Kurzgutachten zur Erteilung eines Datenschutzgütesiegels für das IT-Produkt „HealthDataSpace, Version 2“

im Auftrag der Telepaxx Medical Archiving GmbH

datenschutz cert GmbH

22. September 2015

Inhaltsverzeichnis

1. Vorbemerkung

Mit diesem Kurzgutachten werden die Ergebnisse der Auditierung des IT-Produkts „HealthDataSpace, Version 2“ zusammengefasst, welches seitens des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein erfolgreich gemäß der Datenschutzgütesiegelverordnung (DSGSVO)[1] zertifiziert wurde.

2. Zeitraum der Prüfung und Prüfungsart

Die Auditierung erstreckte sich auf den Zeitraum von 01.02.2014 bis 22.09.2015 und beinhaltete eine konzeptionelle Analyse der zur Verfügung gestellten Unterlagen sowie Besichtigungen des Testsystems. Ferner ist der Authentifikationsvorgang praktisch getestet worden.

Hervorzuheben ist, dass im Rahmen dieses Audits nicht untersucht wird, ob der HealthDataSpace konform zum Medizinproduktegesetz aufgestellt ist.

3. Antragstellerin

Antragstellerin ist die

Telepaxx Medical Archiving GmbH
Wasserrunzel 5,
91186 Büchenbach, Deutschland

als Mitbetreiberin des HealthDataSpace. Ansprechpartner ist Herr Andreas Dobler, Geschäftsführer der Telepaxx Medical Archiving GmbH.

4. Sachverständige/Prüfstelle

Sachverständige dieser Auditierung ist die Prüfstelle

datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen

unter der Leitung von Frau Dr. Irene Karper (Recht) und Herrn Dr. Sönke Maseberg (Technik). Ansprechpartner für diese Auditierung sind Frau Dr. Irene Karper (Recht) und Herr Ralf von Rahden (Technik).

5. Kurzbezeichnung des IT-Produkts

Auditiert wird das IT-Produkt „HealthDataSpace“ in der Version 2 mit den zwei Anwendermöglichkeiten als

--- HealthDataSpace – HDS – genutzt von Privatpersonen (auch sogenannte Basisversion) und

--- Health DataSpace Professional – HDS PRO - genutzt von Ärzten.

HDS steht in der Basisversion nur Privatpersonen (Patienten) zur Verfügung und besitzt wiederum zwei Ausprägungen:

[1] Landesverordnung über ein Datenschutzgütesiegel (Datenschutzgütesiegelverordnung – DSGSVO) v. 30.11.2013, GVOBl. Schl.-H. 2013, S.536ff.

--- Die erste Ausprägung ist eine kostenlose Nutzungsfunktion des HDS. Hierbei ist der Speicherplatz auf 1 GB begrenzt. Zudem werden alle Bilddaten nur 3 Monate nach Ablage im HDS gespeichert. Vor dem automatischen Löschvorgang eines betroffenen Datensatzes erhält der Anwender eine Benachrichtigung über die Löschung per E-Mail.

--- Zweite Ausprägung ist die Nutzung des HDS als kostenpflichtige Variante. Hier steht dann ein Speichervolumen von 5 GB zur Verfügung und Bilder werden so lange gespeichert, wie der Anwender dies möchte.

HDS PRO steht ausschließlich Ärzten (insbesondere Radiologen) und ihrem medizinischen Personal zur Verfügung („Professionals"). Auch hier gibt es zwei Ausprägungen:

--- Eine kostenlose Variante mit 1 GB Speicherplatz und Löschung von Bilddaten nach 3 Monaten nach Ablage mit vorheriger E-Mail-Benachrichtigung sowie

--- die kostenpflichtige Variante mit 5 GB Speichervolumen und unbegrenzter Speichermöglichkeit.

Beide Nutzungsmöglichkeiten, HDS und HDS Pro, werden gemeinsam als HealthDataSpace oder „HDS" bezeichnet. Das IT-Produkt und die damit verbundenen IT-Serviceleistungen wurden im Funktionsstand vom 12.08.2015 geprüft.

Der HDS kann z.B. von Ärzten in öffentlich-rechtlich organisierten Krankenhäusern in Schleswig-Holstein genutzt werden. Der HDS ist damit auditierbar nach DSGSVO.

6. Beschreibung des IT-Produkts

Das IT-Produkt HealthDataSpace ist ein webbasierender, virtueller Datenraum, in welchem Daten zu medizinischen Zwecken hochgeladen, gespeichert, verwaltet und ausgetauscht werden können. Die online unter https://app.healthdataspace.de zur Verfügung gestellte Verarbeitungskapazität ist eine typische Cloud-Dienstleistung.

