Kurzgutachten zur Erteilung eines Datenschutz-Gütesiegels für „Codira PACS 9.1“

im Auftrag der Codira GmbH

datenschutz cert GmbH

11.05.2012

datenschutz cert

Inhaltsverzeichnis

Dokumentenhistorie

Version	Datum	geänderte Kapitel	Grund der Änderung	geändert durch
1.0	11.05.2012	alle	Finalisierung	Dr. Irene Karper, Dipl. Math. Ralf von Rahden

1. Über die Auditierung von Codira PACS 9.1

Mit diesem Kurzgutachten werden die Ergebnisse der datenschutzrechtlichen und IT-sicherheitstechnischen Auditierung von „Codira PACS“ in der Version 9.1 dokumentiert, mit welcher die datenschutz cert GmbH seitens der Codira GmbH beauftragt wurde.

Das Produkt Codira PACS ist ein digitales Bildarchiv- und Kommunikationssystem für radiologische Bilddaten.

Die Prüfung wurde anhand des Standards des Datenschutz-Gütesiegels gemäß der Schleswig-Holsteinischen Landesverordnung über ein Datenschutzaudit (DSAVO)[1] durchgeführt. Grundlage für die Erstellung dieses Kurzgutachtens gemäß DSAVO ist die Version 1.2 des Anforderungskatalogs für ein Datenschutz-Gütesiegel des ULD.

Im Ergebnis stellen die Auditoren fest, dass Codira PACS in der Version 9.1 konform zu den gesetzlichen Anforderungen an den Datenschutz und die Datensicherheit eingesetzt werden kann und dass Codira PACS in der Version 9.1 in besonderem Maße den Datenschutz beim Anwender fördert.

2. Antragstellerin

Antragstellerin der Auditierung und Zertifizierung gemäß DSAVO ist die

Codira GmbH
Prüner Gang 16-20
24103 Kiel.

als Hersteller des IT-Produkts Codira PACS 9.1.

Ansprechpartner sind Herr Dr. Johannes Hezel und Herr Bert Meemann.

3. Sachverständige Prüfstelle

Sachverständige Prüfstelle gemäß DSAVO ist die

datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen
Tel.: 0421-696632-50
E-Mail: office@datenschutz-cert.de
Web: www.datenschutz-cert.de

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

[1] Landesverordnung über ein Datenschutzaudit (Datenschutzauditverordnung - DSAVO) v. 18.11.2009, *GVOBl.* Schl.-H. *2008, S. 562ff. / GVOBl.* Schl.-H. *2009, S. 742ff.*

4. Zeitraum der Auditierung

Die Auditierung erstreckte sich auf den Zeitraum von 23.05.2011 bis 11.05.2012 und beinhaltete eine konzeptionelle Analyse der zur Verfügung gestellten Unterlagen sowie verschiedene Besichtigungen des Testsystems. Darüber hinaus ist der Authentifikationsvorgang praktisch getestet worden.

5. Kurzbezeichnung des IT-Produkts

Auditiert wurde das Produkt „Codira PACS“ in der Version 9.1, nachfolgend kurz als „Codira PACS“ bezeichnet.[2]

6. Zweck, Einsatzbereich, Komponenten

Codira PACS ist ein digitales Bildarchiv- und Kommunikationssystem für radiologische Bilddaten. Es realisiert einen Workflow zwischen Radiologen und dem Überweiser bzw. dem Arzt der Behandlungskette (Anwender).

Das digitale Archiv von Codira PACS übernimmt die Bilddaten von der lokalen Medizintechnik, entweder aus einem PACS (Picture Archiving and Communication System) oder einem Radiologieinformationssystem (RIS) und archiviert sie auf Bandlaufwerken. Als Kommunikationsplattform authentisiert und verwaltet Codira PACS die Benutzer und bietet die Möglichkeit, Bilddaten patientenbezogen Überweisern oder anderen konsultierten Ärzten der Behandlungskette sowie der bildgebenden Radiologie wieder zugänglich zu machen.

