Factsheet: Telemedizin während der COVID-19-Pandemie

Aktualisiert am: 12. Juli 2021

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

Kurzfassung Factsheet: Telemedizin während der COVID-19-Pandemie

Dieses Faktenblatt informiert Ärztinnen und Ärzte über die Möglichkeiten der sicheren telemedizinischen Konsultation im Kontext der COVID-19-Pandemie. Dies umfasst insbesondere die rechtlichen Grundlagen der telemedizinischen Konsultation, die tarifarische Abgeltung sowie eine Risikobewertung der gängigen Informations- und Kommunikationstechnologien.

Rechtliche Rahmenbedingungen	Auch im Falle einer telemedizinischen Konsultation ist die Krankengeschichte so zu führen, dass die Behandlung nachvollziehbar ist. Befunde und Behandlungsschritte müssen dokumentiert sein. Weiter ist zu erfassen, wann, von wem und auf welche Weise diese Daten erhoben wurden.	Krankengeschichte
	Die Bestimmungen des Datenschutzes und die Bestimmung des Art. 321 StGB zur ärztlichen Schweigepflicht kommen ebenso zur Anwendung wie beim persönlichen Arzt – Patientenbehandlungsverhältnis.	Datenschutz und Berufsgeheimnis
	Liegen die Daten an einem Ort, der nicht unter das schweizerische Datenschutzgesetz fällt (z.B. weil sich die Cloud im Ausland befindet) und ist der Dienstanbieter nicht bereit, sich zu verpflichten, die in der Schweiz geltende Datenschutzgesetzgebung einzuhalten, ist der Patient schriftlich darauf aufmerksam zu machen. Seine Daten sollten nur dann erhoben werden, wenn er sich mit dieser Datenbearbeitung einverstanden erklärt. Dasselbe gilt, wenn der Anbieter keine genügende Sicherheit in der Datenbearbeitung gewährleisten kann.	Einverständnis einholen
	Sobald die behandelnde Ärztin nicht mehr davon ausgehen kann, ihre Patientin mittels Telemedizin sorgfältig behandeln zu können, hat sie die Behandlung entsprechend anzupassen und die Patientin entweder selbst physisch zu untersuchen oder dann entsprechend zu überweisen.	Sorgfalt
Abrechnungsmöglichkeiten	Derzeit besteht lediglich die Tarifposition «Telefonische Konsultation durch den Facharzt» (vgl. Tarifpositionen 00.0110ff) bei welcher telemedizinische Leistungen abgerechnet werden können. Im Bereich der Psychiatrie gibt es eigene spezifische Tarifpositionen «Telefonische Konsultation durch den Facharzt für Psychiatrie» 02.0060, 02.0065 und 02.0066. Bei allen Leistungen müssen die jeweiligen Limitationen beachtet werden.	TARMED
Durch die FMH empfohlene Anwendungen	FMH und Health Info Net AG (HIN) bieten Ärztinnen und Ärzten kostenfrei eine sichere und einfache Möglichkeit für die Durchführung von Videokonferenzen an. Dieser Dienst wird im sicheren Rechenzentrum der HIN betrieben und unterliegt daher strengsten Sicherheitsvorkehrungen. Der Dienst sowie eine Anleitung sind unter der Website https://hintalkvideo.hin.ch verfügbar (benötigt Chrome-Browser).	Angebot der FMH und HIN
	Der Einsatz von Messenger- oder Videodiensten obliegt der Eigenverantwortung der Ärztin oder des Arztes. Die FMH hat in einer separaten Tabelle die gängigsten Produkte für Videokonsultationen einschliesslich einer Risikobewertung aufgeführt.	Andere Angebote

Zielsetzung

Bei der ambulanten Diagnose von COVID-19-Verdachtsfällen durch praktizierende Ärztinnen und Ärzte ist das Management von Kontaktpersonen wichtig. Aus diesem Grund kann es erforderlich sein, Informations- und Kommunikationsmittel zur telemedizinischen Konsultation (Diagnostik und Behandlung) sowie zu kommunikativen Zwecken zwischen Gesundheitsfachpersonen einzusetzen.