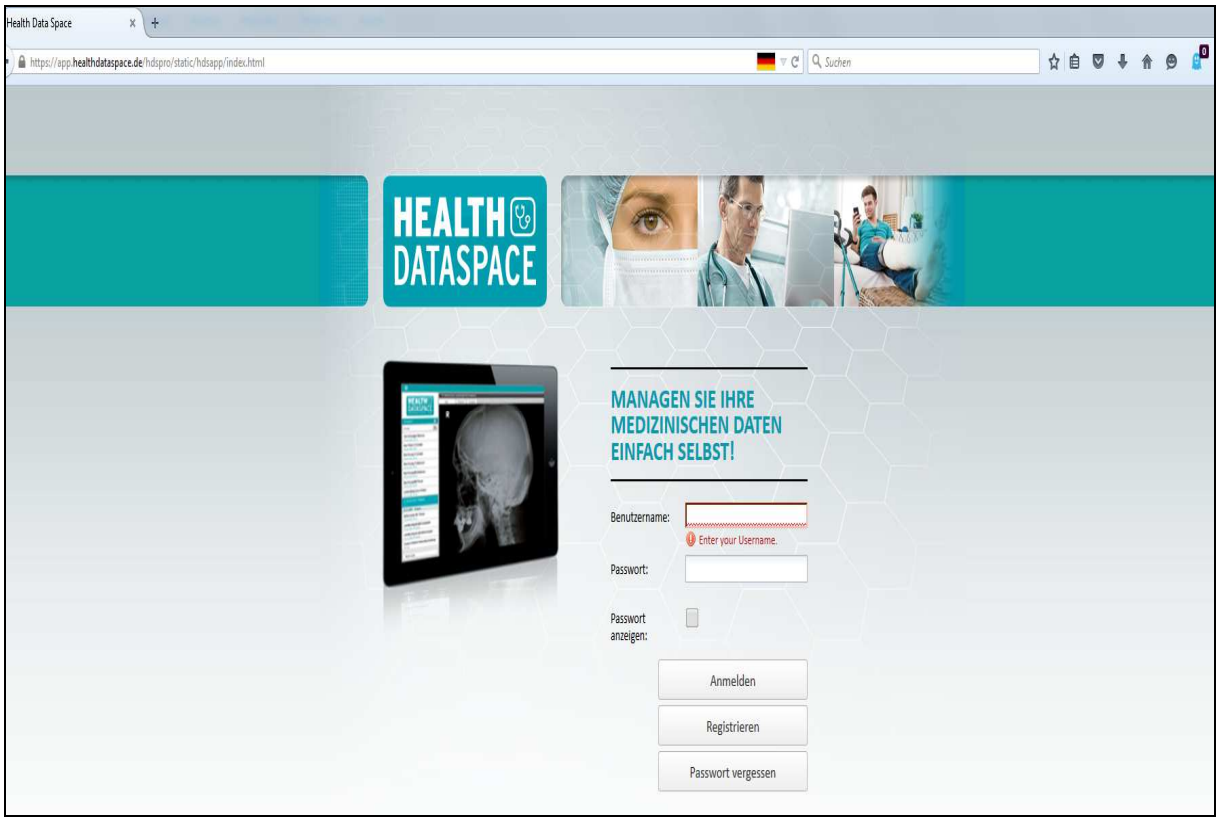


Abbildung 1 Startseite des HDS

Im Zentrum des HDS steht dabei die Selbstverwaltung medizinischer Daten durch den Patienten. Als registrierter Teilnehmer am HDS kann er seine medizinischen Daten, wie z.B. Befunde und Röntgenbilder, jederzeit über das Internet abrufen, verwalten oder anderen Personen (insbesondere Ärzten) zur Verfügung stellen.

Hingegen werden Daten, die vom Patienten einem oder mehreren Ärzten zur Verfügung gestellt worden sind, vom teilnehmenden Arzt über den HDS PRO abgerufen, verwaltet oder können anderen Ärzten zur Verfügung gestellt werden, sofern der Patient die Daten hierfür vorher freigegeben hat.

HealthDataSpace ist ein Verbundprojekt der Telepaxx Medical Archiving GmbH (Telepaxx) und der Digithurst Bildverarbeitungssysteme GmbH & Co. KG (Digithurst). Beide Unternehmen sind ansässig in Büchenbach, Deutschland. Die Firmen haben unterschiedliche Aufgaben bezogen auf den HDS:

Telepaxx stellt das hauseigene Rechenzentrum am Standort in Büchenbach für die vom HDS bzw. HDS PRO benötigte Infrastruktur bereit. Telepaxx ist zudem Betreiber der HDS Basisversion. Ferner bietet die Telepaxx die HDS Basisversion für Patienten im Rahmen des Vertriebs an. HealthDataSpace in der Basisversion wird von der Telepaxx Medical Archiving GmbH als *Software as a Service* (SaaS) betrieben.

Digithurst ist Entwickler der Software für HDS und HDS PRO. Digithurst ist Betreiber des HDS PRO und bietet den HDS PRO im Vertrieb für Ärzte an. HDS PRO wird von der Digithurst als *Software as a Service* (SaaS) im Auftrag der teilnehmenden Ärzte in

Deutschland im Rechenzentrum der unterbeauftragten Firma Telepaxx in Büchenbach betrieben.

6.1 Rollen und Berechtigungskonzept

Innerhalb des HDS können die Anwender folgende Rollen einnehmen:

Patient: Er kann HealthDataSpace in der Basisversion in folgendem Umfang nutzen:

- --- Konto anlegen
- --- Konto aktivieren
- --- Konto löschen
- --- Bilder und Befunde selbst hochladen
- --- Zuordnungen für das automatische Hochladen von Bildern + Befunden gestatten
- --- Content löschen
- --- Content ansehen
- --- Content downloaden
- --- Content datenschutzkonform teilen (Share-Links)

Arzt: Ein Arzt kann den HDS PRO in folgendem Umfang nutzen:

- --- Konto anlegen
- --- Konto aktivieren
- --- Konto löschen
- --- Content ansehen
- --- Content downloaden
- --- Content löschen
- --- Content datenschutzkonform teilen (Share-Links)
- --- Bei kostenfreier Nutzung passive Teilnahme an Communities (Keine Upload von Inhalten möglich)
- --- Bei kommerzieller Nutzung aktive Teilnahme an Communities (Upload von Inhalten möglich)
- --- Zuordnungen von Patienten-ID's auf HDS-Konten für Patienten anlegen
- --- Zuordnungen von Receiving AET's auf HDS-Konten für Communities anlegen
- --- Bilder und Befunde mit dem HealthDataSpace Collector automatische in Zielkonten hochladen

Communities: Ein Community Mitglied kann den HDS PRO in folgendem Umfang nutzen:

- --- Einer Community nach Einladung beitreten
- --- Aus einer Community austreten
- --- Content gemeinsam mit anderen HDS PRO Mitgliedern der Community betrachten.

--- Bei kostenfreier Nutzung passive Teilnahme an Communities (Keine Upload von Inhalten möglich)

--- Bei kommerzieller Nutzung aktive Teilnahme an Communities (Upload von Inhalten möglich)

Medizinisches Personal. Sie können den HDS PRO in folgendem Umfang nutzen:

--- Mappings von Patienten-ID's auf HDS-Konten für Patienten anlegen

--- Mappings von Receiving AET's auf HDS-Konten für Communities anlegen

6.1.1 Nutzung des HDS-Kontos als Patient

Über die Unterfunktion „*Teilen*" kann der Anwender den ausgewählten Content mit anderen HDS-Teilnehmern teilen. Gewährte Zugriffsrechte können zeitlich befristet und vom Kontoinhaber jederzeit eingesehen und auf Wunsch widerrufen werden.

Zum Herunterladen von Daten aus dem HDS Konto auf lokale Speichermedien muss der Anwender den Downloader auf seinem Endgerät installiert haben, welchen er im HDS-Konto als Tool herunterladen und installieren kann.

Durch Betätigen des Buttons „*Löschen*" werden die selektierten Inhalte unwiederbringlich gelöscht. Hierdurch werden automatisch auch alle Freigaben für geteilte Inhalte ungültig. Um versehentliches Löschen zu verhindern, muss der Anwender die Löschabsicht bestätigen. Bei der kostenfreien Nutzung werden Bilder und Befunde 3 Monate nach dem Einspeichern nach vorheriger E-Mail Benachrichtigung automatisch gelöscht. Bei der kommerziellen Nutzung werden Bilder und Befunde nicht automatisch gelöscht. Dort erfolgt Löschen ausschließlich durch den Anwender. Dieser kann jederzeit beliebige Inhalte und auch das komplette Konto selbst löschen. Mit dem Löschen von Inhalten oder Konten werden zudem automatisch alle betroffenen erteilten Freigaben und Zuordnungen (mappings) unwirksam.