6.1.1 DICOM-Datensätze

Codira PACS und die jeweilige lokale Medizintechnik kommunizieren über den sogenannten DICOM-Standard („Digital Imaging and Communications in Medicine“) miteinander. DICOM ist ein international anerkannter Standard für die Radiologie zum Austausch von Bildern und Daten von unterschiedlichen bildgebenden und bildverarbeitenden Geräten. Ein Datensatz besteht aus den sog. DICOM-Tags und den DICOM-Bilddaten.

Die DICOM-Tags sind Metadaten und enthalten Patienten-, Behandlungs- und Gerätedaten („Patientendatencontainer“). Je nach System können hieraus alle oder nur bestimmte DICOM-Tags genutzt werden. Der standardmäßig vorgegebene Datensatz wird in der Regel vom Radiologen nicht vollständig ausgefüllt.

DICOM-Bilddaten enthalten das eigentliche Bild, einen pseudonymisierten Datensatz der DICOM-Tags, sowie eine vom bildgebenden Radiologen vergebene Patienten-ID. Dabei weist die Codira GmbH den Radiologen ausdrücklich darauf hin, dass die Patienten-ID keine „sprechende“ Nummer sein darf, um die Pseudonymisierung aufrecht zu erhalten.

DICOM-Tags und DICOM-Bilddaten können in unterschiedlichen Daten-Containern im lokalen bildgebenden System abgelegt werden. Dadurch findet eine Datentrennung statt. Sollten es nicht möglich sein, Bilddaten und Patientendaten zu

[2] Die Beschreibung Codira oder Codira PACS bezieht sich nachfolgend auf das Produkt. Soweit der Hersteller gemeint ist, wird dieser als „Codira GmbH“ bezeichnet.

trennen, wird der gesamte DICOM-Datensatz mit einem Untersuchungsschlüssel verschlüsselt im Langzeitarchiv gespeichert und steht nicht auf der Kommunikationsplattform zur Verfügung. Über die in beiden Containern gespeicherte, vom bildgebenden System zufällig erzeugte DICOM-UID (SOPClassUID) kann wieder eine Zusammenführung erfolgen.

Folgende Abbildung 1 verdeutlicht die Bestandteile eines DICOM-Datensatzes:

