Kurzgutachten für das

Datenschutz-Gütesiegel (ULD)

für MedicalPad 7

bestehend aus den Modulen:

MedicalPad Mobile
MedicalPad Server

Im Auftrag der:
Tech2go
Mobile Systems GmbH
Jarrestraße 44
22303 Hamburg

Auditor: Tim-Oliver Ritz
Senior Consultant Datenschutz und IT-Compliance,

Telefon: 040 / 790 235 – 232
E-Mail: tritz@intersoft-consulting.de

Inhalt

Zusammenfassung

Mit diesem Gutachten werden die Ergebnisse der datenschutzrechtlichen und IT-sicherheitstechnischen Prüfung der Anwendung MedicalPad, bestehend aus den Modulen MedicalPad Mobile und MedicalPad Server in der Version 7.0 dokumentiert, mit der die intersoft consulting services AG seitens der Tech2go GmbH beauftragt wurde. Das Abrechnungsmodul und die verwendete Hardwaresind kein Teil des Zertifizierungsgegenstandes, gleichwohl kann die Anwendung auch ohne Abrechnungsmodul betrieben werden. Die Schnittstellen sind lediglich textbasiert und unidirektional, d.h. ein möglicher Datenexport zum Server kann nur über das MedicalPad Mobile erfolgen. Es existiert dabei kein Verzeichnis nach außen, jedwede Datenübertragung erfolgt nur im gesicherten und internen VPN-Netzwerk.

Die Anwendung MedicalPad ist eine elektronische Patientendatenerfassungs- und Protokollsoftware zur Einsatzdokumentation und Protokollierung von Rettungsdiensteinsätzen. Sie ist derzeit ausschließlich bei öffentlichen Stellen (Rettungsdienste der jeweiligen Landkreise, Städte und Kommunen) im Einsatz.

Hersteller und Entwickler ist die in Hamburg ansässige Tech2go GmbH, welche die Anwendung selbst erstellt hat und fortlaufend entwickelt. Die Tech2go GmbH ist spezialisiert auf die Entwicklung mobiler Systemlösungen. Die Anwendung MedicalPad sowie Recherche und Statistikauswertungen (MedicalPad Desktop).

Die Prüfung wurde anhand des Standards des Datenschutz-Gütesiegels gemäß der Schleswig-Holsteinischen Landesverordnung über ein Datenschutgütesiegel (DSGSVO)[1] durchgeführt. Grundlage für die Erstellung dieses Gutachtens gemäß DSGSVO ist die Version 1.2 des Anforderungskatalogs für ein Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz in Schleswig-Holstein (ULD)[2].

Im Ergebnis stellt der Auditor fest, dass das MedicalPad unter Beachtung der dem Anwender zur Verfügung gestellten Datenschutzhinweise konform zu den gesetzlichen Anforderungen an den Datenschutz und der IT-Sicherheit ist und in besonderem Maße den Datenschutz fördert.

[1] Landesverordnung über ein Datenschutzgütesiegel (Datenschutzauditverordnung - DSGSVO) vom 30. November 2013 Fundstelle: GVOBl. 2013, 536

[2] Prüfschema des Gutachtens für die Produktzertifizierung V1.1, 2005-11-01.

A Allgemeiner Teil

1 Zeitraum der Prüfung

Die Auditierung von MedicalPad erstreckte sich auf den Zeitraum vom 12. März bis 03. November 2015 und beinhaltete eine strukturierte Datenschutzanalyse auf der Basis von Interviews, der Durchführung von Tests, der Sichtung von Dokumentationen sowie Besichtigungen vor Ort.

2 Antragstellerin

Antragstellerin der Auditierung und Zertifizierung gemäß DSGSVO ist die

Tech2go Mobile Systems GmbH
Jarrestraße 44
22303 Hamburg

als Hersteller des IT-Produkts MedicalPad und als IT-Dienstleister.

3 Sachverständige Prüfstelle

Sachverständige Prüfstelle gemäß DSGSVO ist die

intersoft consulting services AG
Frankenstraße 18a
20097 Hamburg
Tel.: 040 790 235 – 0
E-Mail: info@intersoft-consulting.de
Web: www.intersoft-consulting.de

unter der Leitung von Herrn Matthias Lindner (Recht/Technik).

4 Kurzbezeichnung des IT-Produktes / IT-Services

Auditiert wurde das Produkt MedicalPad, bestehend aus den Modulen MedicalPad Mobile und MedicalPad Server in der Version 7.0 sowie der entsprechende IT-basierende Service.

