Kurzgutachten zur Erteilung eines Datenschutzgütesiegels für teamplay

im Auftrag der Siemens Healthcare GmbH

datenschutz cert GmbH

06. Oktober 2016

Inhaltsverzeichnis

1. Vorbemerkung

Nachfolgend wird die datenschutzrechtliche und sicherheitstechnische Begutachtung des IT-Produktes und IT-basierenden Services „teamplay“ der Siemens Healthcare GmbH zusammengefasst, mit der die datenschutz cert GmbH als Prüfstelle beauftragt wurde. Die Begutachtung erfolgte anhand der Datenschutzgütesiegelverordnung Schleswig-Holsteins (DSGSVO) i.V. m. der Version 2 des Anforderungskatalogs zum Datenschutz-Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD)[1].

2. Zeitraum der Prüfung

Die Begutachtung erstreckte sich auf den Zeitraum von 01.05.2015 bis 06.10.2016.

3. Antragstellerin

Antragstellerin dieses Gutachtens ist die

Siemens Healthcare GmbH
Henkestr. 127
91052 Erlangen

Ansprechpartner sind

Herr Frank Rottmayer	Frau Dr. Ute Rosenbaum
Siemens Healthcare GmbH	Siemens AG
Services Digital Health Services HC SV DS TP	Corporate Technology, CT RDA ITS CER-DE
Henkestr. 127	Otto-Hahn-Ring 6
91052 Erlangen	81739 München

4. Sachverständiger/Prüfstelle

Sachverständige dieses Gutachtens ist die Prüfstelle

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

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

5. Kurzbezeichnung des IT-Produkts und IT-basierenden Services

Begutachtet wurde das IT-Produkt „teamplay“. Das Produkt ist zugleich ein IT-basierender Service, der mit Funktionsstand vom 06.10.2016 auditiert wurde. teamplay kommt in der auditierten Version ausschließlich auf europäischen Märkten zum Einsatz.

[1] Weitere Informationen sind abrufbar unter https://www.datenschutzzentrum.de/. Alle benannten Webseiten waren mit Stand zum 06.10.2016 online abrufbar.

6. Beschreibung des IT-Produkts und IT-basierenden Services

teamplay ist eine onlinebasierende Plattform zur Vernetzung medizinischer, bildgebender[2] Systeme (z.B. digitales Röntgen, Magnetresonanztomographie (MRT), Computertomographie (CT), Sonographie). teamplay erfasst Daten der vernetzten Geräte, minimiert diese und erstellt hierüber Statistiken, die im Rahmen einer Cloud-basierten Lösung online abgerufen werden können. Anhand der Auswertungen können dann Geräteauslastungen und Strahlendosis optimiert werden.

7. Tools, die zur Herstellung des Produkts verwendet wurden

Es wurden keine für die Bewertung relevanten Tools eingesetzt.

8. Zweck und Einsatzbereich

Anwender von teamplay sind Kliniken, radiologische Arztpraxen und Radiologen. Der teamplay Receiver wird dabei in einem lokalen Netzwerk installiert und übernimmt die Kommunikation zwischen den Systemen und der teamplay Plattform, indem es die Daten minimiert und an die Plattform sendet. Dabei wird über DICOM („Digital Imaging and Communications in Medicine“) kommuniziert, einem international anerkannten Standard für die Radiologie zum Austausch von Bildern und Daten.

teamplay wird als Basic Account und als Premium Account angeboten. Basic Accounts werden kostenlos zur Verfügung gestellt und können von der Institution auf einen Premium Account mit zusätzlichen, kostenpflichtigen Funktionen hochgestuft werden. Gegenstand dieses Audits ist der Premium-Account, der die Funktionalität des Basic Accounts umfasst.

Über die online unter https://teamplay.siemens.com aufrufbare Plattform können registrierte Anwender Statistiken abrufen. Hier stehen im Standard-Nutzer-Account die Funktionen „Home“, „Usage“, „Dose“ und „Protocols“ zur Verfügung.

Home ist die Startseite mit einer Übersicht zu den Accountdaten und Funktionen.

Usage bietet eine Übersicht und Statistiken über die Geräte (z.B. MRT, CT) und deren Auslastung und Wechselzeiten. Dadurch soll dem Anwender ermöglicht werden, den Behandlungsablauf zeitlich zu optimieren.