6.2 Upload in andere HDS-Konten

HDS-PRO Anwender können mittels der Collector Software Daten in die Konten anderer Nutzer laden. Hierzu werden je nach dem vom Arzt verwendeten logischen Namen (AET = „*Application Entitiy Title*") des DICOM-Knotens sowie der IP-Adresse und der Portnummer des DICOM-Knotens folgende Informationen zur Zuordnung auf das richtige Konto verwendet:

--- Patient-ID zum Mapping eines HDS-Patienten-Kontos

--- Zugehöriger Arzt ("*Reffering Physician*") zum Mapping eines HDS-PRO-Kontos

--- Erhaltene AET zum Mapping einer HealthDataSpace Community

Diese Mappings wurden im Vorfeld mittels der HealthDataSpace Web-Oberfläche einmalig erstellt. Sie können vom Kontoinhaber des Empfangskontos jederzeit eingesehen und auf Wunsch widerrufen werden, so dass sie bei Widerruf im Empfänger-Konto sofort nicht mehr zur Verfügung stehen.

6.3 HDS PRO – Communities

HDS PRO ermöglicht die Anbindung an Communities. Dies sind Zusammenschlüsse von Ärzten in Zentren, die einrichtungsübergreifend zusammenarbeiten, wie z.B. bei einem Tumorboard. Auch eine Community kann in HDS PRO im Rahmen der Mit- und Weiterbehandlung eingebunden werden und Daten erhalten. Eine Community wird verwaltet von einem Community Administrator. Dieser kann Mitglieder einladen und entfernen.

Jeder teilnehmende Arzt verpflichtet sich in seinem Online-Vertrag zur Nutzung von HealthDataSpace dazu, Daten in Communities nur zu teilen, wenn dies aufgrund der Mit- und Weiterbehandlung notwendig ist oder eine Schweigepflichtentbindung vorliegt. § 5 der [EULA HDS PRO] lautet:

„Ärztliche Schweigepflicht: Im Rahmen des Datenschutzes nimmt die Sicherstellung der ärztlichen Schweigepflicht einen besonders hohen Stellenwert ein. Nur der Patient bestimmt, wer seine medizinischen Daten personenbezogen sehen darf. Werden Daten einer Community zur Verfügung gestellt, ist durch den Kunden sicherzustellen, dass es sich um eine Mit- und Weiterbehandlung handelt oder eine dokumentierte Schweigepflichtentbindung des Patienten vorliegt."

Zitat § 5 der [EULA HDS PRO]

6.4 Upgrade auf die kostenpflichtige Version des HDS

Bei der Nutzung des HDS als kostenpflichtige Variante steht ein größeres Speichervolumen zur Verfügung und Bilder werden so lange gespeichert, wie der Anwender dies möchte. Die Aktivierung dieser Erweiterung erfolgt entweder per telefonischer oder schriftlicher Bestellanfrage bei der Firma Telepaxx (für Patienten) oder der Firma Digithurst (für Ärzte) oder über eine Bestellung in einem Online-Webshop der Firma Telepaxx. Die Offline- und Online-Bestellvorgänge sind nicht Auditgegenstand.

6.5 Authentisierung und Verschlüsselung

Alle Objekte (Befunde) werden mit einem per Zufallsgenerator erzeugten Random Key verschlüsselt. Dieser Random Key wird mit dem Public Key des Zielkontos verschlüsselt und ebenfalls in der Datenbank abgelegt. Hierdurch wird sichergestellt, dass weder medizinischer Content, noch für die Entschlüsselung notwendige Schlüssel im Klartext beim Anbieter Telepaxx bzw. Digithurst vorliegen.

Alle Daten sind mit Random Keys verschlüsselt. Die Random Keys sind mit dem Public Key des Zielkontos verschlüsselt in der Datenbank gespeichert. Der einzige Weg, die Daten zu entschlüsseln ist, ist die Entschlüsselung des Random Keys mit Hilfe des Private Keys des HDS-Kontos. Der Private Key ist mit dem nur dem Kontoinhaber bekannten Passwort (mindestens 10 Zeihen, Komplexität: 4 aus 4) des Kontos verschlüsselt und kann nur vom Kontoinhaber entschlüsselt werden. Hierdurch ist unbefugter Zugriff ausgeschlossen.

Hierbei werden zu jedem Zeitpunkt folgende Sicherheitsmerkmale sichergestellt:

--- Die Daten werden niemals unverschlüsselt übertragen

--- Die Daten liegen auf dem HealthDataSpace nur in verschlüsselter Form vor, dies gilt sowohl für die Ablage auf einem Dateisystem als auch für die Verarbeitung im Speicher.

--- Die kryptografischen Schlüssel, mit welchen die Dateien entschlüsselbar sind, liegen auf dem HDS nur in verschlüsselter Form vor.

--- Die Entschlüsselung der Daten kann nur auf dem Endgerät einer zugriffsberechtigten Person mit Hilfe eines nur dem Zugriffsberechtigten bekannten Passwortes erfolgen.

--- Das Passwort, um die Daten zu entschlüsseln, verlässt das Endgerät des Zugriffsberechtigten nur in gehashter Form. Auch ein Systemadministrator, der Zugriff zum Rechenzentrum der Telepaxx hat, ist nicht in der Lage ohne Hilfe einer zugriffsberechtigten Person (Endbenutzer und dessen Passwort) Einsicht in die Daten zu erhalten.

Alle Daten liegen im Rechenzentrum ausschließlich in verschlüsselter Form vor. Die Personalisierung erfolgt lokal nach clientseitiger Entschlüsselung mittels des nur dem Patienten bekannten Passworts.