5 Detaillierte Beschreibung des IT-Produkts / IT-Services

5.1 Zweck

Das MedicalPad ermöglicht die elektronische Einsatzdokumentation nebst Protokollierungen von Rettungsdiensteinsätzen. Kernelemente des Systems sind dabei die mobilen Datenerfassungsgeräte, welche Stammdaten, Messwerte und Maßnahmen mittels Kommunikationsdienst auf den Server der Einsatzleitstelle abgleicht und von dort auch Informationen (Updates, Einstellungen) erhalten kann. Mit Hilfe des MedicalPad können Rettungskräfte im Einsatz Patientendaten nach dem DiVi-Protokoll elektronisch aufnehmen und diese Daten ggf. später auf der Rettungswache nachbearbeiten. Die Erhebung der Daten erfolgt durch den Notarzt, Rettungssanitär, Rettungsassistenten, bzw. Notfallsanitäter und nach standardisierten Vorgaben.

5.2 Einsatzbereich

Das IT-Produkt ist für den Einsatz bei Rettungsdiensten konzipiert und ist daher für den Einsatz bei öffentlichen Stellen des Landes Schleswig-Holstein geeignet.

6 Modellierung des Datenflusses

Mit MedicalPad werden sowohl Primär- als auch Sekundärdaten erhoben und verarbeitet. Die Datenfelder werden entsprechend des Divi Standards ggf. erweitert. Im Rahmen der Zweckbindung können auch die notwendigen zusätzlichen Daten erhoben werden. Des Weiteren dient die Datenerhebung auch der Erfüllung des mint 3 Baden-Württemberg.

6.1 Primärdaten

Nr.	Datenart	Personengruppe	Datenfelder
1	Stammdaten	Patient	Vorname Nachname Anschrift Ggf. zusätzliche Informationen bei einem Arbeitsunfall (Beruf, Arbeitgeber, BG, Anschrift) Status Geburtsdatum Geschlecht
2	Patientendaten	Patient	Daten nach dem DiVi-Standard (Daten des Patienten sowie Erstbefund, Diagnosen, eingeleitete Maßnahmen und Übergabewerte)
3	Krankenversicherungsdaten	Patient	Kostenträger, Krankenkassen-Nr.,

			Versicherten-Nr., Status, Gültigkeit der Karte.

6.2 Sekundärdaten

Nr.	Datenart	Personengruppe	Datenfelder
1	Einsatzdaten	Rettungswagen-besatzung	- Name, Vorname und Qualifikation der Rettungswagenbesatzung Einsatznummer, Einsatzzeiten, Kilometerstände, Einsatzor- - Einsatznummer - Einsatzzeiten (z. B. Alarmzeit, Ausrückzeit, Ankunftszeit) - Ausrückort z. B. Wache - Kilometerstände - Einsatzort o Einsatzort – Typ: z. B. Krankenhaus, Altenheim o Straße, Hausnummer, PLZ, Ort, ggf. Zusatz - Patientendaten o Nachname, Vorname, Geschlecht, Geburtstdatum, Alter o Straße, Hausnummer, PLZ, Ort - Kostenträger, Krankenkasse-Nr., Versicherten-Nr., Status, Gültigkeit KK. o Zusätzliche Informationen bei Arbeitsunfall (Beruf, Arbeitgeber, BG, Anschrift), Abweichendem Rechnungsempfänger (Name, Anschrift, Kontaktdaten) oder Internationalem Patienten - Beschreibung Notfallsituation - Erstbefund - Neurologie - Erstbefund - Messwerte - Erstbefund - EKG - Erstbefund - Atmung - Erstbefund - Psychischer Zustand - Erstbefund - APGAR-Schema - Diagnose - Diagnose - Verletzungen - Diagnose - Verbrennungen/Verbrühungen - Verlauf - Messwerte - Maßnahmen - Übergabe - Zustand