Dose stellt Auswertungen über die verwendete Strahlungsdosis dar und hilft, diese zu überwachen und so niedrig wie möglich zu halten. Damit wird u.a. eine medizinrechtliche Anforderung in den USA in Bezug auf die Kenntlichmachung der Strahlendosen umgesetzt. Das Modul dient der Umsetzung von Qualitätssicherungsprozessen, der Verringerung von Haftungsfällen aufgrund Überdosierung aber auch der optimalen Mischung zwischen Bildqualität und Strahlungsdosis.

Protocols stellt eine Übersicht über erstellte Protokolle der Auswertungen des Anwenders zusammen.

Der Administrator-Account hat zusätzlich die Funktion „Einstellungen“, über welche die Benutzerverwaltung des teilnehmenden Instituts erfolgt. Hier werden Angaben zum Institut, den Modalitäten und Benutzern verwaltet. Außerdem lässt sich das für

[2] Nicht gemeint sind Fotos von Äußerlichkeiten einer Person.

teamplay spezifische Datenschutzprofil (dazu sogleich) konfigurieren und Auswertungs-Funktionen aktivieren.

teamplay wird in zukünftigen Versionen weitere Module enthalten, wie z.B. eine Benchmarking-Funktion, anhand derer anonymisierte Daten eines Instituts mit denen anderer Anwender verglichen werden können. Bereits aktiv – aber nicht Gegenstand der Evaluation – sind das Modul „Images" zur gemeinsamer Nutzung von Daten und Bildern und der Bildung einer Online Community, sowie die Authentifikation über den Siemens Corporate Entitlement Service, welcher eine alternative Loginfunktionalität anbietet. Diese Funktionen gehören derzeit nicht zum Auditgegenstand. Auf sie wird in der Datenschutzerklärung von teamplay aber entsprechend hingewiesen.

Teamplay bietet u.a. folgende Funktionen:

- --- Usage- und Dose-Analytik aus Daten mehrerer Anbieter und nicht nur von Siemens Modalitäten
- --- Individuelle Dosisanforderung, mit der Vergleichsansichten zur Dose-Analyse erstellt werden können.
- --- Dose PACS-Aufruf, mit dem die PACS-Webschnittstelle für ein bestimmtes Dosisereignis aufgerufen werden kann, um die Bildqualität zu steigern (PACS = „Picture Archiving and Communication System")
- --- Patientenspezifische Dose-Ansichten, mit denen die Anzahl der pro Patient in der Einrichtung durchgeführten Untersuchungen anzeigen können (nur verfügbar im Datenschutzprofil „Standard Datenschutz" und „Hoher Datenschutz")
- --- Dose SSDE, um die Dosiswerte nach der Patientengröße aus den DICOM-Header-Informationen oder geschätzt von CT-Topogrammen zu normalisieren (nur verfügbar im Datenschutzprofil „Standard Datenschutz").

DICOM und Datenminimierung mittels des Receivers - Datenschutzprofile

Der DICOM Standard definiert ca. 4000 verschiedene Tags, in denen das Ergebnis von bildgebenden Verfahren, das eigentliche Bild inklusiv der Patientendaten, Untersuchungsparameter und Gerätedaten strukturiert gespeichert werden. Daraus sind ca. 250 tags personenbeziehbar oder personenbezogen (z.B. Name, Geschlecht, Alter des Patienten, Arzt-bezogene Daten, vgl. hierzu die Leitlinien des DICOM Standards, Teil 15, Anhang E, Fassung 2011, PS 3.15-2011[3]). Diese können durch Entfernen oder Ersetzen der Werte anonymisiert werden.

Der Receiver dient als DICOM-Knoten. teamplay übernimmt bestimmte, ausgewählte DICOM-Dateien über den Receiver aus dem PACS oder direkt von den bildgebenden Geräten. Der Receiver empfängt nur ganz bestimmte DICOM-Dateien und minimiert diese nun zusätzlich in drei möglichen Stufen (= „Datenschutzprofile"). Dabei werden nur die DICOM Werte behalten die für die Auswertungen benötigt werden. Insbesondere werden personenbeziehbare Daten bzw. Daten die zur Re-

[3] Vgl. http://medical.nema.org/dicom/2011/11_15pu.doc .

identifikation beitragen könnten gemäß dem eingestellten Datenschutzprofil gelöscht, durch ein Pseudonym ersetzt oder in der Genauigkeit reduziert. Bilddaten werden nicht erfasst mit Ausnahme einzelner Übersichtsbilder (Topogramme) die für die Berechnung der optimalen Dosis benötigt werden. Ziel dieser Minimierung ist eine Reduktion der Daten bis hin zu einer vollständigen Anonymisierung. Der Anwender kann aus drei Datenschutzprofilen die Minimierung auswählen: „Standard Datenschutz"; „Hoher Datenschutz" und „Restriktiv". Eine vollständige Anonymisierung wird nur mit dem Profil „Restriktiv" erreicht.

