Technisches und rechtliches Rezertifizierungs-Gutachten - Kurzgutachten -

“RED Medical“

für:
RED Medical Systems GmbH
Lutzstraße 2
80687 München

für das Gütesiegel für IT-Produkte (ULD)

erstellt von:

Andreas Bethke
Dipl. Inf. (FH)
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (technisch)

Papenbergallee 34
25548 Kellinghusen
tel 04822 – 36 63 000
fax 04822 – 36 63 333
mob 0179 – 321 97 88
email bethke@datenschutz-guetesiegel.sh

Stephan Hansen-Oest
Rechtsanwalt
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich)

Im Tal 10a
24939 Flensburg
tel 0461 – 900 138 21
fax 0461 – 900 138 22
mob 0171 – 20 44 98 1
email sh@hansen-oest.com

Stand: 03.05.2018

A. Einleitung

Die RED Medical Systems GmbH strebt die Rezertifizierung ihres Produktes „RED Medical“ für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) an.
Die Vorlage eines rechtlichen und technischen Gutachtens ist Voraussetzung für die Rezertifizierung des Produktes. Dieses Dokument dient als Gutachten zur Vorlage beim ULD im Zusammenhang mit der Rezertifizierung des Produktes.
Dem Gutachten wird der Anforderungskatalog in der Version 2.0 zugrunde gelegt.
Eine Änderung an dem Produkt gab es seit der letzten Rezertifizierung am 19.12.2016 nicht.

Evaluationsmethoden:

Der Produkthersteller hat mitgeteilt und versichert, dass am Kernprodukt keine Änderungen erfolgt sind. Hinzugekommen ist jedoch das zusätzliche Modul der „RED Connect Videosprechstunde“. Für dieses Modul hat der Hersteller eine umfangreiche und verständliche Dokumentation zur Verfügung gestellt.
Das WebRTC-Protokoll ist ein Standardprotokoll für verschlüsselte „flüchtige“ Kommunikation über eine Ende-zu-Ende-Verschlüsselung, der hier beschrieben ist: https://www.w3.org/TR/webrtc/

Im Hinblick auf WebRTC wurde die technische Einbindung überprüft.

B. Zeitpunkt der Prüfung

Die Prüfung des Produktes fand vom 31.01.2018 bis zum 03.05.2018 statt.

C. Änderungen und Neuerungen des Produktes

Seit der letzten Rezertifizierung des Produktes im Dezember 2016 wurde das Produkt in der zertifizierten Version nicht weiterentwickelt.
Jedoch wurde ein Modul entwickelt, das über das Produkt verfügbar gemacht wird. Diese Änderung nennt sich „**RED Connect Videosprechstunde**“ und ist Teil des

Zertifizierungsgegenstands. Dieses zusätzliche Modul greift jedoch *nicht* auf den Datenbestand des Kernproduktes zu.

Das Modul beinhaltet folgende Services:
Der Hersteller möchte den Anwendern seines bestehenden Arzt-Informations-Systems zusätzlich die Möglichkeit geben, mit deren Patienten entsprechende Videosprechstunden durchzuführen. Hierbei soll die Videosprechstunde als separater Dienst betrieben werden, und die bestehende Anwendung nur insofern berühren, als von dieser aus Termine für Videosprechstunden angefordert werden können. Die Implementierung folgte dabei den Vorgaben der Kassenärztlichen Bundesvereinigung (KBV).
Diese sehen vor, dass

a) sich der Arzt für den Videodienst registrieren muss;
b) der Videodienst keinen Zweitzugang vorhalten muss;
c) Patienten sich ohne Account anmelden können müssen, der Klarname für den Arzt jedoch erkennbar sein muss;
d) der Zugang nur zum Kontakt mit dem initierenden Arzt führen und zeitlich höchstens auf einen Monat begrenzt sein darf;
e) der Anbieter gewährleisten muss, dass die Videosprechstunde ungestört durchgeführt werden kann;
f) die Videosprechstunde über eine Peer-to-Peer-Verbindung und ohne Einsatz eines zentralen Servers zu erfolgen hat (der zentrale Server darf höchstens als Gesprächsvermittler fungieren);
g) der Anbieter gewährleisten muss, dass sämtliche Inhalte verschlüsselt sind (Ende-zu-Ende);
h) die eingesetzte Software bezüglich Ton- und Bildqualität adaptiv sein muss bei Schwankungen in der Verbindungsqualität
i) der Anbieter des Dienstes keinen Zugriff auf die Inhalte einer Sprechstunde haben darf;
j) der Anbieter nur Server, die in der EU stehen, nutzen darf und Metadaten nach 3 Monaten gelöscht werden müssen;

k) die Nutzungsbedingungen in deutscher Sprache und ohne vorige Anmeldung online abrufbar sein müssen;
l) Werbeeinblendungen nicht erlaubt sind.