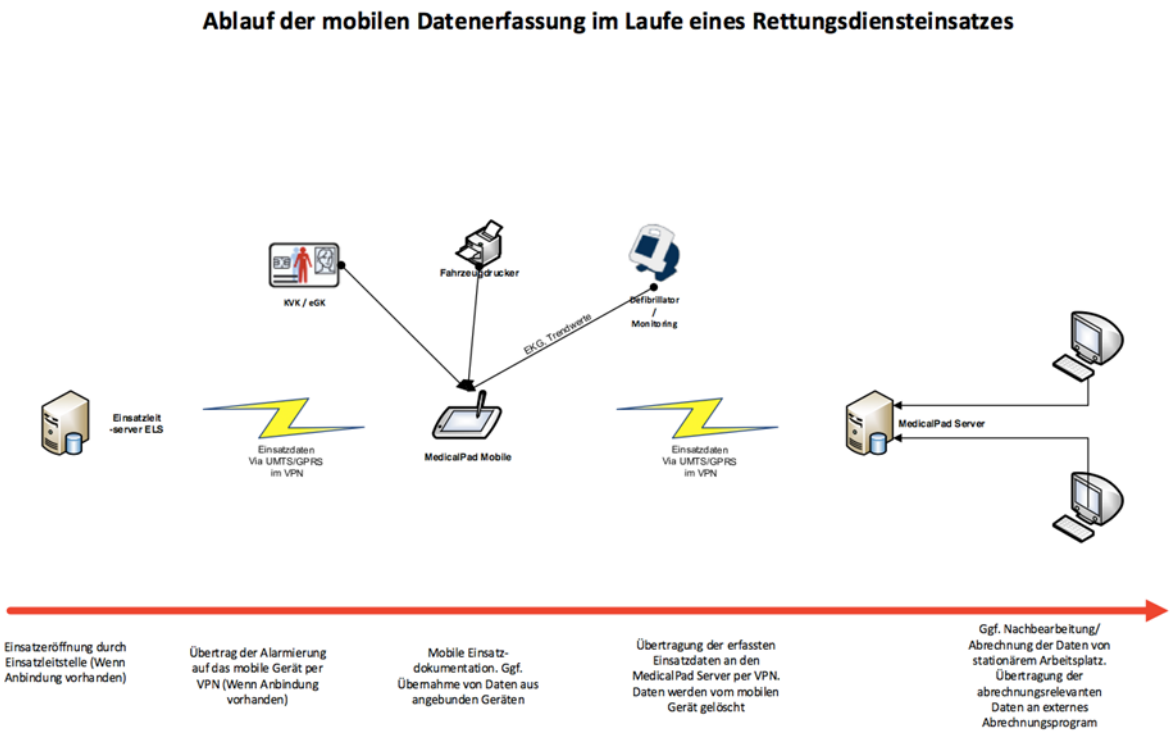
			- Übergabe - Messwerte - Übergabe - EKG - Übergabe - Atmung - Einsatzbeschreibung (z. B. Polizei anwesend, Desinfektion) - Einsatzbehinderung (z. B. Glätte, Nebel) - Ersthelfermaßnahmen - NACA-Score - Einsatzverstärkung - Wertsachen inkl. „Übergabe an" - Bemerkungen - Transportziel o Transportziel – Typ: z. B. Krankenhaus, Altenheim o Straße, Hausnummer, PLZ, Ort, ggf. Zusatz - Transportgrund -
2	Protokolldaten	Administration	Fehlerlogs

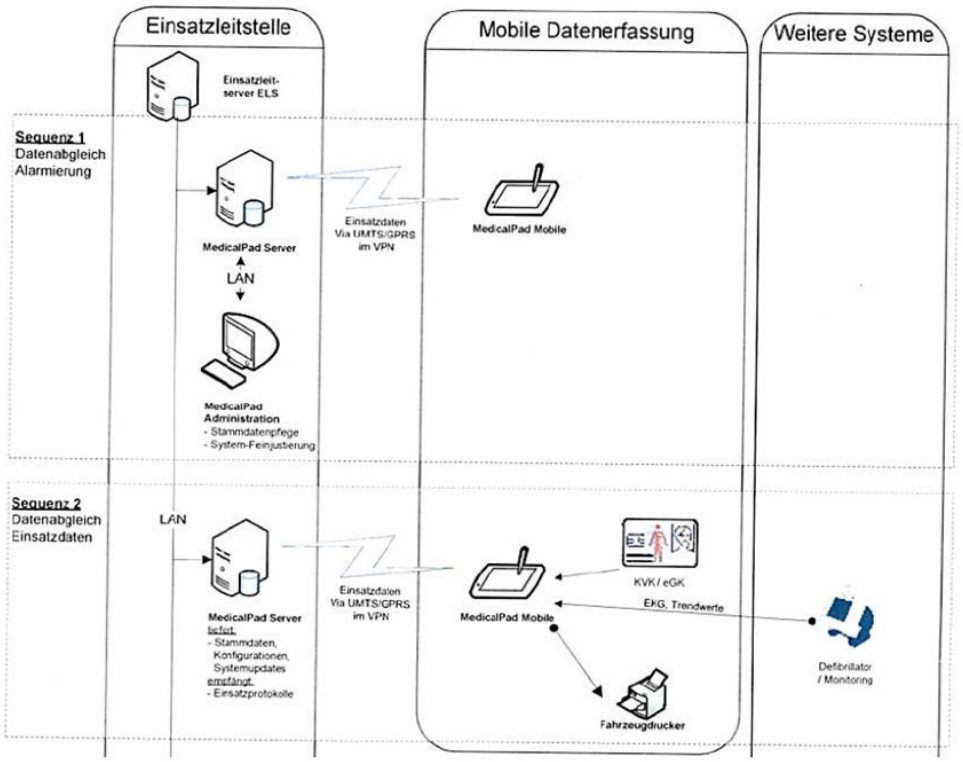
Wegen der Fülle der erhobenen Daten wird auch auf die Anlage der Feldliste verwiesen.