Datengruppe	Standard Datenschutz	Hoher Datenschutz	Restriktiv
Geräte-Informationen und technische Daten	beibehalten	beibehalten	beibehalten
Zeit/Datum	beibehalten	beibehalten	reduzierte Genauigkeit
Patientenalter	reduzierte Genauigkeit	reduzierte Genauigkeit	reduzierte Genauigkeit
Personalinformation zur Institution	beibehalten	beibehalten	Ersatzwert
Patienten-ID	Ersatzwert	Ersatzwert	Ersatzwert
UID	Ersatzwert	Ersatzwert	Ersatzwert
Verfahrensbeschreibung	beibehalten	beibehalten	entfernt
Patienteneigenschaften	beibehalten	reduzierte Genauigkeit:	entfernt
Informationen zur Institution	beibehalten	entfernt	entfernt

Tabelle 1 Datenschutzprofile zur Minimierung der DICOM-tags

Die Tabelle enthält dabei in der linken Spalte zusammengefasste Datengruppen. Die Datenminimierung ist für jeden DICOM-tag einer solchen Gruppe ausführlich in der Produktdokumentation dargestellt. Zuerst werden in allen drei Profilen alle Informationen gelöscht, die eine direkte Beziehung zu einem Patienten ermöglichen, wie Name, Adresse, Telefonnummer. Dann werden Informationen identifiziert, die die Identifikation des Patienten möglicherweise unterstützten. Das sind Werte für

- Zeit/Datum der Untersuchung
- Alter
- Geschlecht
- Patienteneigenschaften (z.B. Gewicht, Größe, Bodymaßindex)
- Identifier, der die Zuordnung mehrerer Untersuchungen zu einem Patienten ermöglicht. (Patienten-ID).

Patienten- und Untersuchungs-ID werden in allen Profilen durch kryptographische Ersatzwerte ersetzt, um die Konsistenz der Daten sicherzustellen. Die übrigen Werte werden im Standard-Datenschutz-Profil weitestgehend unverändert übernommen. Im Profil „Hoher Datenschutz" wird der Detailgrad der Informationen bereits deutlich

reduziert. Damit kann eine Re-Identifikation des Patienten aufgrund von Extremwerten ausgeschlossen werden. Im Profil „Restriktiv“ werden die meisten Werte entfernt oder durch kryptographische Ersatzwerte ersetzt. Lediglich Untersuchungszeitpunkt und -monat bleiben erhalten. Das Patientenalter wird in Kategorien angegeben. Auf diese Weise lässt sich zeigen, dass selbst bei einer sehr vorsichtigen Rechnung in jedem Fall eine k-Anonymität von k=10 erreicht wird. Für die Praxis realistisch ist sogar eine deutlich höhere k-Anonymität Zusätzliche Informationen zur Untersuchungsart werden ebenfalls gelöscht, um Datenangriffe hierüber zu verhindern. Da in den zwei weniger minimierten Profilen eine Re-Identifikation eines Patienten nicht ganz ausgeschlossen werden kann, können diese Profile nur bei Sicherstellung einer rechtlichen Grundlage, d.h. einer Einwilligungserklärung der betroffenen Personen i.V.m. einer Entbindung von der ärztlichen Schweigepflicht, genutzt werden. Hierfür hält die Siemens Healthcare GmbH eine Patientenerklärung samt Schweigepflichtentbindung bereit.

teamplay ermöglicht Prozeduren vom Bediener der Geräte (i.d.R. ist dies ein Beschäftigter) zu analysieren. Diese Option ist standardmäßig in teamplay deaktiviert und kann vom Anwender aktiviert werden. Im Datenschutzprofil „Restriktiv“ werden nur anonymisierte Werte der Bedienernamen hochgeladen, die keine direkten Rückschlüsse auf den Bediener zulassen.

