Kurzgutachten

„RED Medical“

für RED Medical Systems GmbH
c/o Jochen Brüggemann
Maximilianstr. 16
82319 Starnberg

für das Gütesiegel für IT-Produkte (ULD)

von

Andreas Bethke
Dipl. Inf. (FH)
Papenbergallee 34
25548 Kellinghusen
email: bethke@datenschutz-guetesiegel.sh

Stephan Hansen-Oest
Rechtsanwalt & Fachanwalt für IT-Recht
Neustadt 56
24939 Flensburg
email: sh@hansen-oest.com

Date: 11.07.2013

Inhaltsverzeichnis

A. Zeitpunkt der Prüfung

Die Prüfung des Verfahrens fand von 17.10.2012 bis 10.07.2013 statt.

B. Adresse des Antragstellers

RED Medical Systems GmbH
c/o Jochen Brüggemann
Maximilianstr. 16
82319 Starnberg

C. Adresse der Sachverständigen

Andreas Bethke
Dipl. Inf. (FH)
Papenbergallee 34
25548 Kellinghusen
email: bethke@datenschutz-guetesiegel.sh

Stephan Hansen-Oest
Rechtsanwalt & Fachanwalt für IT-Recht
Neustadt 56
24939 Flensburg
email: sh@hansen-oest.com

D. Kurzbezeichnung

RED Medical

E. Detaillierte Bezeichnung des Begutachtungsgegenstandes

RED Medical (im Folgenden kurz RED genannt) ist eine Webapplikation, die alle administrativen und medizinischen Prozesse einer Arztpraxis unterstützt. Durch ein zentrales Hosting von RED und einer verschlüsselten Speicherung der personenbezogenen Daten in einem sicheren Rechenzentrum kann die Praxis auf den Betrieb einer eigenen komplexen IT-Infrastruktur verzichten.

Die Daten verarbeitende Stelle ist jedoch angehalten die Software in einer möglichst sicheren Systemumgebung zu betreiben. Da vom Hersteller keine solche Hardware geliefert wird, muss diese von der einsetzenden Stelle erst geschaffen werden. Hierzu hat der Hersteller in seiner Dokumentation entsprechende Empfehlungen ausgesprochen. Nur in einer solchen abgesicherten Umgebung ist der Einsatz der Software unter

datenschutzrechtlichen Aspekten zu empfehlen. Die Zertifizierung bezieht sich auf eine solche Systemumgebung.
Die Benutzung der Software ist an Geräte, sog. „Terminals“ gebunden. Diese gehören zu einer Praxis oder einem Krankenhaus und müssen explizit durch einen berechtigten Benutzer freigegeben werden. Diese Freigabe kann jederzeit widerrufen werden, so dass Geräte nur für einen notwendigen Zeitraum freigegeben werden. Somit ist auch eine temporäre „Sperrung“ eines „Terminals“ möglich, etwa bei Abwesenheit wie Urlaub.

Der Zugriff auf RED erfolgt dabei über ein internetfähiges Gerät mit einem Standard-Browser. Somit können Ärzte jederzeit und von jedem Ort über gesicherte Verfahren (Datenverschlüsselung) auf ihre Daten zugreifen. Das ermöglicht eine Verfügbarkeit von wichtigen Patientendaten z. B. vor Ort am "Bett des Patienten".
Durch die schon im Browser stattfindende Datenverschlüsselung sowie durch eine mandantenbezogene Trennung innerhalb der Datenhaltung wird sichergestellt, dass Unbefugte keinen Zugriff auf Patientendaten haben und auch zwischen Berufsgeheimnisträgern die Vorgabe der ärztlichen Schweigepflicht i.S.d. § 203 StGB eingehalten werden.
Das Produkt gliedert sich in die vier folgenden Bereiche:

- Organisation: Einrichtung und Verwaltung der Organisationsstruktur
- Administration: Aufnahme und Verwaltung der Patienten, Abrechnung der Leistungen
- Medizinische Dokumentation: Führen der Patientenakte
- Arzneimittelverschreibung: Alles rund um das Thema Arzneimittel