Ändert der Kontoinhaber sein Passwort, so wird der private Schlüssel in HDS mit dem neuen Passwort verschlüsselt abgespeichert. Der mit dem alten Passwort verschlüsselte private Key wird gelöscht. Sollte ein Benutzer sein Passwort und den Aktivierungscode verloren haben, so sind die gespeicherten Inhalte seines Kontos nicht mehr abrufbar. Es besteht aber die Möglichkeit ein neues Schlüsselpaar zu generieren, so dass das Konto weiterhin nutzbar ist. Eine solche Umschlüssel-Funktion, die evtl. auch bei Kompromittierung des Schlüssels notwendig werden könnte, kann derzeit noch nicht direkt über die Anwenderebene angestoßen werden. **Diese Funktion erscheint den Auditoren allerdings wichtig, da der Kontoinhaber auf diese Weise aktiv sicherstellen kann, dass auf seine Daten nicht unbefugt zugegriffen werden kann, sollte der Verdacht bestehen. Daher empfehlen wir der Zertifizierungsstelle die Umsetzung dieser Funktion als Auflage auszusprechen.**

Die externe Anbindung an das HDS Webportal erfolgt mittels serverseitiger Authentifikation auf der Basis eines gültigen SSL-Zertifikates (RSA-4096) unter Verwendung von TLS mit kryptographisch starken CipherSuiten.

6.6 Komponenten und Schnittstellen

HealthDataSpace besteht aus Client-Komponenten, die lokal beim Anwender („Customer“) laufen, sowie Backend-Komponenten, die im Rechenzentrum bei Telepaxx („Provider“) gehostet werden.

Der **HealthDataSpace Client** ist in HTML5 und JavaScript implementiert und ermöglicht die Device-unabhängige Nutzung, ohne dass Daten lokal gespeichert oder Software lokal installiert werden muss.

Der **HealthDataSpace Collector** wird beim Ersteller medizinischen Contents (Radiologen) in dessen Einsatzumgebung als Dienst installiert. Er dient der Integration in den klinischen Workflow und übernimmt die Datenakquisition über die Schnittstellen DICOM und HL7 sowie mittels Mapping den automatischen Upload der Daten ins richtige Konto.

HealthDataSpace Up- & Download Center

Das HealthDataSpace Up- & Download Center ermöglicht den manuellen Up- bzw. Download von Content durch den Kontoinhaber. Um auf die lokalen Ressourcen des Arbeitsplatzes (z.B. CD-Laufwerk) zugreifen zu können, muss das Center heruntergeladen und lokal auf dem Rechner in der Einsatzumgebung des Anwenders installiert werden.

Im Uploadmodus können dann DICOM-CD's und eingescannte Dokumente hochgeladen werden. Im Downloadmodus wird Content lokal heruntergeladen und ggfs. direkt mittels DICOM Send automatisch an einen Zielknoten verschickt.

Client Site Encryption

Die Verschlüsselungsebene stellt sicher, dass alle Daten clientseitig ver- und entschlüsselt werden und damit eine unbefugte Kenntnisnahme durch Dritte ausgeschlossen werden kann. Die Mechanismen sind identisch für Client, Collector und Up + Download Center.

Hierzu stellt HDS Skripte zur Verfügung, die per TLS sicher übertragen werden. Die Integrität dieser Skripte lässt sich an Hand der folgenden Prüfsummen verifizieren:

Dateiname	SHA-256 Prüfsumme
cryptojs.min.js	c46c02cde046650b6a7dbc2c56f174d07f83f816d0c786e0716fb56a804c445f
dhCryptoAccount.js	265c94a3c93c675c2b801e29fc5aec58366b3d61ec35d19266b4173c2b18db74
dhCryptoAes.js	dc3e0ef7c01e060e3915b8c62f04df8f8a74858da76fa79cf195bf634d961dc2
dhCryptoHelper.js	b4e82b1ba5da196cdc57377647dbb8aa5a92178fa02a85640b977200c1ee4ffd
dhCryptoHttpRequest.js	59b27a595fac48e5f7a5de73d60c767a2105abc2b586efd17988e579f14af527
dhCryptoRsa.js	75312f87aa61fbf8c3fe52413fd8df427ef3ca9d113ede855112d69bf5e364c6
dhError.js	0c42e0b49eafb081382cec58bf64fa15bf9656b0bb55c245f282dac6b719a53a
dhFileType.js	680a48d1ae58bba52033f8ea7874e201c566dd8b59d8cc0462571b2781d0e875
dhReencryption.js	a7866782da5fb7104827ede7aafd10722eb87469507a0e0f0fbacdbcb3acc569
dhRsaEncryptionWorker.js	03ed2b0e8339d08353037835d0afcc8f4175b2b08fa2bfba51dec39e88afe007
hammer.min.js	0a300e789ed9480f1b6523a8bfea542b480818dd5602363b72bb1fa3de5a0c0f
iscroll.js	ce8cd3a455dd7a7751ec9d2d35e0c474155488e8181cd36bda406ce2534eb32b
jquery.ui.touch-punch.min.js	8074d47b5fc9e9bdcb9656d4f775b9ce839efd9060c3640ed434bfa1f88ba94d
jquery-1.9.1.js	7bd80d06c01c0340c1b9159b9b4a197db882ca18cbac8e9b9aa025e68f998d4
jquery-ui-1.10.2.custom.js	dada08d6838305ec3183027a06ff45fb15b60f41192fb10a15103172513c934
jsbn.min.js	a2590b216b716bb89ef1338d3d9640f2b58d9e5a93d7353fbc00915e4358d31e
jspdf.min.js	46d404ab0691e6b6b88e96380b8c90fc8fcadad36e3754e3be998670311aa939
MedView_de.min.js	6b3934c7170a2b11e10fe52aff5602a9c50b155bfc612dcbb4d41b22e3127e47
MedView_en.min.js	0fa3dcfee84996d0313b5931059bc825bb728f7b0a7ebb41a068e14237af296b
MedView_sl.min.js	2a5bbe9852591a0f31d695cc41a367b14c71deca2f64eb613e49f6187acb8f12
MedView-hds.js	9212336f31f44495f12a89889303570a79c0b63f4d7e12b8c0e6fcb949946224
options.js	9bc027be0c9992a5ddceea9e16bb841eb7231807eef3531927a4d6559dce8927
pdf.js	77d78dcdf8d653e0cf568432bdf84fde19fa865974356365b16899179dc92919
pdf.worker.js	4733a9a290582b8ea1d24a4d94de28526bf8fb42b10f664cf70aa8e8ae0e9a66
versionInfo.js	2e8d1cb5ae72ef2333ae776dac4bb8db3e23d4c2183cd34fd5d2d95de1a84aa2
ZeroClipboard.min.js	a61c552c6e39c69dcaf32915ec21ee7714742fffd13991559f855841b32b38ec

Tabelle 1 Java-Script Dateien und ihre Prüfsummen

6.7 Systemvoraussetzungen

Für den Zugriff auf den HDS muss ein Internetzugang bestehen und ein HTML 5 – fähiger Browser genutzt werden. Alle Daten sind während der Übertragung vollständig verschlüsselt, so dass auch eine potentielle Man-in-the-Middle-Attacke keine Chance auf Datenzugriff hat.

