Factsheet: Telemedizin während der COVID-19-Pandemie

Datum: 20. März 2020

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. Diese Tarifposition ist jedoch eng limitiert. Pro Sitzung können in der Regel 20 Minuten, bei Patienten über 75 Jahre und unter 6 Jahren, sowie bei Patienten mit erhöhtem Behandlungsbedarf 30 Minuten pro Sitzung abgerechnet werden. Im Bereich der Psychiatrie gibt es dazu eigene spezifische Tarifpositionen «Telefonische Konsultation durch den Facharzt für Psychiatrie» 02.0060, 02.0065 und 02.0066, welche jedoch auch zwischen 20 Minuten und 40 Minuten begrenzt sind pro Sitzung. Zudem muss beachtet werden, dass die Verwendung der Tarifpositionen für einen erhöhten Behandlungsbedarf auf Nachfrage der Versicherung entsprechend begründet werden muss.

Die Limitationen begrenzen den Einsatz von telemedizinischen Konsultationen im Rahmen der COVID- 19-Pandemie. Da wir mit TARMED in der Schweiz einen vom Bundesrat festgelegten Tarif in Kraft haben, kann die FMH leider nicht bestimmen, dass telefonische Sitzungen ohne Limitationen resp. erweiterten Limitationen durchgeführt werden können. Die FMH bemüht sich jedoch um die befristete Aufhebung der Limitationen bei telefonisch ärztlichen Konsultationen für die Dauer der Pandemie. Es können aktuell noch keine endgültigen Angaben zu diesem Thema gemacht werden, da die Entscheidung um eine Anpassung der Limitationen alleine beim BAG resp. Bundesrat liegt.

Welche Anwendungen zur telemedizinischen Konsultation empfiehlt die FMH?

Der Einsatz von Messenger- oder Videodiensten obliegt grundsätzlich der Eigenverantwortung der Ärztin oder des Arztes. 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 (ohne Anspruch auf Vollständigkeit)

Lösung	Wesentliche Sicherheitsmerkmale	Zertifizierungen	Kosten	Mobile App	Account für Gast nötig	Link (Security relevante Informationen)	Bemerkungen	Empfehlung FMH
Zoom	• Die Kommunikation zwischen Client und Server ist verschlüsselt • Zusätzliche End-to End-Verschlüsselung aktivierbar (Option) • Anmeldung für Host mit Benutzername/Passwort • Beitrag Gast durch Eingabe von Meeting-ID resp. Teilnahmelink	• SSAE 16 • SOC 2 • TRUSTe • EU-US Privacy Shield • FedRAMP • No Swiss-US Privacy Shield	14.99 bis 50$ / Host / Monat	Ja	Nein	https://zoom.us/security Security White Paper: https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf	Teilnahme über Browser (mit Installation Plugin) sowie Mobile App möglich	A
GoTo-Meeting	• Die Kommunikation zwischen Client und Server ist verschlüsselt • Daten werden nicht unverschlüsselt beim Anbieter gespeichert • Keine End-to-End Verschlüsselung	• SOC 2 • SOC 3 • C5 BSI Cloud Computing • ISO27001 • AICPA`s Trust Services Criteria • EU-U.S. Privacy Shield • Swiss Privacy Shield	14.99$ / Host / Monat	Ja	Nein	https://www.gotomeeting.com/en-gb/lp/easy-online-meetings?cid=g2m_emea_ggs_cpc_generic_%2Bvideo%20%2Bcalling_b&gclid=Cj0KCQjw6sHzBRCbARIsAF8FMpWbwqa9eh2utdu5NZJEre0MKXrXlym9SCL-fulgT67CfTQToEL_F5TEaAvzqEALw_wcB	Teilnahme über Browser (mit Installation Plugin) sowie Mobile App möglich	B
Cisco WebEx	• Die Kommunikation zwischen Client und Server ist verschlüsselt • End-to-End Verschlüsselung	• ISO 27001 • SOC 2 • FedRAMP • C5: Cloud Computing Compliance Controls Catalogue • Swiss Privacy Shield Framework certified	12.85 bis 25.65 Euro / Host / Monat	Ja	Nein	https://www.webex.com/webexremotehealth.html https://help.webex.com/en-us/WBX264/How-Do-I-Allow-Webex-Meetings-Traffic-on-My-Network Security White Paper: https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf	Teilnahme über Browser (mit Installation Plugin) sowie Mobile App möglich	A
Skype	• Kommunikation zwischen Client und Server ist verschlüsselt • Keine End-to-End Verschlüsselung • "Routine monitoring by Microsoft and Government"	• Swiss-US Privacy Shield	Kostenlos oder 13.99$ / Host / Monat	Ja	Ja	https://support.skype.com/en/skype/all/privacy-security/ https://support.skype.com/en/faq/FA31/does-skype-use-encryption	Teilnahme via Skype Software (kostenlos) **Vorbehalt:** Installation von Software, Keine End-to-End Verschlüsselung, Auswertung von Kommunikationen vorgesehen	C
Lifesize	• Kommunikation zwischen Client und Server ist verschlüsselt • End-to-End Verschlüsslung	• SOC • ISO27001 • Amazon Web Services (AWS) • Swiss-U.S. Privacy Shield Framework	Kostenlos oder 12.95 bis 16.95$ / Host / Monat	Ja	Ja	https://www.lifesize.com/en/solutions/industry/healthcare https://www.lifesize.com/~/media/Documents/Related%20Resources/Product%20Papers/Lifesize%20Cloud%20Security.ashx	**Vorbehalt:** Bisher unbekannte Lösung, daher keine Erfahrungswerte.	B