Einige ältere Scanner nutzen ggf. noch DICOM Secondary Capture-Bilder (sog. „Black Images“), bei denen die Dosis-Information in das Bild gebrannt wurde. Der teamplay Receiver erkennt dies mit Hilfe der optischen Zeichenerkennungsfunktion und entfernt automatisch den eingebrannten Patienten- und Bedienernamen und Geburtsdatum, bevor die Daten an die Plattform übergeben werden. Hierfür werden Algorithmen eingesetzt, die als angemessen bewertet wurden.

teamplay ermöglicht zudem, einzelne Datensätze von einer Übertragung an die Plattform auszunehmen, indem diese auf eine Blacklist im teamplay Receiver gestellt werden. Dadurch können Daten von prominenten bzw. ausgewählten Personen gänzlich ausgenommen werden.

Datensperrung und Datenlöschung

Unmittelbar nach erfolgreichem Upload der minimierten DICOM Dateien werden die originalen Dateien auf dem Receiver durch eine OS-API Call gelöscht. Im Falle, dass ein Patient seine Einwilligung zur Datennutzung widerruft, muss dieser sich an die Daten-erfassende Stelle wenden. Daten eines Patienten sind in teamplay nur dann identifizierbar, wenn der kryptographische Schlüssel im Receiver noch nicht geändert wurde. In dem Fall kann die zugehörige Patienten-ID nur manuell dem kryptographischen Ersatzwert vom Institut in teamplay zugeordnet werden. Über diesen Wert könnten die Datensätze in der Datenbank von einem der DevOps-Administratoren identifiziert werden und dann im Auftrag des Instituts gelöscht werden. Daten werden in teamplay nicht automatisch gelöscht, um langfristige Auswertungen zu ermöglichen. Auf Wunsch des Anwenders oder nach Vertragsende werden hochgeladene DICOM-Daten manuell durch Mitarbeiter der Siemens Healthcare GmbH gelöscht. Mit Vertragsende wird der Account gesperrt und kann nicht mehr aufgerufen werden. Das deaktivierte Benutzerkonto wird gelöscht, wenn es keiner anderen Institution mehr zugeordnet ist.

Auftragsdatenverarbeitung

Siemens Healthcare GmbH ./. Anwender

Die Siemens Healthcare GmbH wird seitens des Anwenders beauftragt mit der Absicherung der Applikation, der Konfiguration der teamplay Plattform und der lokalen Administratoren-Accounts und den damit verbundenen Audit- und Logging-Mechanismen. Ferner wird auf Wunsch des Anwenders die Datenlöschung durchgeführt. Mitarbeiter haben hierfür administrativen Zugang auf die Server über eine VPN-Verbindung des Siemens-Konzern-Netzes in Deutschland. In diesen Fällen liegt eine Auftragsdatenverarbeitung vor. Rechte und Pflichten der Parteien sind im "*Master Service Agreement (MSA) über die Nutzung von teamplay*" geregelt. Das Vertragskonvolut entspricht den gesetzlichen Vorgaben an eine Auftragsdatenverarbeitung in vollem Umfang.

Siemens Healthcare GmbH ./. Siemens Healthcare Private Limited (SHPL)

Der Support für Anwender erfolgt entweder über Mitarbeiter der Siemens Healthcare GmbH in Erlangen, Deutschland oder im Unterauftrag der Siemens Healthcare GmbH über Mitarbeiter der SHPL am Standort in Bangalore, Indien. Innerhalb des Siemens Konzerns wurden für alle Standorte weltweit einheitliche und verbindliche Konzernregelungen zum Datenschutz (BCR, *Binding Corporate Rules for the Protection of Personal Data)* getroffen. Die BCR sind auch nach dem Safe Harbour Urteil des EuGH[4] nicht in Frage gestellt. Ferner haben die Parteien die EU Standardvertragsklauseln für den Transfer personenbezogener Daten inklusive eines Vertrags zur Auftragsdatenverarbeitung abgeschlossen, welche den datenschutzrechtlichen Anforderungen voll entsprechen. Fragen der Zugriffsmöglichkeiten und Rechtsdurchsetzung wurden durch eine Kanzlei bewertet und nicht beanstandet.