Dieses Faktenblatt informiert Ärztinnen und Ärzte über die Möglichkeiten der sicheren telemedizinischen Konsultation im Kontext der COVID-19-Pandemie. Dies umfasst insbesondere die rechtlichen Grundlagen der telemedizinischen Konsultation, die tarifarische Abgeltung sowie eine Risikobewertung der gängigen Informations- und Kommunikationstechnologien.

Welche rechtlichen Rahmenbedingungen sind bei der telemedizinischen Konsultation zu berücksichtigen?

Bei telemedizinischen Konsultationen müssen die Grundsätze der Führung der Krankengeschichte beachtet werden. Zudem müssen die Schweizer Datenschutzbestimmungen, das Berufsgeheimnis sowie die Sorgfaltspflicht der Ärztinnen und Ärzte berücksichtigt werden.

Krankengeschichte

Es sind dieselben Grundsätze in der Führung der Krankengeschichte zu beachten wie anlässlich einer Behandlung mit unmittelbarem Patientenkontakt. Auch im Falle einer telemedizinischen Konsultation ist die Krankengeschichte so zu führen, dass die Behandlung nachvollziehbar ist. Das ist dann gewährleistet, wenn die medizinischen Behandlungsschritte richtig und vollständig festgehalten werden. Es muss unter anderem klar sein, welcher Behandlungsschritt wann von wem durchgeführt wurde. Auch erhobene Befunde gehören dazu, weshalb entsprechende Daten, welche in der verwendeten Informations- oder Kommunikationstechnologie übertragen bzw. gespeichert werden, auch in die Krankengeschichte übertragen werden müssen. Weiter ist zu erfassen, wann, von wem und auf welche Weise diese Daten erhoben wurden.

Datenschutz und Berufsgeheimnis

Die Bestimmungen des Datenschutzes und die Bestimmung des Art. 321 StGB zur ärztlichen Schweigepflicht kommen bei Behandlungen mittels telemedizinischer Methoden ebenso zur Anwendung wie beim persönlichen Arzt – Patientenbehandlungsverhältnis.

Wie die übrigen Daten der Krankengeschichte gehören auch jene Daten, welche mittels Informations- oder Kommunikationstechnologie im Rahmen einer telemedizinischen Konsultation erhoben werden, zu dieser Datensammlung. Grundsätzlich gilt, dass Personendaten rechtmässig bearbeitet werden müssen und die Bearbeitung zweckmässig, also verhältnismässig sein muss. Es ist empfehlenswert, die Daten während 20 Jahren aufzubewahren, denn so lange dauert die privatrechtliche Verjährungsfrist.

Es muss sichergestellt werden, dass die Daten weder beschädigt noch vernichtet oder unbefugt bearbeitet werden können. Dazu gehört auch, dass Vertraulichkeit, Verfügbarkeit, Authentizität und Integrität gewährleistet sind. Werden Daten in der Cloud oder an einem anderen Ort, z. B. ausserhalb einer Arztpraxis gespeichert, muss sichergestellt sein, dass die Authentifizierung hinreichend stark und die Sicherheit gewährleistet ist.

Liegen die Daten an einem Ort, der nicht unter das schweizerische Datenschutzgesetz fällt (z.B. weil sich die Cloud im Ausland befindet) und ist der Dienstanbieter nicht bereit, sich zu verpflichten, die in der Schweiz geltende Datenschutzgesetzgebung einzuhalten, ist der Patient schriftlich darauf aufmerksam zu machen. Seine Daten sollten nur dann erhoben werden, wenn er sich mit dieser Datenbearbeitung einverstanden erklärt. Dasselbe gilt, wenn der Anbieter keine genügende Sicherheit in der Datenbearbeitung gewährleisten kann. Auch hier muss der Patient schriftlich darauf hingewiesen werden und einwilligen. Falls medizinische Daten vom Arzt an Dritte weitergegeben werden, ohne dass die Patientin nach erfolgter Aufklärung darin einwilligt, kann er zudem wegen Verletzung des Berufsgeheimnisses zur Rechenschaft gezogen werden.

