Hinweise und Tipps

zum sicheren Umgang mit der Video-Chat-Software

MD Medicus als Hersteller der Video-Chat-Software ist der Schutz Ihrer personenbezogenen Daten ein ganz besonderes Anliegen. Wir als Hersteller der Video-Chat-Software haben deshalb auch ein ganz besonderes Augenmerk daraufgelegt, Ihnen mit dieser Software eine sichere und verschlüsselte Möglichkeit der Kommunikation zwischen Arzt und Patient zu eröffnen.

Die Verbindung zwischen unserem Arzt und Ihnen als Patient erfolgt über eine Punkt-zu-Punkt-Verbindung direkt vom Browser Ihres Gerätes zum Browser Ihres Gesprächspartners. Die Datenübertragung erfolgt mit einer hochsicheren Verschlüsselung (DTLS). Der Kommunikationsstream erfolgt hierbei ohne Zwischenschaltung eines Streamingservers. Ein zentraler Server ist lediglich zur Gesprächsvermittlung erforderlich. Der Server befindet sich im Hause MD Medicus und ist ausschließlich auf dem Gebiet der Bundesrepublik Deutschland stationiert. Es erfolgt keine Datenspeicherung in einer Cloud. Metadaten werden nur zur Abwicklung der zur Videokommunikation notwendigen Abläufe genutzt und nach deren Beendigung unmittelbar wieder gelöscht.

Um jedoch darüber hinaus Ihren persönlichen Daten den bestmöglichen Schutz zu gewährleisten, sollten Sie sich ebenfalls bewusst sein, dass Sie ein Arzt-/ Patienten-Behandlungsgespräch führen und Sie im Rahmen des Behandlungsgespräches hoch sensible Daten austauschen. Wir bitten Sie deshalb höflich, sich genau zu überlegen, wo, wann und auf welche Art und Weise Sie die Video-Chat-Software nutzen und durch eine sachgerechte Nutzung selbst zum Schutz Ihrer persönlichen Daten beizutragen.

Für den im Hinblick auf den Schutz Ihrer persönlichen Daten sicheren Umgang mit der Video-Chat-Software geben wir Ihnen nachfolgend einige nützliche Hinweise und Tipps.

1. Der Ort, von welchem Sie das Behandlungsgespräch führen

Achten Sie bitte beim Führen eines Behandlungsgespräches über die Video-Chat-Software in Ihrem wohlverstandenen eigenen Interesse auf einen sicheren und geschützten Raum, in welchem Sie vor den neugierigen Augen und Ohren unbeteiligter Dritter geschützt sind.

Führen Sie das Behandlungsgespräch mit unserem Arzt - wenn möglich - nur aus geschlossenen, möglichst aus Ihren Privaträumen und achten Sie darauf, dass keine unbeteiligten dritten Personen anwesend sind. Vermeiden Sie in jedem Fall öffentliche Orte (wie z.B. Flughafen, Bahnhof, Restaurants, Internetcafes und ähnlichen Orten). Bedenken Sie insoweit auch, dass im Rahmen eines solchen Behandlungsgesprächs nicht nur Ihre personenbezogenen Daten, sondern möglicher Weise auch personenbezogene Daten unseres Arztes offenbart werden könnten.

2. Führen eines Behandlungsgesprächs aus dem Ausland

Sollten Sie sich im Ausland aufhalten und beabsichtigen, ein Behandlungsgespräch mittels der Video-Chat-Software aus dem Ausland zu führen, beachten Sie bitte, dass nicht jedes Land ein angemessenes und ausreichendes Datenschutzniveau aufweist. Beachten Sie bitte auch, dass ein hinreichendes Datenschutzniveau lediglich in den EU-Staaten und einiger weniger Drittstaaten gewährleistet ist, für welche die EU-Kommission entsprechende Angemessenheitsbeschlüsse gefasst hat. Ein Angemessenheitsbeschluss gibt es für:

Andorra, Argentinien, Färöer-Inseln, Guernsey, Isle of Man, Israel (eingeschränkt), Jersey, Kanada (eingeschränkt), Neuseeland, Schweiz und Uruguay, USA (bzgl. Privacy Shield) und Japan. Darüber hinaus laufen aktuell Verhandlungen der EU-Kommission mit Südkorea für eine Angemessenheitsentscheidung.

Beachten Sie insoweit bitte auch, dass im Falle des Austritts von Großbritannien (Brexit) aus der EU automatisch auch Großbritannien zu einem unsicheren Drittland im Sinne der DSGVO wird. Darüber hinaus sollten Sie darauf achten, dass die Verschlüsselung von Daten für die Datenübertragung in einzelnen Drittländern, in denen man nicht unbedingt europäische Werte und Ansichten von Freiheit und Demokratie teilt, verboten sein könnte. Sie sollten sich diesbezüglich unbedingt vor Antritt einer Reise informieren.

Darauf hinzuweisen ist, dass nach Art. 9 DSGVO i.V.m. Art. 44 ff DSGVO eine Übermittlung personenbezogener Daten in ein Drittland - von einigen wenigen Ausnahmen abgesehen - grundsätzlich nur mit der Zustimmung Ihres Gesprächspartners (Art. 49 Abs. 1 Lit. a DSGVO) zulässig ist. Sollten Sie sich deshalb in einem Drittland im Sinne der DSGVO aufhalten, so informieren Sie hierüber bitte Ihren Gesprächspartner vor oder ganz zu Beginn des Gespräches und holen Sie dessen ausdrücklich Zustimmung für das Behandlungsgespräch ein.