Der Prozess ist so ausgestaltet, dass sich der Arzt zunächst registrieren muss um an einer Videosprechstunde teilzunehmen.

Dann erzeugt der Arzt im RED Medical einen neuen Termin für eine Videosprechstunde. Es werden zwei Zugangscodes generiert. Ein Code für den Arzt und ein Code für den Patienten. So wird gewährleistet, dass nur Arzt und der betreffende Patient miteinander kommunizieren.
In technischer Hinsicht erfolgt die Videokommunikation über das sog. WebRTC-Protokoll, dass mittlerweile von allen modernen Browsern unterstützt wird.[1]

Der zentrale Server für den Verbindungsaufbau wird erreicht über https://connect.redmedical.de. Der Server wird auf einem dedizierten Server im Rechenzentrum der Hetzner GmbH gehostet.
Über eine VPN-Verbindung wird die entsprechende API-Funktion aufgerufen und es wird automatisch ein Chat-Raum eingerichtet. Der Arzt sieht die Codes in der Patienten-Akte und reicht den Patienten-Code offline (also per Ausdruck oder mündlich) weiter.

Abbildung 1 - Screenshot des Bildschirms des Arztes

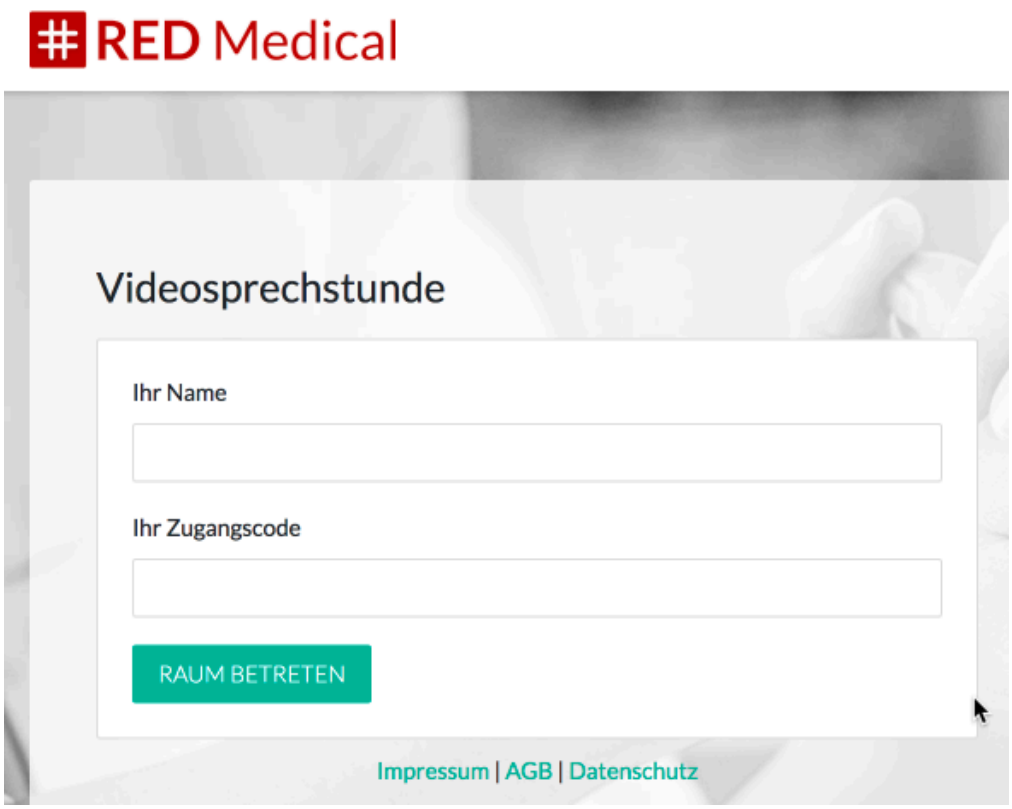
[1] Eine Übersicht findet sich hier: https://caniuse.com/#search=webrtc; Der Internet Explorer wird von RED Medical und auch von der Videosprechstunde nicht unterstützt