Siemens Healthcare GmbH ./. Microsoft

Die Microsoft Ireland Operations Ltd. ist seitens der Siemens Healthcare GmbH unterbeauftragt mit dem sicheren Hosting und Housing der Systemkomponenten der teamplay Plattform inklusive der Systemupdates und Administration der Azure Cloud, der Vergabe von Benutzer Accounts auf der Azure Cloud und den damit verbundenen Audit- und Logging-Mechanismen an den Standorten Dublin bzw. als Backup in Amsterdam. Rechte und Pflichten in Bezug auf Datenschutz und Datensicherheit sind in einem umfangreichen Vertragskonvolut geregelt, welches den gesetzlichen Anforderungen an eine Auftragsdatenverarbeitung voll entspricht. Hierzu wurde auch eine besondere Regelung getroffen, die sicherstellt, dass die mittels der Azure Cloud verarbeiteten Daten bei Microsoft in Europa bleiben und auch aus den Standorten von Microsoft in den USA kein Zugriff ohne Freigabe erfolgen kann.

[4] EuGH, Urteil in der Rechtssache C-362/14 – Maximilian Schrems / Data Protection Commissioner vom 06.10.2015.

Datensicherheit

Die physische Sicherheit der Server wird durch die Sicherheit der Microsoft Rechenzentren gewährleistet, die u.a. durch ein ISO-27001 Zertifikat, sowie durch SOC 1 Type 2 - und SOC 2 Type 2 - Auditierungen von unabhängiger Stelle geprüft und bestätigt worden ist. Die Auditoren hatten Gelegenheit, einen aktuellen Sicherheitsreport im Audit einzusehen. Ferner fand eine Teil-Begehung des Rechenzentrums in Irland statt, welche das hohe Sicherheitsniveau bestätigte.

Bezüglich der Datenschutz- und Datensicherheitsmaßnahmen am Standort der SHPL, Indien, wurden Auszüge aus den Prüfunterlagen zur Informationssicherheit und zum Datenschutz im Rahmen der internen Revision des Siemens Konzerns eingesehen. Für die Vorgänger-Organisation der SHPL lag noch im September 2015 eine Zertifizierung nach ISO 27001:2013 vor, die auf die SHPL bis März 2017 erneuert werden soll. Die Siemens Healthcare GmbH hat mit SHPL zudem eine vertragliche Vereinbarung, welche die in der EU erforderlichen Regelungen der Auftragsdatenverarbeitung vollumfänglich erfüllen.

Der Zugangsschutz administrativer Arbeitsplätze wird über eine Zwei-Faktor-Authentisierung und eine klare Rollen-Trennung sichergestellt. Es gibt nur zwei Administrator Accounts für die Produktiv-Umgebung. Sämtliche Tätigkeiten im Benutzermanagement werden im Audit Log sicher protokolliert. Die logische Sicherheit wird durch ein geeignetes Rollen- und Berechtigungskonzept realisiert sowie durch angemessene Übertragungssicherheit infolge der Verwendung verschlüsselter Kommunikation. Die Verbindung zwischen Receiver und teamplay Server erfolgt über die Microsoft Azure Cloud ausschließlich über HTTPS mit TLS.

Die physische Sicherheit beim Anwender liegt in dessen Verantwortung und ist nicht Bestandteil von teamplay. Das Dokument „*teamplay Datenschutz und –sicherheit Whitepaper*“ sieht vor, wie eine sichere Einsatzumgebung eingerichtet werden soll.

Sensibilisierung der Anwender / Nutzer

Für teamplay liegt eine umfassende Produktdokumentation vor, die transparente und nachhaltige Aspekte zum Datenschutz und zur Datensicherheit enthält Der Anwender wird zudem in den für teamplay veröffentlichten FAQ auf dem Webportal sowie in Anwender-Videos entsprechend sensibilisiert.

Verarbeitung personenbezogener Daten

Bei den primär verarbeiteten personenbezogenen Daten kann zwischen folgenden Patientendaten und Anwender- bzw. Benutzerdaten unterschieden werden:

Patientendaten

--- DICOM-Daten (die vollständige Liste gibt das Dokument „*teamplay Datenschutz und –sicherheit Whitepaper* wieder).

--- In den Pixeldaten der Localizer Images sind Körperumfang sowie innere Strukturen (Organe, Knochen) erkennbar. Offensichtliche medizinische Indikationen könnten daher in den Localizer Images erkennbar sein.

Benutzerdaten

Im Rahmen der Registrierung und Benutzung von teamplay werden Daten des Benutzers und des lokalen Administrators erfasst (geschäftliche E-Mail-Adresse, Vor- und Nachname, geschäftliche Telefonnummer des lokalen Administrators, Passwort, Name der Institution). Diese Daten sind überwiegend geschäftlicher Natur, wobei der Vor- und Nachname einen Beschäftigten der Institution ausweist.