Das Produkt kommuniziert mit externer Peripherie. Hierzu gehören Chipkartenleser und Drucker. Grundsätzlich können JavaScript-basierte Webseiten nicht oder nur sehr eingeschränkt auf die Ressourcen des PCs zugreifen, auf dem sie laufen. Ein Zugriff auf Hardware oder Peripheriegeräte ist ebenso unmöglich wie das Starten anderer Prozesse. Genau diese Funktionen müssen jedoch von dem System ausgeführt werden, um z. B. einen Drucker oder Chipkartenleser anzusprechen oder Daten aus der Schnittstelle eines Medizintechnik-Gerätes entgegen zu nehmen. Hierfür stellt der Hersteller ein sog. "Plugin" zur Verfügung, das auf dem PC installiert werden muss. Mithilfe dieses Plugins können von der Web-Applikation die entsprechenden Funktionen aufgerufen werden.

Beim Zugriff auf einen Chipkartenleser verfügt das Plugin über die Möglichkeit, die CT_API des jeweiligen Lesegerätes anzusprechen. Die Lesegeräte sind dabei nicht Teil des Zertifizierungsgegenstandes. Wenn eine Chipkarte (KVK oder eGK) eines Patienten eingelesen werden soll, spricht der RED-Client die entsprechende Funktion des Plugins an und liest darüber die Kartendaten ein. Eine Speicherung von Daten auf der Chipkarte ist derzeit gemäß den Festlegungen der „gematik“ nicht möglich.
Der Zugriff auf Drucker oder die Ansteuerung eines bestimmten Druckers erfolgt über eine direkte Ansteuerung durch das Plugin, um Druckfunktionen für den Anwender bequem zur Verfügung zu stellen.
Weiterhin greift das Produkt auf externe Medizintechnikprogramme zu, um von diesen erzeugte Daten zur Dokumentation in die Patientenakte zu übernehmen. Diese Systeme sind in der Regel auf dem Rechner des jeweiligen Nutzers installiert und dienen dazu, medizinische Geräte anzusteuern, ihre Daten auszulesen und den Arzt bei der Befundung und Diagnostik zu unterstützen. Anschließend werden diese Daten an RED übergeben und dort gespeichert. Eine Analyse der Daten findet nicht im Produkt statt. Die Kommunikation ist dabei bidirektional. So übergibt RED u. U. einen Patientennamen an ein Gerät, damit dieses den Namen im Rahmen der Messung angezeigt und ggf. ausdruckt, oder um zu einem früheren Zeitpunkt aufgenommen Messwerte in dem Programm anzuzeigen. Die Datenübergabe geschieht dabei über eine Datei, die nach dem Beenden des externen Programms wieder gelöscht wird.
Es werden – wenn überhaupt – nur der Patientenname und die Daten der letzten Messung an das Drittprogramm übertragen. In der Regel werden meist sogar nur Daten von dem Drittprogramm an RED Medical übergeben. Für jeden Datenaustausch wird ein „Akteneintrag“ von der Software dokumentiert, so dass nachvollzogen werden kann, wann Daten mit welchem Gerät bzw. welcher Software ausgetauscht wurden. Eine weitergehende Dokumentation ist insoweit nicht erforderlich.

Außerdem erfolgt aus RED ein Zugriff auf das Prüf- und Kryptomodul der Kassenärztlichen Bundesvereinigung. Im Rahmen der Abrechnung müssen die Abrechnungsdaten zunächst vom KBV-Prüfmodul geprüft und nach erfolgreicher Prüfung vom KBV-Kryptomodul verschlüsselt werden. Die entsprechenden Abrechnungsdaten (die innerhalb der Datei übergebenen Daten ergeben sich aus der KVDT-Datensatzbeschreibung der KBV) werden dazu auf die lokale Festplatte des entsprechenden Rechners exportiert. Für den Export werden zunächst Daten im Klartext erzeugt (und als Datei lokal geschrieben), die mittels KBV-Tool (Lösung der KV, nicht Zertifizierungsgegenstand)