Dann melden sich beide Teilnehmer mit ihrem Namen und dem Code ein, wobei das System nicht prüft, ob der Name korrekt ist, da es die Teilnehmer nicht kennt. Es kann also auch ein Fantasiename sein. Der Arzt hat die Information über seinen Patienten sowieso im RED Medical.
Über die betreffenden eindeutigen Codes ist jedoch eine Zuordnung des Patienten für den Arzt möglich.

Auf der Login-Seite erhalten die Teilnehmer sämtlichen datenschutzrelevanten Informationen.

D. Datenschutzrechtliche Bewertung

Bei der Nutzung der „Videosprechstunde“ werden nur ein Zugangscode und ein Name des Patienten verarbeitet. Beim Namen wäre zudem die Nutzung eines Pseudonyms möglich, wenn der Arzt dies im Hinblick auf die Therapiesicherheit für ausreichend hält.



Die Verarbeitung dieser Daten ist nach § 14 TMG bzw. Art. 6 Abs. 1 lit. b) DSGVO zulässig, da sie für die Durchführung der vertraglichen Leistungen erforderlich ist.

Die Kommunikationsdaten sind komplett verschlüsselt und werden nicht gespeichert. Auch diese (flüchtige) Verarbeitung ist für die Durchführung der vertraglichen Leistungen zwingend erforderlich. Rechtsgrundlagen wären hier § 15 Abs. 1 TMG bzw. Art. 6 Abs. 1 lit. b) DSGVO.[2]

Zentraler Punkt für die datenschutzrechtliche Bewertung ist zum einen die Verschlüsselung. Hier werden folgende Mechanismen eingesetzt:

- TLS 1.2 mit SHA 256
- AES 128
- RSA 2014

Damit folgt der Hersteller der BSI Richtlinie TR-02102.
Im Sinne der Datenvermeidung und Datensparsamkeit werden durch das Modul keine weiteren personenbezogenen Daten erhoben.

Die zum Einsatz kommende WebRTC-Technologie erlaubt es, direkt aus Browsern heraus Audio- und Video-Verbindungen aufzubauen. Die Besonderheit im Vergleich zu anderen Videokonferenzdiensten wie z.B. Skype ist, dass die Verbindung zwischen den Teilnehmern über das Internet direkt ("Peer-to-Peer") erfolgt, die ausgetauschten Kommunikationsdaten also nicht über zentrale Server des Diensteanbieters geleitet werden. Das WebRTC-Framework basiert auf HTML5 und JavaScript und kann daher direkt im Browser ohne weitere Zusatzinstallation ausgeführt werden. Die ausgetauschten Datenströme sind nach dem WebRTC-Protokoll verschlüsserlt.

WebRTC (Web Real-Time Communication) wird in Form von JavaScript-APIs zur Verfügung gestellt. Damit lassen sich nicht nur Audio- und Video-Verbindungen bewerkstelligen, sondern auch anderes wie Chat, Screen-Sharing und Dateitransfers.

[2] Es kann dahinstehen, ob der Dienst ggf. als Telekommunikationsdienst i.S.d. TKG einzustufen ist. Selbst bei einer entsprechenden Einordnung, die von den Sachverständigen hier nicht vertreten wird, wäre die Datenverarbeitung nach § 96 TKG zulässig, weil sie für Aufbau, Unterhaltung und Beendigung der Verbindung erforderlich wäre.

Datenfluss bei WebRTC

Anwendungs- und Konfigurationsdaten gehen getrennte Wege: Der Server fungiert als Router, der Konfigurationsdaten wie beispielsweise IP-Adressen oder Angaben zu Video- und Audioformaten von dem einem Browser entgegennimmt und an den anderen weiterleitet („Signaling“ nach WebRTC).

Innerhalb des Videosprechstunden-Systems werden überhaupt keine Daten gespeichert. Die Zugangscodes befinden sich im Speicher von RED Medical. Deren Korrektheit wird vom Videosprechstundenserver dort abgefragt. IP-Adressen werden nicht gespeichert. Die tatsächliche Länge einer Videosprechstunde kann gar nicht abgespeichert werden, weil keiner der Server von RED Medical am eigentlichen Telefonat beteiligt ist.