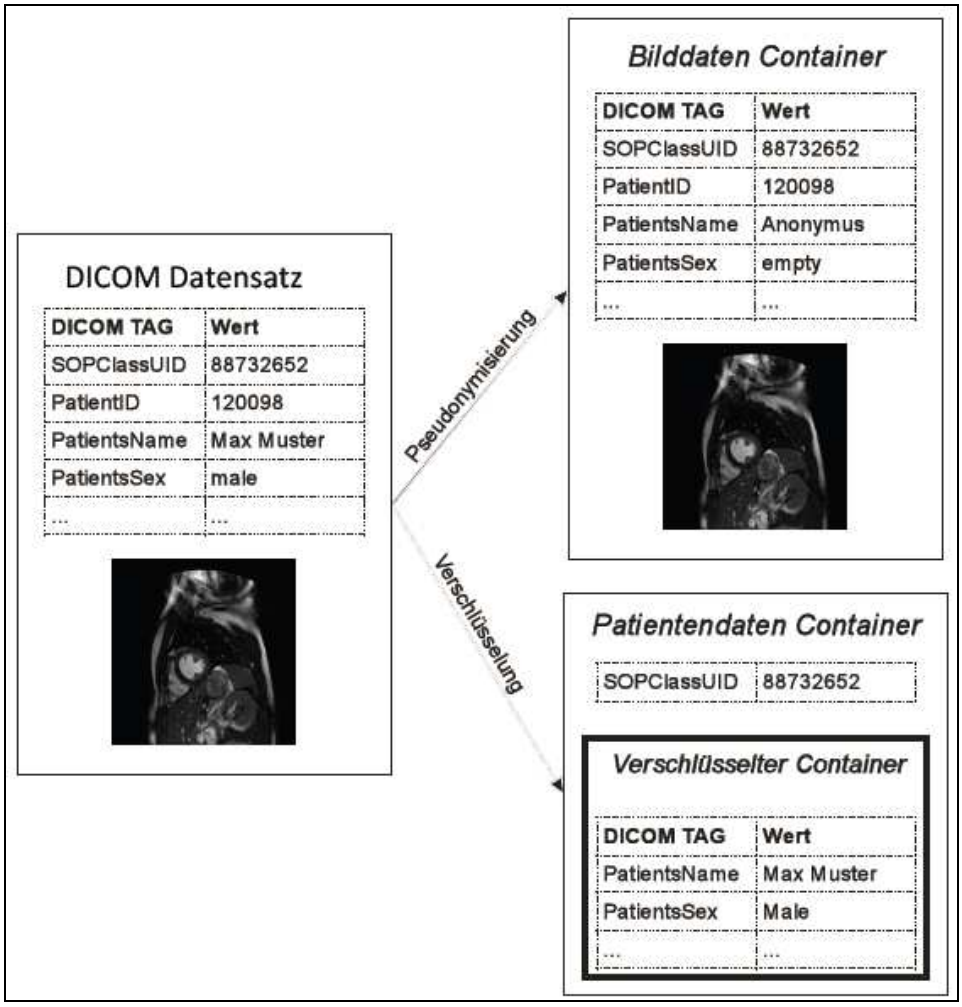

Abbildung 1 DICOM-Datensatz

6.1.2 SuperPACS

Zentrale Komponente von Codira PACS ist das SuperPACS als eigentliches Archiv. Es speichert Daten, welche es von der bildgebenden Radiologie erhält, und stellt diese bei Freigabe zur Verteilung an Überweiser bzw. Ärzte der Behandlungskette zur Verfügung. Das SuperPACS wird in einem Rechenzentrum der T-Systems in Frankfurt am Main, Deutschland, gehostet.

6.1.3 Satellite Workflow Manager

Lokal innerhalb der bildgebenden Radiologie wird der Satellite Workflow Manager (sWfM) installiert. Der sWfM ist ein Gateway-Rechner. Er übernimmt die DICOM-Daten aus dem lokalen Radiologiesystem und teilt sie in einen Bilddatensatz und

einen Patientendatensatz auf. Ersterer wird im sWfM pseudonymisiert, letzterer im sWfM mit einem für die Untersuchung individuellen Studienschlüssel verschlüsselt. Der Studienschlüssel ist wiederum mit dem Site-Schlüssel verschlüsselt und im SuperPACS abgelegt. Der Patientendatensatz kann nur auf dem sWfM entschlüsselt werden, der ihm zugeordnet ist, da nur dieser über den entsprechenden Site-Schlüssel verfügt. Anschließend werden beide Datensätze über eine mit LineCrypt gesicherte VPN-Verbindung ans SuperPACS gesendet.

Werden Daten aus dem Archiv abgerufen, werden diese über den sWfM übermittelt und wieder entschlüsselt. Für die Authentisierung gegenüber dem SuperPACS und zur verschlüsselten Kommunikation wird das chipkartenbasierte Produkt T-TeleSec LineCrypt L (RSA 1024 bit und IDEA 128 bit) verwendet. Es realisiert Verschlüsselung, Schlüsselaustausch und Authentifizierung der Verbindung.

SuperPACS und sWfM basieren auf dem Produkt Carestream PACS in der Version 11.

6.1.4 Anbindung der Anwender

Überweiser/Ärzte der Behandlungskette können über das Internet per SSL-Verbindung auf die für sie bestimmten Daten im Archiv zugreifen. Der Zugriff erfolgt über den *Carestream Client*. Die Authentisierung erfolgt per One-Time-Passwort. Die Internetkommunikation zwischen dem Client und dem SuperPACS erfolgt per SSL (RC4 mit 128bit). Der Webserver des SuperPACS authentisiert sich durch ein SSL-Zertifikat/SHA-1 mit RSA Verschlüsselung (2048bit) gegenüber dem Client.

6.1.5 Revisionskontrolle durch das Carestream Audit Trail Tool

Änderungen und Löschvorgänge von Daten werden von dem sWfM an das SuperPACS weitergegeben. Zur Systemüberwachung werden Zugriffsdaten im Carestream Audit Trail Tool protokolliert und pseudonymisiert gespeichert.

6.1.6 Datenpflege und Datenlöschung

Der Anwender von Codira PACS ist selbst für die Pflege der Datensätze zuständig. DICOM-Daten, Datenbankdaten und Anwendungsprotokolle werden für maximal 30 Jahre im Langzeitarchiv von Codira PACS aufbewahrt. Einzelne Datensätze werden aus dem Codira PACS-System auf Anfrage entfernt bzw. gelöscht.