dann geprüft und verschlüsselt. Diese verschlüsselte Datei wird dann vom Anwender verschickt. Die vom Produkt erzeugte Datei (mit Klartextdaten) muss anschließend gelöscht werden. Dieser Löschvorgang passiert automatisch mittels des sicheren Löschtools "SDelete" von Microsoft/Sysinternals, das mit dem Produkt mitgeliefert wird. Im Rahmen der KV-Abrechnung gibt es umfangreiche Protokolle sowohl innerhalb von RED Medical vor der Datenübergabe an das KBV-Prüfmodul, als auch anschließend nach der Prüfung durch das KBV-Prüfmodul. Eine lokale Speicherung der internen Protokolle findet nicht statt. Der Anwender muss diese ausdrucken, um dauerhaft Zugriff auf sie zu haben. Dies gilt auch für die Protokolle des KBV-Prüfmoduls, da diese nach der Verschlüsselung der Klartextdatei mit dem KBV-Kryptomodul gemeinsam mit den Klartextdaten mittels Sdelete sicher gelöscht werden. Der Hersteller empfiehlt den Ausdruck des Protokolls der Übermittlung der Daten durch das KBV-Tool.

Zur persönlichen Datensicherung aber auch, falls ein Anwender das System wechseln möchte, kann ein vollständiger Export aller im System gespeicherten Daten vorgenommen werden. Hierzu werden die entsprechenden Daten und Dateien im standardisierten BDT-Format gezippt und AES-verschlüsselt auf die lokale Festplatte des entsprechenden Rechners heruntergeladen. Der Anwender wird explizit auf den Speicherort hingewiesen und darauf, dass die Daten mit dem Ende des Exportvorganges in seine Verantwortung übergehen.

Für den Zertifizierungsgegenstand wird optional ein Statistik-Modul angeboten, das jedoch nicht Bestandteil der Zertifizierung ist.

Ebenfalls nicht zum Zertifizierungsgegenstand gehört die vollständige Einhaltung der ärztlichen Dokumentationspflichten durch das Produkt.

F. Tools, die zur Herstellung des Produktes verwendet wurden

Programmierwerkzeuge:

- Webstorm 4.0 - Editor
- Visual Studio 2010 - Editor
- JavaScript - Programmiersprache
- HTML5 - Programmiersprache

- Visual C++ - Programmiersprache

Infrastruktur

- Node.js -Applikationsserver 0.10.12
- Mongo DB - Datenbank 2.4.4
- Apache Solr -Datenbank für die Suche 4.3.1
- redis In-Memory-Datenbank Steuerungsdaten 2.6.14