HealthDataSpace wird für eine Positivliste von Browsern (Chrome, Firefox, Safari, iE in den jeweils aktuellsten Fassungen) freigegeben. Wird HealthDataSpace auf einem nicht freigegebenen Browser gestartet, erfolgt eine Warnmeldung mit Hinweis auf die freigegebenen Browser. Dann kann der Anwender entscheiden, ob die Anwendung dennoch gestartet werden soll.

Um alle Funktionen nutzen zu können, müssen JavaScript und Cookies aktiviert sein.

6.8 Einsatzumgebung

Der HDS wird im Rechenzentrum der Telepaxx Medical Archiving GmbH in Büchenbach betrieben. Das Rechenzentrum besitzt eine redundante Ausstattung aller wesentlichen HDS-Komponenten.

Die Betriebsumgebung im Telepaxx Rechenzentrum wird bereits seit einigen Jahren regelmäßig für den e-pacs Speicherdienst gemäß DSGSVO geprüft und als angemessen sicher bewertet. Das IT-Produkt e-pacs wurde seitens des ULD mit dem Datenschutzgütesiegel gemäß DSGSVO (ULD Reg-Nr. 3-5/2003) sowie seitens der EuroPriSe GmbH mit dem Gütesiegel EuroPriSe (Reg-Nr. DE-080003p) ausgezeichnet.

Wesentliche Sicherheitsmerkmale sind neben der redundanten Infrastruktur ein autonomes System für die hochverfügbare Internetanbindung, sowie die Auslegung des Objekt-Stores mit zweifacher Replikation (= mindestens drei Kopien jeder Datei) und die Cluster-Konfiguration der Datenbankumgebung mit Online-Spiegelung. Die Telepaxx Medical Archiving GmbH hat hierzu eine *„Telepaxx Security Policy“* [SecurityPolicy] erlassen, in welcher Sicherheitsanforderungen und die hierzu umgesetzten Sicherheitsmaßnahmen dokumentiert sind. Technisch-organisatorischen Datenschutzmaßnahmen des Rechenzentrums gehen ferner aus dem Vertrag zur Auftragsdatenverarbeitung der Firma Digithurst mit der Firma Telepaxx hervor.

Die IT-Landschaft beim Anwender kann im Rahmen der Auditierung nicht konkretisiert werden. Sie gehört daher nicht zum Auditgegenstand.

6.9 Verarbeitung von Primär- und Sekundärdaten

Folgende Daten werden im HealthDataSpace verarbeitet:

Patientendaten:

--- E-Mail-Adresse des Patienten
--- Konto-Art „Patient“
--- Geschlecht
--- Geburtsdatum
--- Optional: Befunde mit Gesundheitsdaten

--- Optional: Studien im DICOM-Format oder PDF
--- Optional: Bilddaten mit Gesundheitsdaten
--- Date created Upload Process
--- Date Medical Record
--- Optional: Description Medical Record
--- Optional: Name Medical Record
--- Type Upload Process
--- UID Medical Record
--- Optional: Accession Number
--- Patienten-ID (lokale ID des behandelnden Arztes)
--- Konto-ID (UUID des Kontos)
--- Vertragsart (kostenlose Nutzung oder kostenpflichtige Nutzung für Abrechnung)
--- Passwort / Benutzername

Arztbezogene Daten:

--- Vor- + Nachname des Arztes
--- Fachrichtung
--- Akademischer Grad
--- E-Mail-Adresse (geschäftlich)
--- Auswahl als „Arzt-Konto“
--- LANR, lebenslange Arztnummer
--- Optional: Name der Institution
--- Optional: Postanschrift (geschäftlich)
--- Ersteller-ID
--- Registrierungsnummer
--- Optional: Telefonnummer (geschäftlich)
--- Optional: Profilfoto
--- Optional: „bio“ – dies ist eine Freitextmöglichkeit zur Selbstdarstellung und Eigenwerbung des Arztes
--- Optional: „type“ – dies ist eine Typisierung des Arztes als „Arzt“ oder als „HC Professional“
--- Konto-ID (UUID des Kontos)
--- Vertragsart (kostenlose Nutzung oder kostenpflichtige Nutzung für Abrechnung)
--- Passwort / Benutzername

Medizinisches Personal:

Zusätzlich zu den arztbezogenen Daten werden bei einem Anwender des medizinischen Personals folgende Daten erfasst:

--- E-Mail-Adresse (geschäftlich)

--- Auswahl als medizinisches Personal-Konto

--- Rolle (= medizinische Funktion)

--- Konto-ID (UUID des Kontos)

--- Vertragsart (kostenlose Nutzung oder kostenpflichtige Nutzung für Abrechnung)

--- Passwort / Benutzername

Sodann entstehen durch die Logging- und Protokollmechanismen Sekundärdaten.

Systemseitige Protokolldaten zur Fehlersuche und Fehlerbehebung werden in einem Errorlog erfasst.

Bei Einsatz des Collectors in der Arzt-Praxis werden zu Revisionskontrollen des Arztes sowie zum frühzeitigen Erkennen von Systemstaus durch höhere Datenmengen Daten im Collector Log erfasst.

6.10 Abgrenzung des Auditgegenstands

Diese Auditierung des HealthDataSpace mit den Nutzungsfunktionen als HDS Basisversion für Patienten und HDS PRO für die Nutzung durch Ärzte und deren medizinisches Personal umfasst folgende Komponenten:

--- HealthDataSpace Client

--- HealthDataSpace Collector

--- Clientseitige Ver- & Entschlüsselung

--- HealthDataSpace Backend (Rechenzentrums-seitig) inklusive des Datenmodells

Folgende Komponenten sind Bestandteile der definierten Einsatzumgebung und damit kein Zertifizierungsgegenstand:

--- Betriebssystem clientseitig

--- Browser clientseitig

--- Betriebssystem RZ-seitig

--- LIGHTSSL-Server

--- TOMCAT Application Server

--- RADOS Object Store

--- PostgreSQL Datenbank

Ferner nicht auditiert werden:

--- Der Webshop und andere Vertriebsmethoden für die kostenpflichtigen Anwendungen des HDS und des HDS PRO

--- HealthDataSpace Up- & Download Center

--- Die Hardwarebestandteile und das diesbezüglich verwendete Betriebssystem im Rechenzentrum

--- Die Bildgebungssoftware medVIEW

--- Andere Services der Firmen Telepaxx oder Digithurst

Nicht Auditgegenstand ist ferner die Einsatzumgebung des Anwenders inklusive eingesetzter Tablets, Apps oder Smartphones.