6.1.7 Auftragsdatenverarbeitung

Die Codira GmbH übernimmt im Auftrag der Anwender von Codira PACS administrative Tätigkeiten (Einrichtung der User-Accounts, Überwachung der Speicherkapazität von Festplatten, Datenbank und Bandlaufwerken, Desaster Recovery, Kontrolle der Log-Files) und wird insofern als Auftragsdatenverarbeiter tätig. Leistungen werden dabei immer durch den Anwender veranlasst und kontrolliert.

Die Carestream Health Deutschland GmbH übernimmt im Unterauftrag für die Codira GmbH den 2nd level support (Installation, Wartung, Updates, Einrichtung der sWfM). Auch hier werden die Leistungen immer durch den Anwender veranlasst und kontrolliert.

Die Codira PACS-Server, auf denen sich ausschließlich verschlüsselte Daten befinden, werden im Auftrag der Codira GmbH in einem ISO27001-zertifizierten Rechenzentrum bei der Deutsche Telekom AG (T-Systems) gehostet.

Die phexnet UG übernimmt für die Codira GmbH die technische Aktivierung, Einrichtung sowie Wartung der TeleSec OneTimePass Token. Hierbei erhält die phexnet UG allerdings keinerlei patientenbeziehbare Daten.

In allen aufgeführten Dienstleistungsverhältnissen liegen schriftliche Regelungen zur Auftragsdatenverarbeitung vor. Ein Zugriff auf ent-pseudonymisierte Datensätze ist dabei nur im Einzelfall bei Wartungsarbeiten im Auftrag des verantwortlichen Anwenders möglich. Es gibt zwei Szenarien für diese Einzelfälle:

1.: Der Kunde wünscht ausdrücklich einen solchen Zugriff durch die Codira GmbH und/oder die Carestream Health Deutschland GmbH.

2:. Die Codira GmbH führt im Auftrag des Kunden ein Desaster Recovery durch.

Beide Fälle sind im Mustervertrag der Codira GmbH mit dem Kunden in § 12 Abs. 3 beschrieben. Darin verpflichtet sich einerseits die Codira GmbH, die Wartungsarbeiten möglichst so durchzuführen, dass keine personenbezogenen Daten wahrgenommen werden. Andererseits wird der verantwortliche Arzt darauf hingewiesen und vertraglich verpflichtet, eine Entbindung von der Schweigepflicht für diese Fälle einzuholen.

7. Modellierung des Datenflusses

Der Datenfluss innerhalb des Codira PACS-Netzwerks wird in der nachfolgenden Abbildung verdeutlicht:

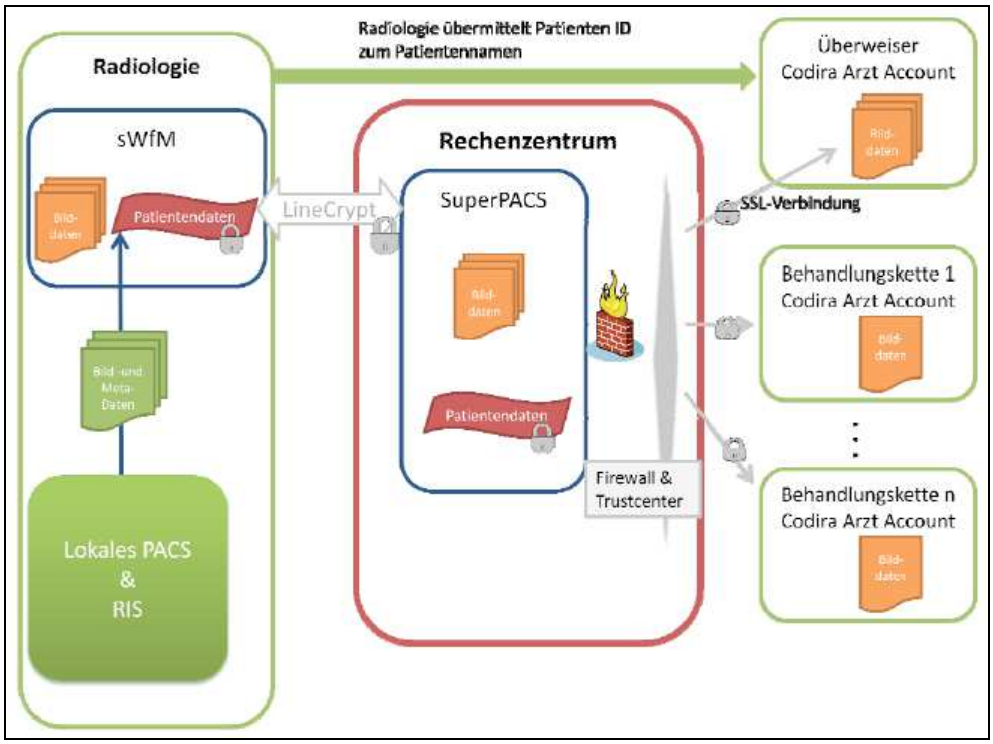

Abbildung 2 Datenfluss bei Codira PACS

Zusammengefasst werden folgende Datenarten mittels Codira PACS verarbeitet:

Primärdaten:

--- DICOM-Daten (Bilddaten und DICOM-Tags)

--- Patienten-ID.

Sekundärdaten:

--- Protokolldaten des Audit-Tools

--- Codira PACS-ID + zeitliche Zugriffsdaten des Anwenders.

8. Abgrenzung des Auditgegenstands

Diese Auditierung des Produkts Codira PACS umfasst folgende Komponenten:

--- Zentraler Workflow-Manager (SuperPACS)

--- Satellit Workflow-Manager (sWfM)

--- Carestream Client über https als Schnittstelle für den Zugriff auf das Kommunikationsportal

--- Zertifikatsmanagement

--- Benutzerverwaltung inklusive Audit-Tool.

Nicht auditiert wird hingegen das lokale PACS oder RIS beim angebundenen Radiologen sowie das Rechenzentrum, in welchem die Codira PACS-Systeme gehostet werden. Ebenfalls nicht auditiert werden das Verschlüsselungsprodukt T-TeleSec LineCrypt L, das verwendete SSL-Protokoll, Java Runtime Environment, der Firewall einschließlich Intrusion Detection System, die Server-Betriebssysteme, die Oracle Datenbank einschließlich Datenbank-Verschlüsselung sowie die Backup-Mechanismen.

Auf diese Komponenten wird aber Bezug genommen, sofern sie für die Gewährleistung technisch-organisatorischer Sicherheitsmaßnahmen oder zur rechtlichen Bewertung des Produkts Codira PACS von Bedeutung sind. Dabei werden vorhandene Zertifikate, beispielsweise für das Verschlüsselungsverfahren LineCrypt oder das ISO 27001 -Zertifikate des Rechenzentrums zu berücksichtigen sein.

9. Herausragende Prüfergebnisse

Im Rahmen der Auditierung konnten folgende herausragende Prüfergebnisse festgestellt werden:

9.1 Umsetzung von rechtlichen Anforderungen

Für die Auditierung waren u.a. die Vorgaben der Datenschutzauditverordnung Schleswig-Holstein (DSAVO), des Landesdatenschutzgesetzes Schleswig-Holstein (LDSG S-H)[3], der Datenschutzverordnung (DSVO)[4], das Bundesdatenschutzgesetz

[3] Landesdatenschutzgesetz - LDSG - Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen v. 27.01.2012, GVBl. Schl.-H. 1/2012, S. 78 ff. u. 89 ff.

[4] Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten v. 09. 1 2008 , GVOBl Schl.-H. 2008, S. 841ff.

(BDSG)[5] sowie bereichsspezifische Bestimmungen des Gesundheitswesens anzuwenden. Etwa besteht eine Pflicht zur Aufbewahrung von Patientendaten gemäß § 10 der Musterberufsordnung (MBO)[6] bzw. gemäß der gleichlautenden Berufsordnung für Ärzte des Landes Schleswig-Holstein. Für Röntgenbilder gilt zudem § 28 der Röntgenverordnung (RöntgenVO)[7]. Im Vordergrund steht dabei die Wahrung des Patientendatenschutzes. Er wird durch § 203 Strafgesetzbuch (StGB)[8] und § 9 MBO dargelegt und geschützt. Ferner ist in diesem Zusammenhang ein Beschlagnahmeschutz gemäß § 97 der Strafprozessordnung (StPO)[9] zu gewähren.