3. Aktualität Ihrer Software

Die Sicherheit Ihrer Daten hängt u.a. auch von der Aktualität Ihrer Software, insbesondere Ihres Betriebssystems und Ihres Browsers ab. Aktualisieren Sie deshalb bitte regelmäßig Ihr Betriebssystem und Ihren Browser. Um kein Sicherheitsupdate zu versäumen, sollten Sie gegebenenfalls die Up-Date-Automatisierung einschalten. In keinem Fall sollten Sie ein bereits abgekündigtes Betriebssystem oder ein Betriebssystem nutzen, welches durch den Hersteller nicht mehr mit Sicherheits-Up-Dates versorgt wird. In diesem Zusammenhang erlauben wir uns den Hinweis, dass die Fa. Microsoft für das Betriebssystem "Windows 7" den kostenlosen Supports Ende Januar 2020 beendet hat.

Die Aktualisierung von Betriebssystem und Browser ist auch im Hinblick auf die Verschlüsselungstechnik nicht nur sinnvoll, sondern regelrecht geboten. Zur Sicherung des Datenschutzes wird das Gespräch verschlüsselt. Zwar setzt die Video-Chat-Software moderne Verschlüsselungstechniken ein, diese gehen jedoch fehl, wenn Ihr Hardwaregerät und/ oder die von Ihnen eingesetzte Software diese Technik nicht unterstützt.

Die Verschlüsselung Ihrer Daten basiert auf einem von Ihrem Browser mit dem Server ausgehandelten Verschlüsselungsstandard. Hierbei richtet sich die Qualität der Verschlüsselung auch nach der Aktualität Ihres Browsers. Verwenden Sie einen sehr alten Browser, so kann dieser nur ältere Verschlüsselungsstandards, die in der Regel nicht so sicher sind, wie neuere. Daher sorgen Sie dafür, dass Sie sowohl Ihr Betriebssystem als auch den verwendeten Browser auf dem neuesten Stand halten.

4. Technische und organisatorische Maßnahmen zum Schutz Ihres PC

Schützen Sie bitte Ihren PC vor Angriffen von unbefugten Dritten von außen. Die Aktualisierung Ihres Betriebssystems und Ihres Browsers allein bietet keinen hinreichenden Schutz Ihrer Daten. Sie sollten deshalb in jedem Fall zusätzlich einen aktuellen Virenscanner auf Ihrem Endgerät installiert und eine Firewall eingerichtet haben und diese regelmäßig, am besten auch mittels automatischer Up-Date-Funktion aktualisieren.

Schützen Sie Ihren Rechner und Ihren Internetanschluss möglichst auch durch ein hinreichend sicheres Passwort. Bei der Wahl Ihres Passwortes sollten Sie die empfohlenen Standards beachten. So empfiehlt z.B. das Bundesamt für Sicherheit in der Informationstechnik (BSI) für Onlinezugänge Passwörter mit mindestens zwölf Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern zu verwenden, für WLAN-Zugänge hingegen Passwörter aus mindestens zwanzig Zeichen. Dies ist insbesondere dann nötig, wenn eine unbeschränkte Anzahl von Versuchen mit verschiedenen Passwörtern einen Zugang zulässt und damit einen Angriff („Erraten“) nach der sogenannten Brute-Force-Methode ermöglicht. Entsprechendes gilt zum Schutz Ihres PC.

Vermeiden Sie einfache Passworte wie z.B. "123456" oder auch die Tastaturfolgen wie z.B. "qwertz". Wechseln Sie, wenn möglich, das Passwort regelmäßig, spätestens nach Ablauf eines Zeitraums von 3 Monaten. Benutzen Sie für unterschiedliche Anwendungen unterschiedliche Passworte. Bedenken Sie vor allem auch, dass die Sicherheit Ihres Passwortes auch davon abhängt, dass es geheim bleibt. Vermeiden Sie es deshalb am besten, Ihr Passwort zu notieren und die Notiz irgendwo zu deponieren. Untersagen Sie Ihrem PC bitte auch die Speicherung Ihres Passwortes.

5. Bilder und Dokumente

Über die Video-Chat-Software haben Sie gegebenenfalls auch die Möglichkeit auf Ihrem PC gespeichert Bilder und Dokumente (z.B. Röntgenbilder etc.) an Ihren Gesprächspartner zu übersenden. Wenn Sie im Rahmen eines ärztlichen Videogespräches Bilder aufnehmen oder Dokumente erhalten, denken Sie bitte daran, dass diese möglicherweise in ungesicherten Bereichen Ihres Gerätes gespeichert werden.

Wenn Sie als Patient unserem Arzt entsprechende Bilder und Dokumente übersenden möchten, so bedenken Sie bitte, dass diese in ungesicherten Bereichen Ihres Gerätes gespeichert werden. Um Ihre Sicherheit zu gewährleisten, sollten Sie die gespeicherten Bilder und Dokumente wieder löschen, sobald das Behandlungsgespräch beendet ist und/ oder Sie diese nicht mehr benötigen.