6.11 Rechtlichen und technische Rahmenbedingungen

Der rechtliche Rahmen zur Entwicklung eines Anforderungsprofils gemäß der Datenschutzgütesiegelverordnung Schleswig-Holstein besteht in dem Landesdatenschutzgesetz Schleswig-Holstein (LDSG S-H), der Datenschutzverordnung (DSVO), dem Bundesdatenschutzgesetz (BDSG) sowie den bereichsspezifischen Bestimmungen des Gesundheitswesens. Die Auslegung dieser Rechtsnormen wird konkretisiert durch Rechtsprechung und durch Mitteilungen der Datenschutzaufsichtsbehörden. Da der HDS als Subsystem in einem Krankenhausbetrieb eingesetzt werden könnte, ist etwa die „*Orientierungshilfe Krankenhausinformationssysteme*“ der Unterarbeitsgruppe Krankenhausinformationssysteme der Arbeitskreise Gesundheit und Soziales sowie Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu beachten. Wie bereits gesehen, handelt es sich bei HDS zudem um eine Public Cloud Dienstleistung, so dass u.a. die Auslegungshilfen des Working Paper No. 196 der Artikel-29-Datenschutzgruppe („*Opinion 05/2012 on Cloud Computing*“) sowie die „*Orientierungshilfe – Cloud Computing, Version 2.0*“ der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu beachten sind.

Die Pflicht zum ordnungsgemäßen Umgang mit Patientendaten ergibt sich für den Arzt zudem aus einer Vielzahl von bereichsspezifischen Rechtsvorschriften. Dies folgt aus § 10 der (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) bzw. den nahezu gleichlautenden landesgesetzlichen Ausprägungen der Berufsordnungen. Wesentlich ist die **ärztliche Schweigepflicht**, welche eine der ältesten bekannten Datenschutzbestimmungen darstellt. Sie gilt gemäß **§ 203 Strafgesetzbuch (StGB) in Verbindung mit § 9 MBO-Ä** 1997 für das gesamte Behandlungsverhältnis. Im Zuge der Datenverarbeitung mittels HealthDataSpace darf das Patientengeheimnis weder innerhalb Praxisgemeinschaften, noch gegenüber externen Personen rechtswidrig offenbart werden, sofern diese Rollen nicht zugleich einem behandelnden Arzt zuzuordnen sind oder sofern keine Entbindung von der Schweigepflicht vorliegt. Insbesondere dürfen die Patientendaten nicht der Telepaxx oder der Digithurst rechtswidrig offenbart werden.

Dabei ist hervorzuheben, dass beim HDS in der Basisversion Patientendaten ausschließlich durch den Patienten an andere Personen übermittelt werden. Der Patient offenbart seine Daten demnach ausschließlich selbst an die von ihm ausgewählten Personen. Eine Entbindung von der Schweigepflicht für Berufsgeheimnisträger ist hier nicht erforderlich. Rechtsgrundlage der Datenverarbeitung des HDS in der Basisversion ist ausschließlich der [EULA HDS] als vertragliche Regelung.

Etwas anderes kann gelten, wenn Patientendaten vom Patienten zunächst an einen Arzt im Rahmen des Behandlungswunsches weitergegeben werden und der

behandelnde Arzt dann diese Daten der HDS-Community zur Verfügung stellt. Auch hier behält der Patient allerdings jederzeit die Selbstbestimmungsrechte über seine Daten, da nur er bestimmt, an wen die Daten über einen Link weitergegeben werden. Er wird zudem benachrichtigt, wenn die von ihm freigegeben Daten mit anderen Personen geteilt werden. Ferner kann er die Rechte jederzeit entziehen, so dass dann ein Zugriff auf die Daten verwehrt ist. Für die reguläre Weitergabe der Patientendaten an die HDS-Community liegt damit immer eine bewusste Entscheidung des Patienten vor.

Es sind allerdings Fälle denkbar, in denen Bilddaten aus dem HDS PRO heraus kopiert und dann außerhalb der Systeme des HDS PRO an Dritte weitergegeben werden könnten. In der Regel wird es sich dabei um ein (Röntgen-)Bild handeln, welches keinen Bezug zu einem Patienten aufweist und anonymisiert weitergegeben wird (z.B. an Konsiliarärzte). Es kann aber im Ausnahmefall bei einer älteren Röntgenaufnahme vorkommen, dass der Name des Patienten mit auf dem Bild abgebildet ist. Diese dann nicht mehr anonymisierte Bildweitergabe, die in der Praxis inzwischen allerdings sehr selten vorkommt, könnte dann als Offenbarung von Patientendaten gewertet werden. Daher ist für diesen Einzelfall entweder ein Behandlungsvertrag notwendig, welcher die Weitergabe erlaubt oder eine Entbindung von der Schweigepflicht. Das IT-Produkt HealthDataSpace kann für diese seltene Konstellation, in welcher auch kein individueller Behandlungsvertrag als Rechtsgrundlage eingreift, kein allgemeingültiges Muster für eine Schweigepflichtentbindung vorsehen. Allerdings wird der teilnehmende Arzt auf diese Situation in § 5 der [EULA HDS PRO] sensibilisiert und vertraglich dazu verpflichtet, entweder Bilddaten zu anonymisieren, einen Behandlungsvertrag abzuschließen oder eine Schweigepflichtentbindung einzuholen. Verstöße hiergegen können neben der strafrechtlichen Sanktionierung demnach auch als Vertragsverstoß gegen die Nutzungsbestimmungen des HDS PRO gewertet werden, so dass zivilrechtliche Sanktionen möglich sind. Zudem befindet sich in der Datenschutzerklärung ein deutlicher Hinweis auf die Schweigepflichtentbindung als erforderliche Rechtsgrundlage.

Letztendlich wird durch die aufgeführten **Verschlüsselungsmechanismen** auch eine Offenbarung gegenüber Unbefugten systemseitig bereits ausgeschlossen; dadurch wird zugleich der Beschlagnahmeschutz des **§ 97 der Strafprozessordnung** (StPO) zugunsten der ärztlichen Schweigepflicht unterstützt.

HealthDataSpace ist allerdings kein Archivsystem zur Sicherstellung dieser gesetzlichen Aufbewahrungsvorschriften. Diese sind vom Arzt nach wie vor durch andere geeignete Lösungen zu realisieren. Weder die Archivierungsregelungen der MBO-Ä noch der **Röntgenverordnung** sind daher für den HDS einschlägig.