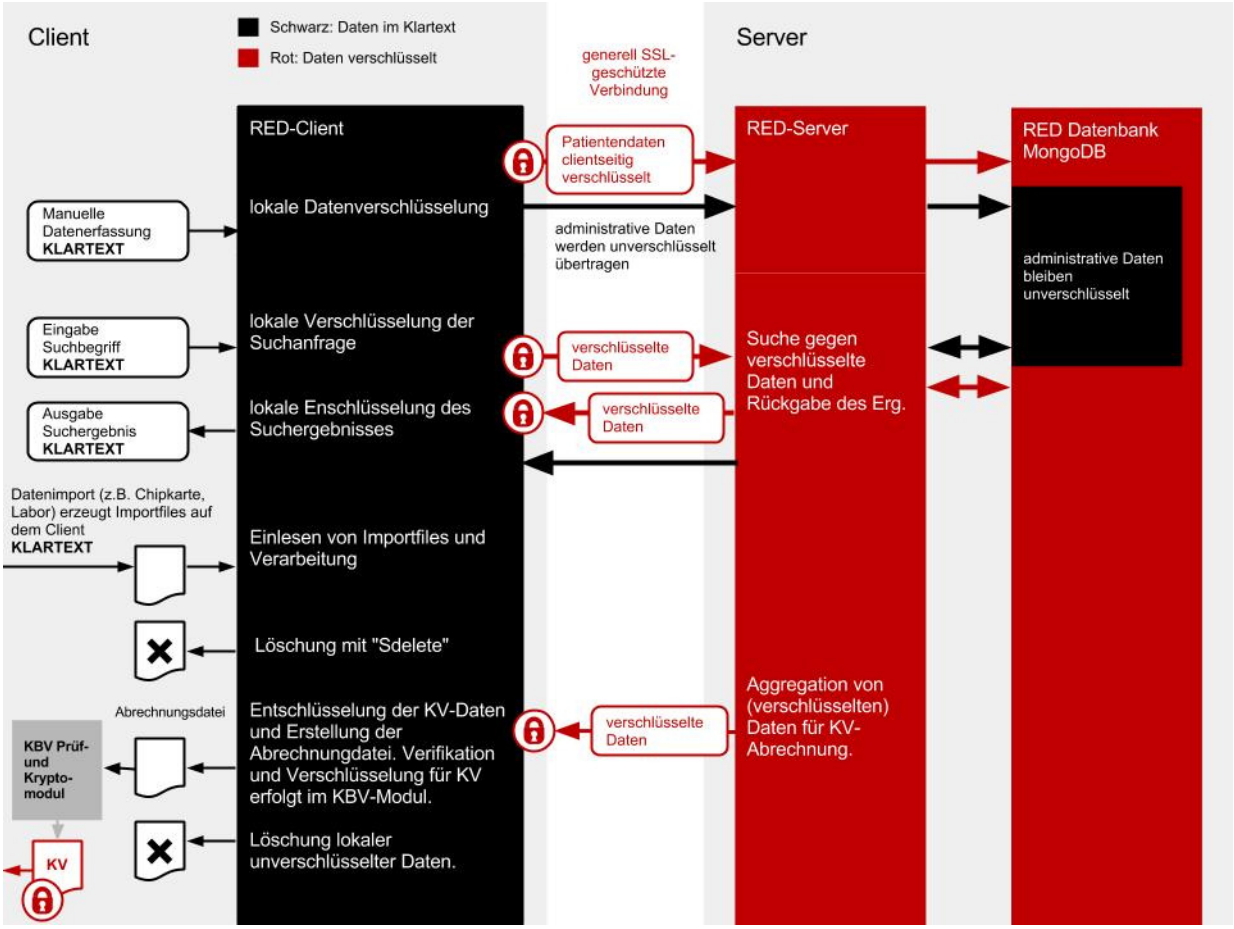
Hilfsprogramme:

- Sdelete.exe zum sicheren Löschen lokaler Files
- KBV Prüf- und Kryptomodul

G. Zweck und Einsatzbereich

Zweck des Verfahrens ist die Erhebung, Verarbeitung und Nutzung von medizinischen Patientendaten zur Unterstützung von Anamnese, Diagnose und Therapie, die von Ärzten durchgeführt wird. Es handelt sich um ein komplettes Arzt-Informations-System (AIS).
Das Produkt ist grundsätzlich auch für den Einsatz bei öffentlichen Stellen des Landes Schleswig-Holstein geeignet.

H. Modellierung des Datenflusses



I. Version des Anforderungskataloges

Dem Gutachten wird der Anforderungskatalog in der Version 1.2 zu Grunde gelegt.

J. Zusammenfassung der Prüfungsergebnisse

In datenschutzrechtlicher Hinsicht bestehen keine Bedenken gegen die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten von Patienten durch die Software.

Bei der Anlage neuer Patienten werden die Patientendaten in der Regel von der Versichertenkarte übernommen. Bei der Speicherung weiterer Daten zu einem Patienten, wie z. B. einer Telefonnummer oder einer E-Mail-Adresse, obliegt es dem Arzt, den Patienten darüber aufzuklären, dass diese Informationen freiwillig sind. Der Softwarehersteller kann dies nicht kontrollieren.