Protokolldaten

Zur Gewährleistung der Services werden verschiedene Logs auf den Systemen erzeugt. Die Inhalte und Speicherfristen sind Bestandteil der Prüfung gewesen und als angemessen bewertet worden.

Abgrenzung des Auditgegenstands

Das Audit von teamplay, Premium Account, umfasst folgende Komponenten:

- --- teamplay Receiver, der als Gateway-Dienst beim Anwender installiert wird
- --- teamplay Plattform mit dem Premium Account und den Modulen Home, Usage, Dose und Protocols.

Nicht evaluiert werden hingegen weitere Angebote oder Produkte der Siemens Healthcare GmbH. Dies umfasst insbesondere das IT-Produkt teamplay für den US-amerikanischen Markt oder andere Märkte außerhalb Europas.

Auch das geplante teamplay-Modul „Images“, das zurzeit nicht zum Produktumfang gehört, ist nicht Gegenstand dieser Prüfung. Bereits aktiv – aber nicht Gegenstand des Audits – sind Funktionalitäten der „Online Community" und "gemeinsamer Nutzung von Daten und Bildern"

Ebenfalls nicht Evaluationsgegenstand ist die Microsoft Azure Cloud oder Komponenten der eingesetzten Rechenzentren.

Darüber hinaus könnten im Zusammenhang mit teamplay separate Fernwartungsdienste notwendig werden. Hierbei wäre dann ein Zugriff auf personenbezogene Daten nicht gänzlich auszuschließen. Diese Fernwartungen sind allerdings immer separat beauftragte Dienste und daher nicht Auditgegenstand.

Nicht Evaluationsgegenstand ist schließlich die Einsatzumgebung des Anwenders inklusive ggf. eingesetzter Tablets, Apps oder Smartphones.

9. Modellierung des Datenflusses

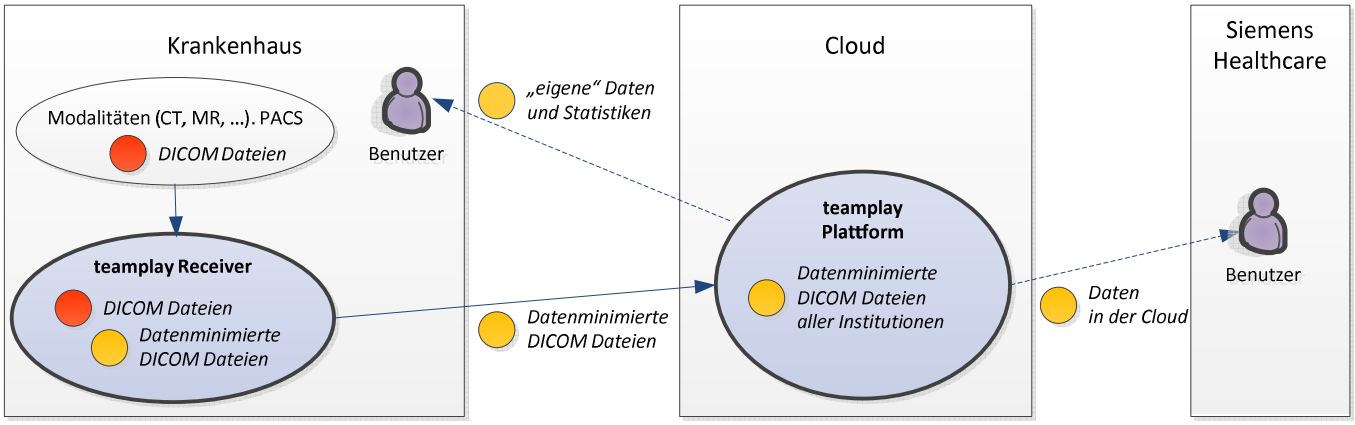

Abbildung 1 Datenfluss zwischen PACS, teamplay Receiver & teamplay Plattform

Die roten Punkte stellen unveränderte DICOM-Daten dar, die gelben Punkte reduzierte bzw. anonymisierte und/oder aggregierte Daten. Der Receiver empfängt vom lokalen PACS DICOM-Daten und reduziert diese. Anschließend werden die reduzierten Daten, bei denen es sich im besten Fall um anonymisierte Daten handelt, an die Server in der Azure Cloud übertragen (unten links, durchgehende Linie/Pfeil). In der Plattform werden die Daten aggregiert und Statistiken über Strahlendosierung und Geräteauslastung erstellt. Diese können vom Anwender über einen Webbrowser abgerufen werden (obere, gestichelte Linie/Pfeil). Siemens Healthcare-Mitarbeiter haben administrativen Zugriff auf Server der Azure Cloud (rechte, gestrichelte Linie/Pfeil), nicht aber auf den Receiver oder das PACS.