Die Speicherung der Logdateien ist konfigurierbar und beträgt max. 6 Monate. Die grundsätzliche Empfehlung ist die Logdaten für die Dauer eines Monats zu speichern. Ein Zugriff erfolgt nur im Fehlerfall oder bei der Inbetriebnahme des Systems ohne Echtdaten und im Echtbetrieb nur nach Bedarf. Die verantwortliche Stelle wird bei der Implementierung auf die Voraussetzungen nach § 6 Abs. 4 LDSG hingewiesen, insbesondere dass die Änderungsprotokollierung entsprechend der Einsatzdaten zu speichern ist, während die Fehlerlogs, welche keine personenbezogenen Daten enthalten, nach der technischen Behebung des Fehlers zu löschen sind.

6.3 Datenfluss

Der Datenfluss des MedicalPad Mobile in Verbindung mit dem MedicalPad Server lässt sich wie folgt darstellen:





7 Eingesetzte Tools

MedicalPad Mobile Handheld
Windows 7 Professional
Datenbank SQL Compact 4
Integriertes UMTS Modem und SIM-Karte des Providers.

MedicalPad Server
Windows Server 2008 R2, 2012
Microsoft SQL Server
C# und .Net

8 Anforderungskatalog

Version des der Prüfung zugrunde gelegten Anforderungskatalogs: 1.2[3].

9 Zusammenfassung der Prüfergebnisse

9.1 Umsetzung von rechtlichen Anforderungen

Die rechtlichen Anforderungen in Bezug auf die Zulässigkeit der Datenverarbeitung werden eingehalten. Dies bezieht sich insbesondere auf die Einhaltung der Vorschriften nach dem Zehnten Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz - (SGB X) und dem Schleswig-Holsteinischen Gesetz zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz - LDSG -).

Die Anforderungen an eine wirksame (gesetzliche) Einwilligung im Rahmen der Speicherung der personenbezogenen Daten von Patienten werden eingehalten.

9.2 Datensparsamkeit

In allen Modulen obliegt es dem Rettungssanitäter oder Notfallmediziner, nur die für die Zweckerfüllung erforderlichen Daten zu erheben. Das Programm hält sich dabei an den DiVi-Standard und den entsprechenden Feldern der bedienten Schnittstellen (z. B. EKG). Nicht mehr benötigte Daten können nach Ablauf der gesetzlichen Aufbewahrungsfristen gelöscht werden. Ein Löschungskonzept wird individuell mit dem Kunden nach den Anforderungen des Rechtsträgers umgesetzt. Es besteht ein detailliertes und wirksames Berechtigungskonzept.

Die gesetzliche Aufbewahrungsfrist beträgt 10 Jahre. Nur und ausschließlich der verantwortlichen Stelle ist eine Löschung der vorhandenen Daten möglich. Dies kann durch einen Berechtigten durch einen „Lauf über alle Akten älter als X Jahre" erfolgen. Grundsätzlich wird so verfahren, wobei die Daten nicht vollständig gelöscht, sondern anonymisiert im System verbleiben. Die Implementierung einer

[3] Anforderungskatalog v 1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH mit Stand 29.08.2005.

automatischen Löschroutine durch den Hersteller würde zu einer nicht tragbaren Haftungserweiterung führen.

Gleichwohl wird bei der Implementierung die verantwortliche Stelle sowie der behördlich Datenschutzbeauftragte auf die Einhaltung der Löschfristen hingewiesen sowie auch auf die Möglichkeit eine automatisierte Löschung nach Ablauf der entsprechenden Fristen durch Konfiguration der Datenbank vorzunehmen.