Für Codira PACS wurden zudem die Vorgaben der „Orientierungshilfe Krankenhausinformationssysteme“ (OH-KIS) der Unterarbeitsgruppe Krankenhausinformationssysteme der Arbeitskreise Gesundheit und Soziales sowie Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder[10] betrachtet. Da Codira PACS allerdings lediglich ein Subsystem eines KIS darstellt, wurden die für den Hersteller obligatorischen Regelungen der OH KIS nur als anwendbar betrachtet, soweit sich diese nicht auf die reine elektronische Patientenakte beziehen.

Codira PACS trägt den verschiedenen datenschutzrechtlichen Anforderungen durch die beschriebenen Mechanismen der Pseudonymisierung und Verschlüsselung in vollem Umfang Rechnung. Die Einhaltung der ärztlichen Schweigepflicht wird insbesondere dadurch umgesetzt, dass die DICOM-tags innerhalb des Codira PACS-Systems pseudonymisiert gespeichert werden. Der verbleibende DICOM-Datensatz enthält aufgrund der Löschung bestimmter DICOM-tags keine personenbeziehbaren Daten mehr. Lediglich die Patienten-ID ermöglicht es dem behandelnden Arzt, die Daten wieder einem Patienten zuzuordnen. Dritte, die nicht ausdrücklich durch den behandelnden Arzt für eine Freigabe der Patienten-ID vorgesehen sind, können die mittels Codira PACS verarbeiteten Daten keiner betroffenen Person zuordnen. Da Ärzte, die in Praxisgemeinschaften zusammengeschlossen sind, jeweils eine andere Codira PACS-ID zugewiesen wird, ist ferner garantiert, dass die ärztliche Schweigepflicht auch gegenüber Ärzten gewahrt wird, die nicht an der Behandlung beteiligt sind.

Die Verarbeitung der pseudonymen Patientendaten kann auf § 11 LDSG S-H bzw. § 28 Abs. BDSG gestützt werden. Denn die Datenverarbeitung durch Codira PACS basiert auf dem Behandlungsverhältnis und ist insofern vertraglich begründet. Ferner trägt die Verarbeitung radiologischer Bilddaten und deren Kommunikation dazu bei, ggf. lebenswichtige Interessen des Patienten zu wahren.

Da die Zuordnungsfunktion im Pseudonymisierungskonzept von Codira PACS ausschließlich bei der bildgebenden Radiologie als „Herrin“ der Daten liegt, können

---

[5] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung v. 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 des Gesetzes v. 14.08.2009 (BGBl. I S. 2814).
[6] MBO-Ä 1997 in der Fassung der Beschlüsse des 114. Deutschen Ärztetages 2011 in Kiel.
[7] Röntgenverordnung in der Fassung der Bekanntmachung v. 30.04.2003 (BGBl. I S. 604).
[8] Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 4 des Gesetzes v. 23.06. 2011 (BGBl. I S. 1266)
[9] Strafprozessordnung in der Fassung der Bekanntmachung v. 07.04.1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Art. 5 des Gesetzes v. 23.06.2011 (BGBl. I S. 1266).
[10] Z.B. Abrufbar unter http://www.datenschutz.hessen.de/download.php?download_ID=229 (Stand 05/2012).

insgesamt alle Anforderungen in vollem Umfang erfüllt werden. Ein Zugriff auf entpseudonymisierte Datensätze durch die Codira GmbH bzw. durch die von ihr Unterbeauftragte Carestream Health Deutschland GmbH wäre nur im Einzelfall bei Wartungsarbeiten im Auftrag der verantwortlichen Stelle möglich. Die oben hierfür beschriebenen Fälle sind im Mustervertrag der Codira GmbH mit dem Kunden in § 12 Abs. 3 als Wartungsarbeiten beschrieben. Darin verpflichtet sich einerseits die Codira GmbH, die Wartungsarbeiten möglichst so durchzuführen, dass keine personenbezogenen Daten wahrgenommen werden. Andererseits wird der verantwortliche Arzt darauf hingewiesen und vertraglich verpflichtet, eine Entbindung von der Schweigepflicht für diese Fälle einzuholen. Zudem werden die der Codira GmbH obliegenden Pflichten per Vertrag zwischen der Codira GmbH und der Carestream Health Deutschland GmbH an alle Subunternehmer weitergegeben.