10. Version des Anforderungskatalogs

Version 2.

11. Zusammenfassung der Prüfergebnisse

Die Prüfergebnisse im Einzelnen werden wie folgt zusammengefasst:

Nr.	Anforderungen nach Katalog oder sonstigen Rechtsnormen	Bewertung
	A Anforderungsprofil (Primärdaten)	
	Komplex 1	
A1	1.1 Verfügbarkeit, Integrität, Vertraulichkeit	**vorbildlich**
A2	1.2 Nicht-Verkettbarkeit	**adäquat**
A3	1.3 Transparenz	**adäquat**
A4	1.4 Intervenierbarkeit	**adäquat**
A5	1.5 Anpassung des IT-Produkts	**adäquat**
A6	1.6 Privacy by Default	**vorbildlich**
A7	1.7 Sonstige Anforderungen	**n.a.**
	Komplex 2	

A8	2.1 Ermächtigungsgrundlage	**adäquat**
	2.1.1 Gesetzliche Ermächtigung	**adäquat**
	2.1.2 Einwilligung des Betroffenen	**adäquat**
	2.1.3 Besonderheiten i.d. einzelnen Phasen der Datenverarbeitung	**adäquat**
	2.1.3.1 Vorschriften über die Datenerhebung	**adäquat**
	2.1.3.2 Vorschriften über die Übermittlung	**adäquat**
	2.1.3.3 Löschung nach Wegfall des Erfordernisses	**adäquat**
A9	2.2 Einhaltung allg. Datenschutzgrundsätze und Pflichten	**adäquat**
	2.2.1 Zweckbindung und Zweckänderung	**adäquat**
	2.2.2 Erleichterung der Umsetzung des Trennungsgebots	**adäquat**
	2.2.3 Gewährleistung der Datensicherheit	**adäquat, z.T. vorbildlich**
A10	2.3 Datenverarbeitung im Auftrag	**adäquat**
A11	2.4 Voraussetzungen besonderer technischer Verfahren	**n.a.**
	2.4.1 Gemeinsames Verfahren / Abrufverfahren	**n.a.**
	2.4.2 Trennung der Verantwortlichkeiten	**n.a.**
	2.4.3 Veröffentlichungen im Internet	**n.a.**
	2.4.4 Weitere besondere technische Verfahren	**n.a.**
	2.4.1 Gemeinsames Verfahren / Abrufverfahren	**n.a.**
A12	2.5 Sonstige Anforderungen	**n.a.**
	2.5.1 Unterstützung Pseudonymität / Pseudonymisieren	**adäquat**
	Komplex 3	
A13	3.1 Einzelne technisch-organisatorische Maßnahmen	
	3.1.1 Physikalische Sicherung	**vorbildlich**
	3.1.2 Authentisierung	**adäquat**
	3.1.3 Autorisierung	**adäquat**
	3.1.4 Protokollierung	**adäquat**
	3.1.5 Verschlüsselung und Signatur	**adäquat**
	3.1.6 Pseudonymisierung	**adäquat**
	3.1.7 Anonymisierung	**adäquat**
A14	3.2 Allgemeine Pflichten	**adäquat**
	3.2.1 Technisch-Organisatorische Maßnahmen	**vorbildlich**
	3.2.1.1 Verfügbarkeit	**vorbildlich**

