehen sich "Shares" auf die Aktion, einen Beitrag, ein Video oder eine Nachricht, die von einer Person oder einem Unternehmen erstellt wurde, mit anderen Nutzern zu teilen. Dies kann dazu beitragen, die Reichweite des Inhalts zu erhöhen und ihn einem grösseren Publikum zugänglich zu machen.
Social Engineering-Angriff	Social Engineering-Angriffe nutzen Täuschung und Manipulation aus, um menschliche Schwächen auszunutzen und Zugang zu sensiblen Informationen oder Systemen zu erlangen.

Telekonsultation	Eine Telekonsultation ist eine medizinische Beratung oder Behandlung, die über Telefon, Videoanrufe oder andere digitale Kommunikationsmittel zwischen einem Arzt und einem Patienten stattfindet, ohne dass sie sich persönlich treffen müssen.
Transport Layer Security (TLS)	TLS ist ein Verschlüsselungsprotokoll, das die Sicherheit von Daten während ihrer Übertragung über das Internet gewährleistet.

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

Impressum
Herausgeberin: FMH – Verbindung der Schweizer Ärztinnen und Ärzte, Bern
Diese Broschüre wurde im Auftrag der FMH durch Lumina Health entwickelt.
Publikation: Juli 2024
www.fmh.ch