Ähnliches gilt für die Aufnahme von Diagnosen und/oder Leistungen. Leistungen und Diagnosen werden durch Auswählen aus den vorgegebenen Katalogen (ICD-10, EBM,

GOÄ) dokumentiert. Sollten Teile dieser Daten zu Abrechnungszwecken benötigt werden, so werden diese Daten gem. der Anforderung zur Abrechnung an die KV weitergegeben.
RED Medical steht dem einsetzenden Arzt zur Nutzung als Patientendokumentation zur Verfügung. Dabei kann der Arzt auch Texte in Freitextfeldern nutzen. In datenschutzrechtlicher Hinsicht ist dabei entscheidend, dass alle personenidentifizierenden Patientendaten (Stammdaten, Mitgliedsnummern, Diagnosen, Leistungsziffern, Medikamente, Laborwerte, alle Freitextfelder etc.) clientseitig schon beim Arzt verschlüsselt werden und dann zum Rechenzentrum übertragen werden.
Festzustellen ist, dass bei der Nutzung der Software die gesetzlichen Vorgaben des § 28 Abs. 7 BDSG und § 11 Abs. 3 i.V.m. § 11 Abs. 5 Satz 2 LDSG in Verbindung mit den standesrechtlichen Regelungen für medizinisches Behandlungspersonal und Ärzte eingehalten werden können. Dies beinhaltet auch die Einbindung des Produktherstellers als Auftragsdatenverarbeiter für die jeweils verantwortliche Stelle. Der Produkthersteller bietet mit der verantwortlichen Stelle einen Auftragsdatenverarbeitungsvertrag zum Abschluss an, der den Voraussetzungen des § 11 BDSG und des § 17 LDSG entspricht.
Da das System selbst keine Weitergabe von Daten an nachbehandelnde Ärzte oder die Bereitstellung von Dokumenten bzw. die Einräumung von Zugriffsrechten für Dritte vorsieht, waren diesbezüglich keine weiteren Prüfungen vorzunehmen.
Ein besonderes Augenmerk hat der Hersteller der Software auf den Punkt Verschlüsselung gelegt. Hintergrund hierfür ist einerseits der Schutz der Patientendaten im tatsächlichen Sinne; natürlich dient die Verschlüsselung von Patientendaten aber vor allem der Einhaltung rechtlicher Vorgaben, insbesondere des § 203 StGB, die eine Nutzung des Produktes durch Ärzte erst ermöglicht.
Folgende Daten werden bereits im Client des Nutzers (also in der Arztpraxis) verschlüsselt.

- Titel sowie Namenszusätze
- Name und Vorname
- Straße und Hausnummer, Postfach
- PLZ und Ort
- Geburts- und Sterbedatum
- Telefon, E-Mail-Adressen und alle andere Angaben zur Kommunikation
- Mitgliedsnummer der Krankenkasse
- Identifikationsnummer der Versichertenkarte

- Alle auf der Versicherungskarte gespeicherten Daten
- Alle patienten-identifizierenden / medizinischen Daten (Diagnosen, Leistungsziffern, Medikamente, Laborwerte o.ä.)

Darüber hinaus werden im System auch alle Freifeldtextfelder und Meta-Informationen automatisch verschlüsselt, da natürlich auch hier ggf. eine Angabe von unmittelbar personenbezogenen Daten, z. B. dem Namen des Patienten, erfolgen kann.
Der Hersteller trägt weiter Sorge dafür, dass z. B. weitere identifizierende Angaben, die z. B. im Rahmen von bestimmten Therapieprogrammen (z. B. bei Diabetes Typ I/II) vergeben werden (z. B. Teilnehmer-IDs von Krankenkassen) ebenfalls verschlüsselt werden.
Nicht verschlüsselt werden lediglich administrative Daten. Das sind beispielsweise Benutzerrechte, Kataloginhalte von z.B. Medikamentenlisten, Konfigurationseinstellungen o. ä. Eine unbefugte Offenbarung von Daten, die der ärztlichen Schweigepflicht i.S.d. § 203 StGB unterliegen, kann bei ordnungsgemäßer Nutzung des Systems ausgeschlossen werden. Im Ergebnis werden damit die Vorgaben des § 203 StGB eingehalten.