Die Verarbeitung der Sekundärdaten ist ebenfalls zulässig. Sie beruht auf der ordnungsgemäßen Erfüllung der Auftragsdatenverarbeitung durch die Codira GmbH und stützt sich damit auf eine vertragliche Grundlage.

9.2 Datensparsamkeit

Aspekte der Datensparsamkeit werden im vollen Umfang erfüllt, indem mittels Codira PACS nur solche Daten verarbeitet werden, die für die ärztliche Leistung gegenüber dem Patienten erforderlich sind. Dabei kann das System so eingerichtet werden, dass nur DICOM-Tags genutzt werden, die für die Behandlung zwingend erforderlich sind. Ferner unterstützen die Pseudonymisierungs-Mechanismen hinsichtlich der DICOM-Daten und der Patienten-ID den datensparsamen Umgang. Die zusätzliche Verschlüsselung der Daten sorgt für einen engen Kreis der Zugriffsberechtigten auf die relevanten Datensätze.

9.3 Löschen, Pseudonymisieren

Für radiologische Bilddaten besteht nach §28 RöntgenVO eine 10 jährige Aufbewahrungspflicht, für die Aufzeichnungen der Röntgenbehandlung bis zu 30 Jahre. Die Radiologie als Anwender von Codira PACS ist verantwortlich, diese rechtlichen Fristen einzuhalten. Codira PACS unterstützt dies, indem eine Speicherung über den gesamten Zeitraum sichergestellt wird.

Logdateien von Anwendern werden für 90 Tage gespeichert und nach dem Prinzip „First in, first out“ gelöscht. Access-Logs von Administratoren der Codira GmbH werden aus Gründen der Revisionssicherheit nicht gelöscht.

Aspekte der Pseudonymisierung sind durch die beschriebenen Mechanismen ebenfalls angemessen umgesetzt.

9.4 Datensicherheit

Mit Hilfe des verwendeten Verschlüsselungs-Systems ist sichergestellt, dass nur der jeweilige Radiologe auf die Patientendaten Zugriff hat. Darüber hinaus ist der Zugriff auf die Kommunikationsplattform über eine 2-Faktor-Authentisierung gesichert.

Die Systeme des SuperPACS werden in einem nach ISO 27001 zertifizierten Rechenzentrum betrieben, und die Kommunikationsverbindungen zu den radiologischen Praxen sind über LineCrypt L gesichert.

Maßnahmen zur Datensicherheit sind daher insgesamt vorbildlich umgesetzt.

9.5 Umsetzung der Betroffenenrechte

Da medizinische Daten pseudonymisiert bzw. verschlüsselt archiviert werden, kann nur der auftraggebende Radiologe bzw. der Überweiser Auskünfte über Patientendaten geben oder für die Gewährleistung der Löschfristen oder Datensperrung sorgen.

Codira PACS fördert die Rechte des Betroffenen, indem die dem Anwender ausgehändigten Dokumentationen die Datenverarbeitungsvorgänge und Verantwortlichkeiten in leicht verständlicher Form beschreiben und dadurch eine Vorabkontrolle oder die Erstellung des Verfahrensregisters erleichtern. Auch ist es möglich, anhand der in Codira PACS genutzten DICOM-Tags und der Patienten-ID eine Liste zu erzeugen, die Auskunft über die Speicherung von Daten gibt. Dadurch wird die Tätigkeit des Datenschutzbeauftragten bei Auskunftsersuchen oder Beschwerden unterstützt. Der Codira PACS-Kunde wird im Benutzerhandbuch sowie im Rahmen der Schulung durch die Codira GmbH auf die Löschfunktionen hingewiesen und somit sensibilisiert. Auf expliziten Wunsch können Daten im Archiv von Codira PACS zudem jederzeit gelöscht werden. Schließlich sind die Codira GmbH sowie deren Subunternehmer vertraglich verpflichtet, den Kunden bei der Umsetzung von Betroffenenrechten zu unterstützen.