Bei einem wie von RED Medical angebotenen Dienst einer „Videosprechstunde“ ist rechtlich umstritten, ob es sich um einen Telekommunikationsdienst oder Telemediendienst handelt. Mit Geltung der DSGVO wäre weiterhin ggf. umstritten, ob es sich um einen Telekommunikationsdienst, der dem Anwendungsbereich der ePrivacy-Richtlinie der EU (2002/58/EG) unterliegt, oder um eine Datenverarbeitung i.S.d. der DSGVO handelt. In rechtlicher Hinsicht kann dieser Streit mit Blick auf den Zertifizierungsgegenstand jedoch dahinstehen. Denn der Dienst der Videosprechstunde stellt ein Zusatzmodul für das Produkt „RED Medical“ dar. Inhaltlich werden durch den Hersteller damit keine über das Grundprodukt hinaus andere Kategorien von Daten im Auftrag verarbeitet. Auch der Zweck ist derselbe. Das Zusatzmodul ist daher von dem zwischen RED Medical und dem jeweiligen Arzt geschlossenen Auftragsdatenverarbeitungsvertrag umfasst.

Aufgrund der Tatsache, dass der Produkthersteller aus den Daten keinen Personenbezug herleiten kann, werden unabhängig von der Einordnung die jeweils geltenden rechtlichen Vorgaben eingehalten.

Insgesamt kann festgestellt werden, dass die Datenverarbeitung im Zusammenhang mit dem Modul „Videosprechstunde“ in rechtlich zulässiger Weise erfolgt.

Einhaltung der Anforderungen der „Vereinbarung über die Anforderungen an die technischen Verfahren zur Videosprechstunde gemäß § 291g Absatz 4 SGB V“

Der GKV-Spitzenverband, K. d. ö. R. und die Kassenärztliche Bundesvereinigung haben eine Vereinbarung über die Anforderungen an die technischen Verfahren zur Videosprechstunde gemäß § 291g Absatz 4 SGB V getroffen[3], deren Einhaltung im Hinblick auf die rechtliche Begutachtung ebenfalls zu prüfen war.

Nachfolgend werden die Anforderungen aus § 5 dieser Vereinbarung dargestellt und jeweils aufgezeigt wie die Anforderung von dem Produkt bzw. Hersteller unterstützt bzw. eingehalten wird:

1. Der Arzt muss sich für den Videodienst registrieren.
→ Da nur registrierte Anwender des Arzt-Informations-Systems "RED Medical" Videosprechstunden-Termine vergeben und die entsprechenden Zugangscodes erhalten können, findet der Zwang zur Registrierung für den Arzt implizit über die Registrierung für "RED Medical" statt.

2. Der Videodienst muss keinen Zweitzugang vorhalten. Sofern ein Zweitzugang für Praxispersonal möglich ist, darf dieser allein und ausschließlich zu organisatorischen Zwecken im Zusammenhang mit der Videosprechstunde genutzt und mit diesem keine Videosprechstunde durchgeführt werden.
→ Das System verfügt über keinen Zweitzugang.

3. Patienten müssen sich ohne Account anmelden können, der Klarname des Patienten soll für den Arzt erkennbar sein. Der Zugang darf nur zum Kontakt mit dem initiierenden Arzt führen und muss zeitlich auf höchstens einen Monat befristet sein.
→ Patienten müssen sich nicht registrieren, sondern können nur durch Eingabe ihres Klarnamens, der dem Arzt später angezeigt wird, und dem passenden Zugangscode anmelden. Durch die Kombination von Arztcode und Patientencode kann das Videotelefonat nur zu dem initiierenden Arzt führen. Es ist gewährleistet, dass vergebene

[3] Zu finden unter: http://www.kbv.de/media/sp/Anlage_31b_Videosprechstunde.pdf

Zugangscodes 24 Stunden nach dem entsprechenden Termin ihre Gültigkeit verlieren.

4. Der Videodienstanbieter muss gewährleisten, dass der Arzt die Videosprechstunde ungestört, z. B. ohne Signalgeräusche weiterer Anrufer, durchführen kann.
→ Dies wird durch die WebRTC-Technologie gewährleistet.