Im Hinblick auf die Technik setzt der Hersteller für die Datenhaltung die nicht-relationale Datenbank „MongoDB“ ein. Bezüglich der Sicherheit werden alle Möglichkeiten zur Absicherung angewendet:

- Anfragen nur auf den Datenbankserver beschränken, bzw. Rechner, die sich im angeschlossenen lokalen Netzwerk befinden.
- Nutzung des MongoDB internen Authentifizierungssystems. Standardmäßig ist bei der MongoDB die Authentifizierung abgeschaltet. Der Hersteller betreibt die DB jedoch mit Authentifizierung, auch wenn die Datenbank in einer gesicherten Umgebung eingesetzt wird.

Darüber hinaus hat der Hersteller ein umfangreiches Rollen- und Rechtekonzept umgesetzt.
Dieses sieht Benutzer und Benutzergruppen (als Zusammenfassung von mehreren Benutzern) vor, denen verschiedene Rechte zugeordnet werden können.
Diese sind wie folgt definiert:

1. Rechte auf Daten
   Diese Teilen sich auf in das Recht bestimmte Daten zu erzeugen („Create“), zu lesen („Read“), zu ändern („Update“) und zu löschen („Delete“) (CRUD). Die

Rechte können hierbei pro Datentyp (“model”) vergeben werden. Es ist also beispielsweise möglich, einem rein administrativ tätigen Nutzer den Zugriff auf medizinische Daten zu entziehen, oder Nutzern zwar das Lesen, nicht aber das Schreiben von Daten zu erlauben. Außer beim Lesen, Ändern und Löschen (RUD) werden die Rechte außerdem in Bezug auf die Nutzergruppe, die die Daten ursprünglich erzeugt hat, vergeben.

2. Clientseitige Rechte auf Funktionen
   Diese Rechte bestimmen, welche Funktionen die Mitglieder eine Nutzergruppe auf der Clientseite ausführen darf (z. B. Anlegen eines neuen Nutzers, Lesen der medizinischen Dokumentation oder Patientendaten, Durchführung der Patientenaufnahme oder -abrechnung).
3. Serverseitige Rechte auf Funktionen
   Diese Rechte bestimmen, welche Funktionen die Mitglieder eine Nutzergruppe auf dem Server aufrufen können. Diese Rechte können zwar auch alle clientseitig abgedeckt werden, in dem die entsprechenden Serverfunktionen nicht durch den Client aufgerufen werden können, zur Wahrung der Datenintegrität und –konsistenz ist es aber sinnvoll, diese Rechte auf der Serverseite noch einmal zu überprüfen.

Bei einer webbasierten Lösung, wie im Falle von RED ist es ein besonderes Augenmerk auf die Verfügbarkeit zu legen. Diese wird vom Hersteller durch einen hohen technischen Aufwand sichergestellt. Darüber hinaus hat die verantwortliche Stelle die Möglichkeit, die Verfügbarkeit ihrer Daten zu erhöhen, indem eine lokale Kopie der Daten angefertigt werden kann. Eine entsprechende Funktion ist für den Administrator der verantwortlichen Stelle einfach aufrufbar und gut dokumentiert. Die Daten werden dabei im BDT-Format gezippt und AES-verschlüsselt auf der lokalen Festplatte gespeichert. Eine Entschlüsselung der Datei ist möglich, damit diese dann z. B. wieder ins RED Medical oder aber ein anderes Drittsystem importiert werden kann.
Der Hersteller empfiehlt den regelmäßigen Download der Daten, um die Verfügbarkeit noch weiter zu optimieren, um so eine bestmögliche Therapiesicherheit für die Patienten zu gewährleisten.