Eine automatisierte Löschroutine wird nicht in der Standardkonfiguration ausgeliefert, sondern nur nach Rücksprache mit dem Kunden bei der Implementierung des Systems konfiguriert, oder dieser auf die nach Ablauf der Löschfristen vorzunehmende manuelle Löschung hingewiesen.

Der Gutachter hat sich davon überzeugt, dass im Falle der Löschung von personenbezogenen und personenbeziehbaren Daten keine Auswertungen oder sonstigen Verwendungen mit diesen Daten mehr möglich ist. Ein Zusammenführen von weiteren freien Daten ist dabei nicht möglich, da systemseitig nur auf die vorhandenen nicht personenbezogenen oder personenbeziehbaren Daten zugegriffen werden kann. Lediglich die vorgebenen nicht personenbezogenen oder personenbeziehbaren Daten werden systemseitig, nicht frei konfigurierbar, für festgelegte Auswertungen herangezogen.

9.3 Datensicherheit

Der Hersteller hat durch technische Maßnahmen dafür Sorge getragen, dass nur die berechtigten Personen Zugriff auf das System haben. Nur mit entsprechender Zugriffsberechtigung kann auf das System zugegriffen werden. Die Daten auf den mobilen Geräten sind nach dem Stand der Technik verschlüsselt (AES-256 Bit) und werden mittels eines gesicherten VPN-Tunnels an den Server übertragen. Zudem besteht die Möglichkeit einer vollständigen Systemverschlüsselung mittels der Betriebssystemverschlüsselung Bitlocker, oder der Open Source Software Truecrypt. Das verwendete Passwort muss mindestens 8 Zeichen, mit Groß- und Kleinbuchstaben und Sonderzeichen enthalten.

Der Server ist in der Regel der bereits vorhandene Server der Einsatzzentrale. Nach dem erfolgreichen Übertragungsvorgang auf den Server werden die Daten von dem mobilen Erfassungsgerät gelöscht. Der Übertragungsvorgang kann manuell oder automatisiert gestartet werden. Der Server der Einsatzleitstelle unterliegt besonderen Sicherheitsanforderungen und Schutzmechanismen (integrierte Leitstelle der Feuerwehr, Datensicherheit nach § 9 BDSG bzw. Landesregelungen und ggf. den Empfehlungen des Herstellers). Die Datenbank wird regelmäßig im Rahmen der Serversicherung mitgesichert. Auf Wunsch des Kunden ist zudem eine Individualsicherung der Datenbank unabhängig von dem Server möglich („Dumpsicherung" als vollständiges Abbild der Datenbank).

Das System läuft auf und mit Standardtechnologien. Nicht notwendige Dienste sind über das Betriebssystem deaktiviert. Ein Booten von einem USB-Stick ist nicht möglich. Die Daten der Anwendung liegen verschlüsselt in der eigenen Datenbank vor und lassen sich nur nach dem Start der Anwendung für den jeweils

berechtigten Nutzer auslesen. Zuvor muss sich dieser an der Anmeldemaske des Betriebssystems autorisieren. Nicht notwendige Zusatzsoftware, andere externe Programme sind nicht vorhanden. In Ermangelung von lokalen Administrationsrechten kann der Anwender auch keine weiteren, eigenen Programme installieren, oder Teile des Systems deinstallieren. Insbesondere hat der Anwender keine Berechtigung, Sicherheitsfunktionen abzuschalten, um sich etwa eine automatische Login Funktion auf Betriebssystemebene zu verschaffen. Des Weiteren ist kein Screenshot des Bildschirms möglich, ebenso wie auch kein Drucker installiert ist, sodass die Daten aus der Anwendung auch nicht auf diesem Wege auf unberechtigten Wegen das MedicalPad verlassen könnten.

Durchgeführte Tests und Evaluierung sowie jeweils durchgeführte Prüfungen vor Auslieferung der Geräte (Ergebnisse in Klammern):

- Booten durch USB-Stick/anderes Laufwerk (nicht möglich)
- Überprüfung von Sperrung der Schnittstellen (WLAN/Bluetooth/USB etc.) (Schnittstellen sind gesperrt)
- Prüfung der Zugriffsmöglichkeiten auf das Betriebssystem (nicht möglich ohne Benutzerauthorisation)
- Prüfung der automatischen Sperrung des Gerätes im Betrieb (Sperrung erfolgt)

Der Gutachter hat die Funktionsweise, die Einstellungen und Sicherheitsfunktionen eingehend sowohl persönlich überprüft, als auch Vorführen lassen. Dies geschah beim Antragsteller vor Ort und ebenfalls durch das Sichten der vorhandenen Dokumente, insbesondere solcher zu technischen Beschreibungen und den Inhalten von etwaigen Logdateien, Einstellungen und Konzepten, wie etwa den Datenschutzhinweisen und dem Berechtigungskonzept. Dabei wurde auch die Standardauslieferung überprüft.