10. Gesamtbewertung

Gemäß dem Anforderungskatalog für ein Datenschutz-Gütesiegel in der Version 1.2 konnten die Auditoren folgende Bewertungen treffen:

Nr.	Anforderungsprofil	Bewertung / Kommentar
Datenart A (Primärdaten):		
A1	Datensparsamkeit	Vorbildlich
A2	Löschen, Anonymisieren, Pseudonymisieren	Angemessen
A3	Transparenz	Angemessen
A4	Sonstige Anforderungen	Angemessen
A5	Zulässigkeit	Angemessen
A6	Datenschutzgrundsätze	Angemessen
A7	Auftragsdatenverarbeitung	Verbesserungsfähig
A8	Besondere technischer Verfahren	Nicht anwendbar
A9	Sonstige Anforderungen	Angemessen
A10	Zugangskontrolle	Angemessen
A11	Zutritts- und Zugriffskontrolle	Angemessen
A12	Protokollierung	Angemessen
A13	Weitere technisch-organisatorische	Angemessen

	Maßnahmen	
A14	Vorabkontrolle, Verfahrensverzeichnisses Datenschutzbeauftragter	Angemessen
A15	Spezifische Pflichten	Nicht anwendbar
A16	Pflichten nach DSVO	Angemessen
A17	Sonstige spezifische Anforderungen	Nicht anwendbar
A18	Betroffenenrechte	Angemessen
A19	Sonstige Anforderungen	Angemessen
Datenart B (Sekundärdaten):		
B1	Datensparsamkeit	Angemessen
B2	Löschen, Anonymisieren, Pseudonymisieren	Angemessen
B3	Transparenz	Angemessen
B4	Sonstige Anforderungen	Nicht anwendbar
B5	Zulässigkeit	Angemessen
B6	Datenschutzgrundsätze	Angemessen
B7	Auftragsdatenverarbeitung	Verbesserungsfähig
B8	Besondere technischer Verfahren	Nicht anwendbar
B9	Sonstige Anforderungen	Nicht anwendbar
B10	Zugangskontrolle	Angemessen
B11	Zutritts- und Zugriffskontrolle	Angemessen
B12	Protokollierung	Nicht anwendbar
B13	Weitere technisch-organisatorische Maßnahmen	Nicht anwendbar
B14	Vorabkontrolle, Verfahrensverzeichnisses Datenschutzbeauftragter	Angemessen
B15	Spezifische Pflichten	Nicht anwendbar
B16	Pflichten nach DSVO	Angemessen
B17	Sonstige spezifische Anforderungen	Nicht anwendbar
B18	Betroffenenrechte	Angemessen
B19	Sonstige Anforderungen	Nicht anwendbar

11. Förderung des Datenschutzes

Das IT-Produkt fördert den Datenschutz auf vielfältige Weise:

--- Der Hersteller hat ein besonderes Schlüsselmanagement und ein besonderes Pseudonymisierungskonzept erarbeitet, welches die Offenbarung von Patientengeheimnissen an Unbefugte angemessen verhindern kann. Dieses Konzept ermöglicht zudem eine unkomplizierte Zusammenarbeit zwischen Radiologe und Überweiser durch Freigabe pseudonymisierter Bilddaten.

--- Bereits im Rahmen der Entwicklung von Codira PACS wurden Aspekte des Datenschutzes und der Datensicherheit insbesondere vor dem Hintergrund des besonderen Schutzbedarfs von Patientendaten berücksichtigt und flossen in das Gesamtkonzept ein, insbesondere in das Verschlüsselungskonzept und Schlüsselmanagement.

--- Es werden starke Authentisierungsmechanismen auf Basis einer 2-Faktor-Authentisierung der Anwender eingesetzt.

12. Votum der Auditoren

Das IT-Produkt Codira PACS, Version 9.1, setzt insgesamt die Anforderungen an den Datenschutz angemessen um.

Die Auditoren empfehlen die Gütesiegelvergabe

Bremen, den 11.05.2012.

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

Ralf von Rahden
datenschutz cert GmbH