Anforderung nach Katalog oder sonstigen Rechtsnormen	Bewertung	Kommentare
Allgemeines Anforderungsprofil		
Komplex 1:		
1.1 Datensparsamkeit	adäquat	Es werden lediglich Daten erhoben, die zur Behandlung und Abrechnung von Patienten benötigt werden
1.2 Frühzeitiges Löschen, Anonymisieren oder Pseudonymisieren, wenn Daten noch erforderlich, aber Personenbezug verzichtbar	vorbildlich	Statt einer Anonymisierung oder Pseudonymisierung wird direkt nach der Eingabe und noch vor der Speicherung eine Verschlüsselung der Daten vorgenommen, so dass es nur der Daten verarbeitenden Stelle möglich ist, die Daten mit Personenbezug zu lesen, nicht aber Dritten, wie dem Hersteller oder seinen Dienstleistern.
1.3 Transparenz und Produktbeschreibung	adäquat	
1.4 Sonstige Anforderungen <benennen!>	entfällt	
Komplex 2:		
2.1. Ermächtigungsgrundlage		
2.1.1 Gesetzliche Ermächtigung	vorbildlich	s. o.
2.1.2 Einwilligung des Betroffenen	adäquat	Eine gesonderte Einwilligung des Betroffenen in die Speicherung in einem externen Rechenzentrum ist wegen der verwendeten Verschlüsselungsverfahren nicht erforderlich. ,
2.1.3 Besonderheiten in den einzelnen Phasen der Datenverarbeitung		
2.1.3.1 Vorschriften über die Datenerhebung		
2.1.3.2 Vorschriften über die Über-		

mittlung		
2.1.3.3 Löschung nach Wegfall der Erfordernis		
2.2 Einhaltung allgemeiner datenschutzrechtlicher Grundsätze und Pflichten		
2.2.1 Zweckbindung	vorbildlich	
2.2.2 Erleichterung der Umsetzung des Trennungsgebots	entfällt	
2.2.3 Gewährleistung der Datensicherheit	s. Komplex 3	
2.3 Datenverarbeitung im Auftrag	adäquat	Die gesetzlichen Anforderungen an eine Datenverarbeitung sind sowohl im Verhältnis zwischen dem Anbieter und dem Rechenzentrumsbetreiber sowie im Verhältnis zwischen RED Medical und dem Nutzer (Arzt) in hinreichender Weise geregelt. Die Anforderungen des § 11 BDSG, insbesondere des § 11 Abs. 2 BDSG werden erfüllt.
2.4 Voraussetzungen besonderer technischer Verfahren		
2.4.1 Gemeinsames Verfahren oder Abrufverfahren	entfällt	
2.4.2 Weitere besondere technische Verfahren	entfällt	
2.5 Sonstige Anforderungen <benennen!>	entfällt	
Komplex 3:		
3.1.1.1 Maßnahmen, um Unbefugten den Zugang zu Datenträgern zu verwehren	adäquat	Ein ordnungsgemäßer ADV ist vorhanden. Der Hersteller unterstützt die Daten verarbeitende Stelle durch Informationen und der praktischen Umsetzung in und mit dem Produkt.
3.1.1.2 Maßnahmen, um zu verhindern, dass Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen kön-	vorbildlich	Es ist eine Mehr-Faktor-Authentisierung implementiert worden.