Sorgfalt
Sobald die behandelnde Ärztin nicht mehr davon ausgehen kann, ihre Patientin mittels Telemedizin sorgfältig behandeln zu können, hat sie die Behandlung entsprechend anzupassen und die Patientin entweder selbst physisch zu untersuchen oder dann entsprechend zu überweisen. Befindet sich die Ärztin in Quarantäne, weil sie sich angesteckt hat, ist es möglich, das nichtmedizinische Praxispersonal ebenfalls via telemedizinische Hilfsmittel zu instruieren. Es gilt auch in diesen Fällen, dass dies nur solange gilt, als auf diese Weise eine sorgfältige Behandlung gemäss dem zu diesem Zeitpunkt gültigen medizinischen Standard möglich ist. Dabei ist auch zu beachten, dass die MPA ihre Kompetenzen nicht überschreitet, indem sie ärztliche Tätigkeiten übernimmt.

Wie können telemedizinische Konsultationen abgerechnet werden?

Derzeit gibt es im Tarifwerk TARMED lediglich die Tarifposition «Telefonische Konsultation durch den Facharzt» (vgl. Tarifpositionen 00.0110ff), bei welcher telemedizinische Leistungen abgerechnet werden können. Im Bereich der Psychiatrie gibt es dazu eigene spezifische Tarifpositionen «Telefonische Konsultation durch den Facharzt für Psychiatrie» 02.0060, 02.0065 und 02.0066.

Die FMH hat ein Merkblatt «Abrechnung medizinischer Leistungen in Zusammenhang mit COVID-19» erstellt. Die aktuellste Version ist auf der Webseite der FMH einsehbar.

Welche Anwendungen zur telemedizinischen Konsultation empfiehlt die FMH?

Der Einsatz von Messenger- oder Videodiensten obliegt grundsätzlich der Eigenverantwortung der Ärztin oder des Arztes. **Die FMH empfiehlt grundsätzlich darauf zu achten, dass die Konferenz nur zwischen den gewünschten Teilnehmern geschaltet wird (Verwendung eines Passworts, Meeting für weitere Teilnehmer sperren, Link zu Meetings nicht öffentlich teilen)**. In Tabelle 1 werden die gängigsten Produkte für Videokonsultationen einschliesslich einer Risikobewertung aufgeführt (ohne Anspruch auf Vollständigkeit). Nicht berücksichtigt werden kommerzielle Produkte von Anbieter telemedizinischer Dienstleistungen. Die Empfehlung der FMH bezieht sich ausschliesslich auf die Angaben der Hersteller.

FMH und Health Info Net AG (HIN) bieten Ärztinnen und Ärzten kostenfrei eine sichere und einfache Möglichkeit für die Durchführung von Videokonferenzen an. Dieser Dienst wird im sicheren Rechenzentrum der HIN betrieben und unterliegt daher strengsten Sicherheitsvorkehrungen. Der Dienst ist unter der Website https://hintalkvideo.hin.ch erreichbar[1]. Eine Anleitung zur Verwendung finden Sie unter http://www.hin.ch/hintalkvideo.

[1] Aus technischen Gründen ist derzeit ein Chrome-Browser erforderlich. FMH und HIN arbeitet an einer Unterstützung für andere Browser.

Tabelle 1: Risikobewertung der gängigsten Produkte für Videokonsultationen (in alphabetischer Reihenfolge, ohne Anspruch auf Vollständigkeit)