9.4 Beachtung der Betroffenenrechte

Die Anforderungen hinsichtlich der Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung werden eingehalten. Für eine Auskunft gibt es sowohl ein Formular als auch einen Prozess zur Erteilung eben dieser[4]. Eine Löschung von Daten unabhängig von einer Berichtigung der Daten ist nur eingeschränkt dem Systemadministrator per SQL Befehl möglich, da die Daten in jedem Fall entsprechend der gesetzlichen Aufbewahrungsfristen aufzubewahren sind. In der Historie abgelegte Daten können nicht verändert werden.
Daten, die der Aufbewahrungspflicht unterliegen, können dergestalt gesperrt werden, als dass die Nachbearbeitungsmöglichkeit durch Protokollierung vollständig nachvollzogen werden kann.

Einzelne Datensätze können als gesperrt markiert werden und nur der Datenschutzbeauftragte kann diese Sperrung setzen oder auch wieder entfernen.

[4] vgl. auch § 10 Abs. 2 der Musterberufsordnung der in Deutschland tätigen Ärztinnen und Ärzte, Wahrung der Patientenrechte auf Auskunft durch das Recht auf Einsicht in seine Patientenakte.

Für Benutzer ist im Falle der Sperrung die entsprechende Bildschirmmaske zur Eingabe von Änderungen nicht mehr sicht- oder aufrufbar. Die Daten werden damit nicht mehr angezeigt.

10 Förderung des Datenschutzes

Das MedicalPad dient unmittelbar der Förderung des Datenschutzes. Durch die elektronische Patientendatenerfassung wird vermieden, dass am Ende von verschiedenen Einsatzfahrten diverse handausgefüllte Formulare zwischen Rettungswagen und Einsatzzentrale und schließlich weiter zum Krankenhaus und ggf. behandelndem Arzt und Versicherungsträger versandt und getragen werden müssen. Im Umfeld eines Noteinsatzes ist dabei die Gefahr des Verlusts regelmäßig hoch gewesen, da die Papierformulare in der Eile zunächst im Rettungswagen und sodann letztlich in einem Postkorb im Krankenhaus abgelegt wurden, während auf dem mobilen Endgerät in der elektronischen Version nur der jeweils aktuelle Einsatz zur Bearbeitung geöffnet ist und die vorangegangen bereits an das Krankenhaus übermittelt wurden. Zudem konnten sich unbefugte leicht einen Zugang zu den Dokumenten verschaffen. Der gesamte Arbeitsprozess der Datenverarbeitung ist durch eine elektronische Variante beschleunigt, ebenso die Vorgänge der Weiterverarbeitung. Bei der Übertragung von den Papierformularen in die jeweiligen elektronischen Systeme (Leitstelle, Krankenhaus) kann es mit Einsatz der Software nicht mehr zu Übertragungsfehlern kommen. Funktionen des Qualitätsmanagements und Statistiken helfen zudem bei der effizienteren zukünftigen Planung von Ressourcen für Einsatzfahrten und der Auswertung der Rettungswageneinsätze an sich, da es bislang und auf Basis der Papierformulare keine statistischen Auswertungsmöglichkeiten gab.

Dem Nutzer wird eine angemessene Produktbeschreibung zur Verfügung gestellt, welche für den Nutzer auch verständlich geschrieben ist. Zudem führt ein Handbuch durch die notwendigen Schritte der Dateneingabe und allgemeinen Bedienung.

Des Weiteren steht dem Nutzer ein Kundensupport mittels Hotline und ggf. Technikereinsatz vor Ort zur Verfügung.

11 Votum

Hiermit bestätige ich, dass das Produkt MedicalPad und der dazugehörende IT-Service mit Stand November 2015 den Rechtsvorschriften über den Datenschutz und der Datensicherheit entsprechen.

Hamburg, den 03.11.2015

Mathias Lindner
Managing Consultant Datenschutz und IT-Compliance
Rechtsanwalt, Wirtschaftsinformatiker
Leiter der beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannten Sachverständigen Prüfstelle für IT-Produkte (Recht/Technik)