	3.2.1.2 Integrität	**adäquat**
	3.2.1.3 Vertraulichkeit	**adäquat**
	3.2.1.4 Nicht-Verkettbarkeit	**adäquat**
	3.2.1.5 Transparenz	**adäquat**
	3.2.1.6 Intervenierbarkeit	**vorbildlich**
	3.2.1.7 Protokollierung von Datenverarbeitungsvorgängen	**adäquat**
	3.2.1.8 Test und Freigabe	**adäquat**
	3.2.2 Erleichterung der Vorabkontrolle	**adäquat**
	3.2.3 Erleichterung der Erstellung von Verfahrensverzeichnissen	**adäquat**
	3.2.4 Benachrichtigungspflicht	**adäquat**
	3.2.5 Unterstützung behördlicher Datenschutzbeauftragter	**adäquat**
A15	3.3 Spezifische Pflichten	**adäquat**
	3.3.1 Verschlüsselung	**adäquat**
	3.3.2 Anonymisierung oder Pseudonymisierung	**adäquat**
	3.3.3 Spezielle Anforderungen bei besonderem Technikeinsatz	**n.a.**
	3.3.3.1 Mobile Datenverarbeitungssysteme	**n.a.**
	3.3.3.2 Video-Überwachung und –Aufzeichnung	**n.a.**
	3.3.3.3 Automatisierte Einzelentscheidungen	**n.a.**
	3.3.3.4 Veröffentlichungen im Internet	**n.a.**
A16	3.4 Pflichten nach DSVO	**adäquat**
A17	3.5 Anforderungen beim Betrieb der Auftragsdatenverarbeitung	**adäquat**
A18	3.6 Sonstige Anforderungen	**n.a.**
	Komplex 4	
A19	4.1Aufklärung und Benachrichtigung	**adäquat**
A20	4.2Benachrichtigung bei unrechtmäßiger Kenntniserlangung	**adäquat**
A21	4.3Auskunft	**adäquat**
A22	4.4 Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegendarstellung	**adäquat**
	4.4.1 Berichtigung	**adäquat**
	4.4.2 Vollständige Löschung	**adäquat**
	4.4.3 Sperrung	**adäquat**
	4.4.4 Einwand bzw. Widerspruch gegen die Verarbeitung	**adäquat**
	4.4.5 Gegendarstellung	**n.a.**

A23	4.5 Sonstige Anforderungen	**n.a.**
	B Anforderungsprofil (Sekundärdaten)	
	Komplex 1	
B1	1.1 Datenvermeidung und Datensparsamkeit	**adäquat**
B2	1.2 Zweckbindung	**adäquat**
B3	1.3 Nicht-Verkettbarkeit	**adäquat**
B4	1.4 Transparenz	**adäquat**
	1.5 Sonstige Anforderungen	**n.a.**
	Komplex 2	
B5	2.1 Rechtsgrundlagen	**adäquat**
B6	2.2 Zweckbindung	**adäquat**
B7	2.3 Aufbewahrungsfristen und Löschung	**adäquat**
	2.4 Sonstige Anforderungen	**n.a.**
	Komplex 3	
B8	3.1 Physikalische Sicherung	**vorbildlich**
B9	3.2 Zugriffsschutz	**adäquat**
B10	3.3 Ermittlung / Informationsgehalt	**adäquat**
	3.4 Sichtbarkeit der Protokolldaten	**adäquat**
B11	3.5 Technische Umsetzung der Speicherfristen	**adäquat**
B12	3.6 Unzulässige Verkettung	**adäquat**
B13	3.7 Beschreibung der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit	**adäquat**
	Sonstige Anforderungen	**n.a.**
	Komplex 4	
B14	4.1 Selektive Löschung von Einzeldaten	**adäquat**
	4.2 Beauskunftung	**adäquat**
	4.3 Berichtigung	**adäquat**
	4.4 Sperrung	**adäquat**
	4.5 Einwand	**n.a.**

n.a. = nicht anwendbar

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

teamplay fördert den Datenschutz auf vielfältige Weise. Hervorzuheben sind insbesondere die entwickelten Maßnahmen zur Datenminimierung, Datenvermeidung sowie zur Pseudonymisierung und Anonymisierung von Patientendaten. Die seitens der Siemens Healthcare GmbH entwickelten und umgesetzten Datenschutz- und Sicherheitsmaßnahmen entsprechen vorbildlich dem Privacy-by-Design Grundsatz.

Ferner sind die im unterbeauftragten Rechenzentrum getroffenen technischen und organisatorischen Datensicherheitsmaßnahmen vorbildlich und gehen über durchschnittliche Standards hinaus.

13. Votum der Auditoren

teamplay erfüllt die Anforderungen an den Datenschutz und die Datensicherheit in vollem Umfang.

Bremen, den 06.10.2016.

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

Ralf von Rahden
datenschutz cert GmbH