5. Die Übertragung der Videosprechstunde erfolgt über eine Peer-to-Peer-Verbindung, ohne Nutzung eines zentralen Servers. Ein zentraler Server darf lediglich zur Gesprächsvermittlung genutzt werden.
→ Dies wird durch die WebRTC-Technologie gewährleistet.

6. Der Videodienstanbieter muss gewährleisten, dass sämtliche Inhalte der Videosprechstunde während des gesamten Übertragungsprozesses nach dem Stand der Technik Ende-zu-Ende, beispielsweise nach der Technischen Richtlinie 02102 des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils aktuell gültigen Fassung, verschlüsselt sind.
→ Dies wird durch die WebRTC-Technologie gewährleistet.

7. Die eingesetzte Software muss bei Schwankungen der Verbindungsqualität bezüglich der Ton- und Bildqualität adaptiv sein. Die Entscheidung über die Durch- bzw. Fortführung der Videosprechstunde bei abnehmender Ton- und Bildqualität obliegt den Gesprächsteilnehmern. Sofern Konkretisierungen zu den Anforderungen an die bei der Übertragung einzusetzende Technik sowie Bild- und Tonqualität erforderlich sind, werden diese in einem anwendungsspezifischen Anhang zu dieser Anlage zum Bundesmantelvertrag-Ärzte indikationsbezogen geregelt.
→ Dies wird durch die WebRTC-Technologie gewährleistet.

8. Sämtliche Inhalte der Videosprechstunde dürfen durch den Videodienstanbieter weder eingesehen noch gespeichert werden.
→ Dies wird durch die WebRTC-Technologie gewährleistet.

9. Videodienstanbieter dürfen nur Server in der EU nutzen. Alle Metadaten müssen nach spätestens drei Monaten gelöscht werden und dürfen nur für die zur Abwicklung der Videosprechstunde notwendigen Abläufe genutzt werden. Die Weitergabe der Daten ist untersagt.
→ RED Medical verwendet nur Server, die sich in Deutschland befinden. Metadaten werden nicht gespeichert.

10. Die Nutzungsbedingungen müssen vollständig in deutscher Sprache und auch ohne vorherige Anmeldung online abrufbar sein.
→ Die Nutzungsbedingungen (AGB) sind in deutscher Sprache vor der Anmeldung auf der Webseite einsehbar. Außerdem wird der Anwender durch verschiedene FAQ-Texte über die Nutzung der Videosprechstunde aufgeklärt.

11. Das Schalten von Werbung im Rahmen der Videosprechstunde ist untersagt.
→ Eine Werbung erfolgt nicht.

Nach alledem ist festzustellen, dass die Vorgaben der „Vereinbarung über die Anforderungen an die technischen Verfahren zur Videosprechstunde gemäß § 291g Absatz 4 SGB V“ beim Einsatz des Produktes eingehalten werden.

E. Wie das Produkt den Datenschutz fördert

Die Stärke des Produktes liegt in der sofortigen Verschlüsselung der Daten, die noch auf dem Client stattfindet, also noch vor der Übertragung und Speicherung.
Somit ist es nur der Daten verarbeitenden Stelle möglich, die Daten mit Personenbezug zu lesen, nicht aber Dritten, wie dem Hersteller oder seinen Dienstleistern. Das heißt, sobald ein Feld ein identifizierbares Datum enthalten kann wird das Feld verschlüsselt. Darüber hinaus werden alle auch alle anderen Daten, die in den Anwendungsbereich von § 203 StGB erfasst sind, verschlüsselt.
Insgesamt gibt es keine unverschlüsselten Felder, die patientenidentifizierende Daten enthalten können.

In Punkto Transparenz geht der Hersteller über das übliche Maß hinaus und liefert seinen clientseitigen Programmcode in lesbarer Form mit aus. Darüber hinaus hat der Hersteller in seiner Dokumentation beschrieben, wie der Anwender die Verschlüsselungsmodule selbst auf Manipulationsfreiheit hin überprüfen kann.

F. Zusammenfassung

Insgesamt kann festgestellt werden, dass auch mit dem neuen Produkt die Rechtsvorschriften zu Datenschutz und Datensicherheit eingehalten werden.

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Kellinghusen, den 03.05.2018

Andreas Bethke

Flensburg, den 03.05.2018

Stephan Hansen-Oest