nen		
3.1.1.3 Protokollierung von Datenverarbeitungsvorgängen	vorbildlich	Das Produkt erfüllt die Anforderung einer vollständigen Protokollierung der Datenverarbeitungsvorgänge gem. § 6 Abs. 4 LDSG-SH.
3.1.1.4 Weitere technische und organisatorische Maßnahmen	vorbildlich	Verschlüsselungsmethoden (s. unten)
3.1.2 Erleichterung der Vorabkontrolle	adäquat	Unterstützung durch Dokumentation
3.1.3 Erleichterung bei der Erstellung des Verfahrensverzeichnisses	vorbildlich	Der Hersteller hat Verfahrensbeschreibungen erstellt.
3.1.4 Sonstige Unterstützung der Tätigkeit des behördlichen Datenschutzbeauftragten	adäquat	Eine gesonderte Unterstützung ist durch das Produkt insofern gegeben, als das der Hersteller ein eigenes Testumfeld bereitstellt und sein Datenbankmodell mit Feldbeschreibungen transparent darstellt.
3.2.1 § 6 LDSG, z.B. Verschlüsselung bei tragbaren Computern	vorbildlich	Verschlüsselung erfolgt im Client (Browser)
3.2.2 Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens	entfällt	
3.2.3 Technische Umsetzung von Transparenz- und Beteiligungsgeboten für die Betroffenen bei besonderem Technikeinsatz	entfällt	
3.3 Pflichten nach Datenschutzverordnung (DSVO), insbesondere für Verfahren	adäquat	Einhaltung der Vorgaben der DSVO obliegt der jeweils Daten verarbeitenden Stelle. Die erforderlichen Tests und die Freigabe der Verfahren sind mit dem Produkt "RED Medical" ohne Einschränkungen möglich.
3.4 Sonstige Anforderungen <benennen!>	entfällt	
Komplex 4:		
4.1 Aufklärung und Benachrichtigung	adäquat	Ist jederzeit durch die verantwortliche Stelle möglich.
4.2 Auskunft	adäquat	Ist jederzeit durch die verant-

		wortliche Stelle möglich.
4.3.1 Berichtigung,	adäquat	Ist jederzeit durch die verant-wortliche Stelle möglich.
4.3.2 Vollständige Löschung	adäquat	Kann durch die verantwortliche Stelle angestoßen werden. Die endgültige Löschung ist erfolgt, wenn die Datenbank ordnungs-gemäß repliziert sind.
4.3.3 Sperrung	adäquat	Eine Sperrung kann über das Rechtesystem realisiert werden.
4.3.4 Einwand bzw. Widerspruch ge-gen die Verarbeitung	adäquat	
4.3.5 Gegendarstellung	adäquat	
4.4 Sonstige Anforderungen <benen-nen!>	entfällt	

K. Beschreibung, wie das Produkt den Datenschutz fördert

Statt einer Anonymisierung oder Pseudonymisierung wird direkt nach der Eingabe und noch vor der Speicherung eine Verschlüsselung der Daten vorgenommen, so dass es nur der Daten verarbeitenden Stelle möglich ist, 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 auch alle anderen Daten, die der ärztlichen Schweigepflicht i.S.d. § 203 StGB unterliegen, verschlüsselt.

Insgesamt gibt es keine unverschlüsselten Felder, die Patienten identifizierende Daten enthalten können.

Schlüsselstärken und Absicherungen gegen Brute-Force-Attacken im Browser werden positiv bewertet. Die eingesetzten Verschlüsselungsmechanismen und Algorithmen entsprechen dem Stand der Technik.

So ist das SSL-Zertifikat mit einem 256-Bit-Schlüssel ausgestattet. Zudem werden lokal folgende Algorithmen zur Verschlüsselung verwendet:

- PBKDF2 mit 64-Bit-langem Zufalls-Salt
- AES256, sowie
- SHA-3 mit 512 Bit

In Punkto Transparenz geht der Hersteller über das normale Maß hinaus und liefert seinen clientseitigen Programmcode in lesbarer Form mit aus. Um Veränderungen an diesem Code verfolgen und ggf. abzulehnen zu können und um dem Anwender eine Kontrolle über die zur Verschlüsselung eingesetzten Software zu ermöglichen, hat der Hersteller eine Browsererweiterung implementiert, die auf einem Mozilla Firefox-Browser installiert wird und diese Aufgabe erledigt. Alle Änderungen werden vom Hersteller protokolliert und für die Benutzer transparent dargestellt. Darüber hinaus hat der Hersteller in seiner Dokumentation beschrieben, wie der Anwender auch ohne die Erweiterung die Verschlüsselungsmodule selbst auf Manipulationsfreiheit hin überprüfen kann.

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

Kellinghusen, den 11.07.2013

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

Flensburg, den 11.07.2013

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