

Factsheet: Telemedizin während der COVID-19-Pandemie

Datum: 20. März 2020 erstellt durch die FMH

Abgeändert auf unsere Zwecke: 27. März 2020 mit der Zustimmung der FMH

Überarbeitet: 02. April 2020

Factsheet: Telemedizin während der COVID-19-Pandemie

Dieses Faktenblatt informiert Chiropraktorinnen und Chiropraktoren 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.

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

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.

Sobald die behandelnde Chiropraktin 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.

Abrechnungsmöglichkeiten

Mitglieder können Videokonsultationen gemäss den Empfehlungen der Tarif-Kommission in Rechnung stellen. Wir bitten alle Mitglieder den Tarifvertrag nach bestem Wissen und Gewissen anzuwenden und machen darauf aufmerksam, dass jeder Chiropraktor und jede Chiropraktin persönlich für die Rechnungsstellung verantwortlich ist.

Durch die Chirouisse empfohlene Anwendungen

Der Einsatz von Messenger- oder Videodiensten obliegt der Eigenverantwortung der Chiropraktin oder des Chiropraktors. Die FMH hat in einer separaten Tabelle die gängigsten Produkte für Videokonsultationen einschliesslich einer Risikobewertung aufgeführt. Chirouisse empfiehlt Provider mit der FMH Empfehlung A zu gebrauchen.

Krankengeschichte

Datenschutz und Berufsgeheimnis

Einverständnis einholen

Sorgfalt

Tarif

Angebot

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	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Die Kommunikation zwischen Client und Server ist verschlüsselt Daten werden nicht unverschlüsselt beim Anbieter gespeichert Keine End-to-End Verschlüsselung 	<ul style="list-style-type: none"> 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&clid=Cj0KCQjw6sHzBRCbARIsAF8FMpWbwqa9eh2utdu5NZJERE0MKXrXlym9SCLfulgT67CfTQToEL_F5TEaAvzqEALw_wcB	Teilnahme über Browser (mit Installation Plugin) sowie Mobile App möglich	B
Cisco WebEx	<ul style="list-style-type: none"> Die Kommunikation zwischen Client und Server ist verschlüsselt End-to-End Verschlüsselung 	<ul style="list-style-type: none"> 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/webexremothealth.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	<ul style="list-style-type: none"> Kommunikation zwischen Client und Server ist verschlüsselt Keine End-to-End Verschlüsselung "Routine monitoring by Microsoft and Government" 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Kommunikation zwischen Client und Server ist verschlüsselt End-to-End Verschlüsselung 	<ul style="list-style-type: none"> 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 unbekanntes Lösung, daher keine Erfahrungswerte.	B
Lösung	Wesentliche Sicherheitsmerkmale	Zertifizierungen	Kosten	Mobile App	Account für Gast nötig	Link (Security relevante Informationen)	Bemerkungen	Empfehlung

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

Prexip	<ul style="list-style-type: none"> Kommunikation zwischen Client und Server ist verschlüsselt Keine End-to-End Verschlüsselung 	<ul style="list-style-type: none"> 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	<p>Vorbehalt: Bisher unbekanntete Lösung, daher keine Erfahrungswerte.</p> <p>Gemäss Hersteller keine Installation von Zusatzsoftware oder Plugin notwendig (einfache Anwendung für Gast)</p>	B
Whats-App	<ul style="list-style-type: none"> Kommunikation zwischen Client und Server ist verschlüsselt End-to-End Verschlüsselung 	<ul style="list-style-type: none"> 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=avzPi7IUCQkAX8PIUfM&nc_ht=scontent.whatsapp.net&oh=3e5e2f7a12be622db41a7fee9e858b1f&oe=5E733693	<p>Sehr einfach, hohe Verbreitung.</p> <p>Vorbehalt: Zahlreiche Sicherheitsvorfälle in der Vergangenheit. Zudem wenig öffentlich Angaben über die implementierten Sicherheitsmassnahmen, nur via Mobile App</p>	B
Google Meet	<ul style="list-style-type: none"> Kommunikation zwischen Client und Server ist verschlüsselt Peer-to-Peer Verbindungen (ebenfalls verschlüsselt) für Video Keine End-to-End Verschlüsselung 	<ul style="list-style-type: none"> 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-qsuite.pdf https://gsuite.google.com/security/?secure-by-design_activeEl=data-centers	<p>Einfache Teilnahme</p> <p>Vorbehalt: Keine End-to-End Verschlüsselung, Image von Google, Einschränkungen bei Browser (Chrome)</p>	B
Vidyo	<ul style="list-style-type: none"> Kommunikation zwischen Client und Server ist verschlüsselt End-to-End Verschlüsselung Eigene Installation wäre möglich 	<ul style="list-style-type: none"> ISO 9001 	19.99\$ / Monat / Host	Ja	Nein	https://www.vidyo.com/	Einfache Teilnahme, wird bereits bei CH-Spitäler genutzt	A
Signal	<ul style="list-style-type: none"> Kommunikation zwischen Client und Server ist verschlüsselt End-to-End Verschlüsselung 	<ul style="list-style-type: none"> Keine Angaben 	Kostenlos	Ja	Ja (Installation App)	https://www.signal.com	<p>Einfache Teilnahme</p> <p>Vorbehalt: Verschiedene Sicherheitsvorfälle in der Vergangenheit, wenig Angaben über die technische Umsetzung, geringe Verbreitung in der Schweiz</p>	B

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.

Legende

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