Soweit das Gesundheitswesen keine spezielleren Regelungen vorsieht, gilt für nicht-öffentliche Stellen ergänzend das **BDSG** als allgemeineres Gesetz. Für den Einsatz des IT-Produkts durch öffentliche Stellen Schleswig-Holsteins gilt hingegen das **LDSG S-H**.

Für die Verarbeitung von Gesundheitsdaten durch den Patienten selbst im HDS ist das Bundesdatenschutzgesetz gemäß § 1 Abs. 2 Nr. 3 BDSG allerdings nicht

anwendbar, da die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. Eine Datenverarbeitung dient typischerweise dann familiären und privaten Zwecken, wenn sie im Rahmen einer nicht geschäftlichen Tätigkeit wahrgenommen wird, beispielsweise bei Privatreisen oder privater Kommunikation[2]. In diesem Kontext ist auch das Nutzen des HDS für Patienten als eine private Nutzung einzustufen, da der Patient hier seine medizinischen Daten selbst verwaltet und diese z.B. Familienmitgliedern zur Verfügung stellen oder auf Reisen abrufen möchte. Da das BDSG in diesem Fall nicht einschlägig ist, kann auch der Service der Verarbeitung und Speicherung der medizinischen Daten in der Public Cloud durch die Telepaxx nicht als Auftragsdatenverarbeitung gemäß § 11 BDSG bzw. § 17 LDSG S-H klassifiziert werden.

Anders zu bewerten ist dies für die Datenverarbeitung durch einen HDS PRO Anwender, da dieser sich nicht auf die Ausnahme des § 1 Abs. 2 Nr. 3 BDSG berufen kann. Arbeitet er mit den personenbezogenen Daten im HDS PRO, ist das BDSG einschlägig. Zu berücksichtigen sind dann insbesondere die Grundsätze zum Schutz von besonderen personenbezogenen Daten. Gemäß § 3 Abs. 9 BDSG sind besondere Arten personenbezogener Daten alle Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Die Verarbeitung der besonderen Datenarten ist ebenfalls in § 11 Abs. 3 LDSG S-H geregelt. Die mittels des IT-Produktes verarbeiteten Patientendaten sind Gesundheitsdaten und daher besondere Datenarten. Da das BDSG bzw. LDSG S-H in diesem Fall einschlägig ist, kann auch der Service der Verarbeitung und Speicherung der medizinischen Daten in der Cloud durch die Digithurst mit der Unterbeauftragung der Telepaxx als Rechenzentrumsdienstleister dann als Auftragsdatenverarbeitung gemäß § 11 BDSG bzw. § 17 LDSG S-H klassifiziert werden.

Ferner ist die Datenverarbeitung im Rahmen der vertraglichen Anbahnung, Abwicklung und Abrechnung der kostenpflichtigen Varianten des HDS und des HDS PRO anhand der Bestimmungen des BDSG bzw. des LDSG-SH zu betrachten. Denn mit der Registrierung wird ein Vertrag zwischen dem Nutzer und der Telepaxx (bei Patienten) bzw. der Digithurst (bei Ärzten) geschlossen. Personenbezogene Daten, die zur Vertragsabwicklung und –abrechnung erhoben und verarbeitet werden, unterliegen dann dem § 28 Abs. 1 Nr. 1 BDSG bzw. § 11 LDSG S-H.

Alle Anforderungen sind hier angemessen erfüllt.

Hervorzuheben ist, dass es sich bei dem HealthDataSpace um keinen Telemediendienst im Sinne des **Telemediengesetzes** (TMG) handelt, welcher online für eine offene Benutzergruppe über das Internet erreichbar ist. Vielmehr wird der HealthDataSpace ausschließlich in der Einsatzumgebung des Anwenders eingesetzt und basiert zudem auf einer Datenverarbeitung innerhalb einer geschlossenen Benutzergruppe, so dass die Ausnahme des § 11 Abs. 1 Nr. 2 TMG erfüllt ist. Eine Ausnahme gilt allerdings für solche Webseiten, die für jedermann öffentlich im Internet abrufbar sind und weiterführende Informationen zum enthalten. Die

[2] Taeger, Gabel: Kommentar zu § 1 BDSG, Rn. 31.

Startseite des HealthDataSpace unter https://app.healthdataspace.de sowie Produkt-Informations-Webseiten stellen einen allgemein zugänglichen Telemediendienst im Sinne des TMG dar. Diese Webseiten müssen sich daher diesen Anforderungen stellen und etwa ein Impressum (§ 5 TMG), eine Datenschutzerklärung (§ 13 TMG) sowie einen rechtskonformen Umgang mit Nutzerdaten gemäß § 15 TMG aufweisen. Diese Anforderungen sind hier angemessen erfüllt.

Die **DSVO** regelt hingegen die Dokumentation automatisierter Verfahren bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen (§ 3 Abs. 1 LDSG S-H) sowie deren Tests und die Freigabe dieser Verfahren. Für den HDS kam es daher auf die Prüfung der Dokumentationen, Tests und Freigabeverfahren an, wobei auch diese Anforderungen angemessen erfüllt sind.

7. Tools, die zur Herstellung des Produkts verwendet wurden

Folgende Tools wurden für die Entwicklung eingesetzt:

--- Clientseitig: SENCHA.

--- Serverseitig GRAILS 2.3.4.

Folgende Tools werden für den Betrieb eingesetzt:

--- Object Store Management: RADOS 0.7.2 Emperor.

--- Database Managament: PostgreSQL 9.3.

--- Operating System: Debian WHEZZY 7.4.

--- WebServer: Light TTP 1.4.3.1.

--- Application Server: Tomcat 7.

8. Zweck und Einsatzbereich

Das IT-Produkt HealthDataSpace ist ein webbasierender, virtueller Datenraum, in welchem Daten zu medizinischen Zwecken hochgeladen, gespeichert, verwaltet und ausgetauscht werden können. Die Nutzer des HDS können Privatpersonen (Patienten) und Ärzte (Geschäftskunden) sein.