Lösung	Zertifizierungen (nicht abschliessend)	Mobile App	Account für Gast nötig	Link (Security relevante informationen)	Empfehlung FMH
HIN Talk Video	ISO 27001 RZ-Provider (Schweiz) zertifiziert nach ISO 27001:2013 sowie PCI DSS und auditiert auf die Einhaltung von FINMA-RS 08/7, RS 08/21 und RS 18/3.	Ja	Nein	Datenschutzgutachten: https://community.hin.ch/wp-content/uploads/160105-Gutachten-final-sig.pdf	**A**
Cisco WebEx	ISO 27001 ISO 9001 ISO 27018 SOC 2 Type 2 SOC 3 FedRAMP C5: Cloud Computing Compliance Controls Catalogue Swiss Privacy Shield Framework certified	Ja	Nein	https://www.webex.com/webexremotehealth.html https://www.cisco.com/c/dam/en/us/products/conferencing/cisco-webex-security-infographic.pdf Security White Paper: https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf	**A**
Google Meet	HIPAA EU Model Contract Clauses ISO 27001 ISO 27017 ISO 27018 EY POINT SOC 1 - Type 2 SOC 2 - Type 2 SOC 3 - Type 2 FedRAMP FISC Compliance Esquema Nacional de Seguridad (ENS)	Ja	Nein	https://support.google.com/a/answer/7582940?hl=en https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf https://gsuite.google.com/security/?secure-by-design_activeEl=data-centers https://cloud.google.com/security/compliance?hl=de	**B**
GoToMeeting	SOC 2 Type 2 SOC 3 C5 BSI Cloud Computing ISO 27001 AICPA`s Trust Services Criteria EU-U.S. Privacy Shield Swiss Privacy Shield	Ja	Nein	https://documentation.logmein.com/documentation/EN/pdf/common/LogMeIn_SecurityWhitepaper.pdf https://logmeincdn.azureedge.net/gotomeetingmedia/-/media/pdfs/ucc_security_white_paper.pdf https://www.logmeininc.com/legal/professional-services-terms	**B**
Lifesize	SOC ISO 27001 Swiss-U.S. Privacy Shield Framework	Ja	Ja	https://www.lifesize.com/en/solutions/industry/healthcare https://www.lifesize.com/~/media/Documents/Related%20Resources/Product%20Papers/Lifesize%20Cloud%20Security.ashx	**B**
Microsoft Teams	ISO 27001 ISO 27018 SOC 1 Type 2 SOC 2 Type 2 HIPAA FINMA HITRUST EU-US Privacy Shield Swiss-US Privacy Shield	Ja	Nein	https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-eu-us-privacy-shield?view=o365-worldwide https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide	**A**
Prexip	National Institutes of Standards & Technology (NIST) Pexip complies with the GDPR	Ja	Nein	https://www.pexip.com/healthcare https://docs.pexip.com/admin/security_best_practice.htm https://docs.pexip.com/admin/encryption_methodologies.htm	**B**
Signal	Keine Angaben	Ja	Ja (Installation App)	https://www.signal.org	**B**
Skype	Swiss-US Privacy Shield	Ja	Ja	https://support.skype.com/en/skype/all/privacy-security/ https://support.skype.com/en/faq/FA31/does-skype-use-encryption https://download.skype.com/share/security/2005-031%20security%20evaluation.pdf https://privacy.microsoft.com/en-gb/privacystatement	**B**

Lösung	Zertifizierungen (nicht abschliessend)	Mobile App	Account für Gast nötig	Link (Security relevante informationen)	Empfehlung FMH
Vidyo	ISO 9001	Ja	Nein	https://www.vidyo.com/	**A**
WhatsApp	EU-U.S. Privacy Shield Framework Swiss-U.S. Privacy Shield Framework	Ja	Ja (Installation App)	https://www.whatsapp.com/security/ https://www.whatsapp.com/legal/privacy-shield-addendum/	**B**
Wire (Pro)	GDPR-compliant ISO CCPA SOX-ready	Ja	Nein	https://wire-docs.wire.com/download/Wire+Security+Whitepaper.pdf https://wire-docs.wire.com/download/Wire+Privacy+Whitepaper.pdf https://wire.com/en/security/#audits	**A**
Zoom	SOC 2 Type 2 TRUSTe EU-US Privacy Shield FedRAMP Swiss-US Privacy Shield	Ja	Nein	https://zoom.us/security Security White Paper: https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf	**B**

Wichtige Informationen

- Alle Angaben basieren auf öffentlichen Angaben der Hersteller und nach «Best Effort» (ohne Gewähr)
- Die einzelnen Dienste werden laufend weiterentwickelt. Zudem gibt es laufend neue Publikationen zu möglichen Schwachstellen oder Einschränkungen im Bereich Datenschutz. Gültigkeit daher per Datum
- Die aktuelle starke Nachfrage nach Video-Conferencing Lösungen führt bei einigen Anbietern zu Einschränkungen (primär Performance)
- Die Empfehlung erfolgt in erster Linie aus Sicht Datenschutz und Datensicherheit. Weitere Aspekte (Benutzerfreundlichkeit, Einfachheit usw.) wurden soweit möglich miteinbezogen.

Legende
A: Wird empfohlen
B: Empfehlung mit Vorbehalt
C: nicht empfohlen