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

Lösung	Wesentliche Sicherheitsmerkmale	Zertifizierungen	Kosten	Mobile App	Account für Gast nötig	Link (Security relevante Informationen)	Bemerkungen	Empfehlung FMH
Prexip	• Kommunikation zwischen Client und Server ist verschlüsselt • Keine End-to-End Verschlüsselung	• National Institutes of Standards & Technology (NIST) • Joint Interoperability Test Command (JITC) • Pexip complies with the GDPR	25$ / Host / Monat	Ja	Nein	https://www.pexip.com/healthcare https://docs.pexip.com/admin/security_best_practice.htm	**Vorbehalt:** Bisher unbekannte Lösung, daher keine Erfahrungswerte. Gemäss Hersteller keine Installation von Zusatzsoftware oder Plugin notwendig (einfache Anwendung für Gast)	B
Whats-App	• Kommunikation zwischen Client und Server ist verschlüsselt • End-to-End Verschlüsselung	• EU-U.S. Privacy Shield Framework • Swiss-U.S. Privacy Shield Framework	Kostenlos	Ja	Ja (Installation App)	https://www.whatsapp.com/security/ https://scontent.whatsapp.net/v/t61.22868-34/68135620_760356657751682_6212997528851833559_n.pdf/WhatsApp-Security-Whitepaper.pdf?_nc_sid=41cc27&_nc_ohc=avzPj7IUCQkAX8PlUfM&_nc_ht=scontent.whatsapp.net&oh=3e5e2f7a12be622db41a7fee9e858b1f&oe=5E733693	Sehr einfach, hohe Verbreitung. **Vorbehalt:** Zahlreiche Sicherheitsvorfälle in der Vergangenheit. Zudem wenig öffentlich Angaben über die implementierten Sicherheitsmassnahmen, nur via Mobile App	B
Google Meet	• Kommunikation zwischen Client und Server ist verschlüsselt • Peer-to-Peer Verbindungen (ebenfalls verschlüsselt) für Video • Keine End-to-End Verschlüsselung	• HIPAA • EU Model Contract Clauses • ISO27001 • ISO27017 • ISO27018 • EY POINT • SOC 2 & SOC 3 • FedRAMP • FISC Compliance • Esquema Nacional de Seguridad (ENS)	6 bis 25$ / Monat / Host	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	Einfache Teilnahme **Vorbehalt:** Keine End-to-End Verschlüsselung, Image von Google, Einschränkungen bei Browser (Chrome)	B
Vidyo	• Kommunikation zwischen Client und Server ist verschlüsselt • End-to-End Verschlüsselung • Eigene Installation wäre möglich	• ISO 9001	19.99$ / Monat / Host	Ja	Nein	https://www.vidyo.com/	Einfache Teilnahme, wird bereits bei CH-Spitäler genutzt	A
Signal	• Kommunikation zwischen Client und Server ist verschlüsselt • End-to-End Verschlüsselung	• Keine Angaben	Kostenlos	Ja	Ja (Installation App)	https://www.signal.com	Einfache Teilnahme **Vorbehalt:** Verschiedene Sicherheitsvorfälle in der Vergangenheit, wenig Angaben über die technische Umsetzung, geringe Verbreitung in der Schweiz	B

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

Wichtige Informationen

- Angaben basieren auf öffentlichen Angaben der Hersteller und nach "Best Effort" (ohne Gewähr)
- Die einzelnen Dienste werden laufend weiterentwickelt. 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 wie möglich miteinbezogen.