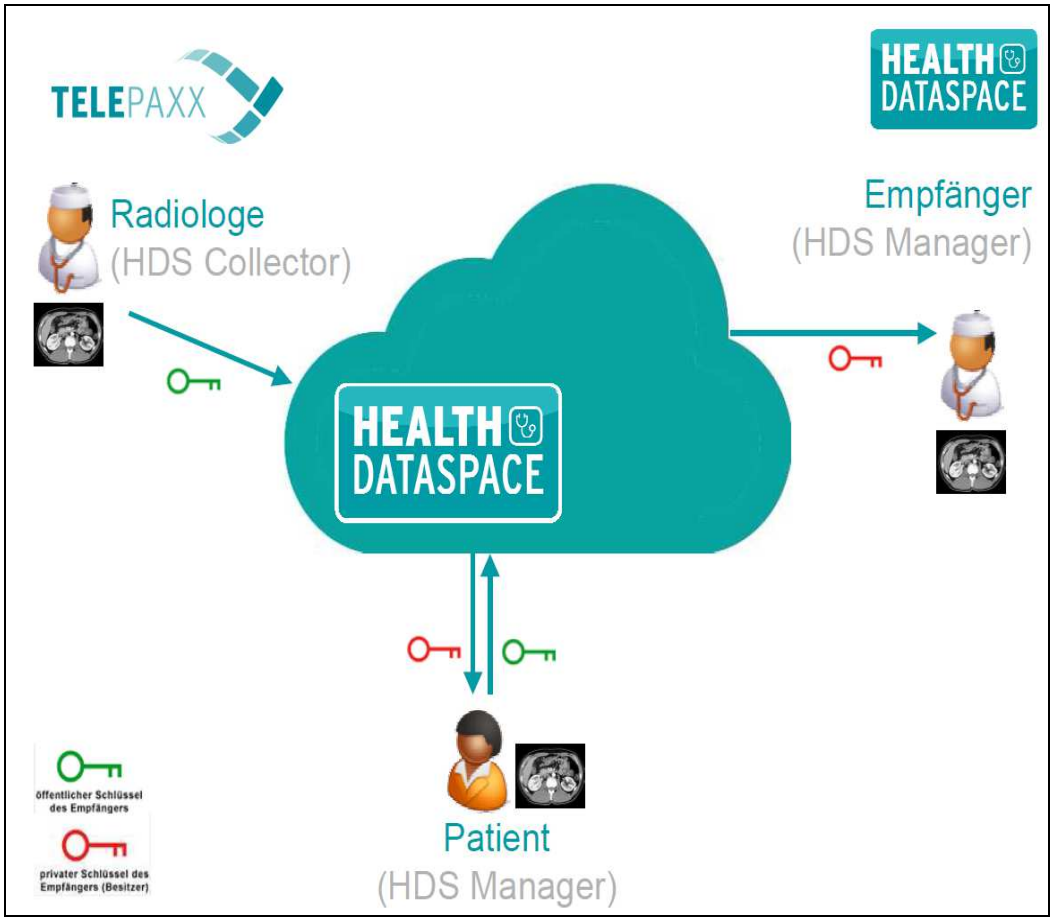
Das IT-Produkt HealthDataSpace unterscheidet zwei Anwenderkonten:

--- HealthDataSpace – HDS (Basiversion).

--- Health DataSpace Professional – HDS PRO.

Näheres siehe Abschnitt 6.

9. Modellierung des Datenflusses



Legende: Radiologe (HDS Collector) = Anwender des HDS PRO; Empfänger (HDS Manager) = Datenempfänger; dies ist i.d.R. ein weiterer Arzt, kann aber z.B. auch ein Verwandter des Patienten sein, der die Daten empfangen soll; Patient (HDS Manager) = Patient:

10. Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Version 2

11. Zusammenfassung der Prüfergebnisse

Für das IT-Produkt HealthDataSpace ergibt sich danach folgende Gesamtbewertung:

Nr.	Anforderungsprofil	Bewertung / Kommentar
Datenart A (Primärdaten):		
A1	Verfügbarkeit, Integrität, Vertraulichkeit	angemessen
A2	Nicht-Verkettbarkeit	angemessen

A3	Transparenz	angemessen
A4	Intervenierbarkeit	angemessen
A5	Anpassung des IT-Produkts	angemessen
A6	Privacy by Default	vorbildlich
A7	Sonstige Anforderungen	angemessen
A8	Zulässigkeit der Datenverarbeitung	angemessen
A9	Einhaltung allg. Datenschutzgrundsätze	angemessen
A10	Datenverarbeitung im Auftrag	angemessen
A11	Besondere technische Verfahren	angemessen
A12	Sonstige Anforderungen	Nicht anwendbar
A13	Einzelne technisch-organisatorische Maßnahmen	verbesserungsbedürftig
A14	Allgemeine Pflichten	angemessen
A15	Spezifische Pflichten	angemessen
A16	Pflichten nach DSVO	angemessen
A17	Betrieb der Auftragsdatenverarbeitung	angemessen
A18	Sonstige Anforderungen	Nicht anwendbar
A19	Aufklärung und Benachrichtigung	angemessen
A20	Benachrichtigung bei unrechtmäßiger Kenntniserlangung	angemessen
A21	Auskunft	angemessen
A22	Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegendarstellung	angemessen
A23	Sonstige Anforderungen	Nicht anwendbar
Datenart B (Sekundärdaten):		
B1	Datenvermeidung und Datensparsamkeit	angemessen
B2	Zweckbindung	angemessen
B3	Nicht-Verkettbarkeit	angemessen
B4	Transparenz	angemessen
B5	Rechtsgrundlagen	angemessen
B6	Zweckbindung	angemessen
B7	Aufbewahrungsfristen	angemessen
B8	Physikalische Sicherung	angemessen

B9	Zugriffsschutz	angemessen
B10	Ermittlung / Sichtbarkeit der Protokolldaten	angemessen
B11	Technische Umsetzung der Speicherfristen	angemessen
B12	Unzulässige Verkettung	angemessen
B13	Beschreibung der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit	angemessen
B14	Selektive Löschung von Einzeldaten, Beauskunftung, Berichtigung, Sperrung, Einwand	angemessen
Förderung des Datenschutzes:		
Das IT-Produkt fördert den Datenschutz insgesamt auf angemessene Weise		

12. Beschreibung, wie das IT-Produkt den Datenschutz fördert

Das IT-Produkt HealthDataSpace fördert den Datenschutz auf vielfältige Weise:

--- Die informationelle Selbstbestimmung des Patienten über seine Daten wird durch das Produkt optimal umgesetzt; der Patient hat es jederzeit in der Hand, über die Verwendung seiner Daten zu bestimmen und diese gleichzeitig schnell und an jedem Ort mit Internetanschluss zur Verfügung zu haben.

--- Durch eine graphische Darstellung der Passwortsicherheit als Ampelsystem

13. Votum der Auditoren

Das IT-Produkt HealthDataSpace setzt insgesamt die Anforderungen an den Datenschutz angemessen um.

Bremen, den 22. September 2015.

Dr. Irene Karper LL.M.Eur.
datenschutz cert GmbH

Ralf von Rahden
datenschutz cert GmbH