Kurzgutachten zum Datenschutz-Gütesiegel gemäß Datenschutzgütesiegelverordnung Schleswig-Holstein für das IT-Produkt „Chronic Care Application - CCA, Version 1.23“

im Auftrag der AstraZeneca GmbH

datenschutz cert GmbH

23. März 2015

datenschutz cert

Inhaltsverzeichnis

1. Über dieses Kurzgutachten

Mit diesem Kurzgutachten werden die Ergebnisse der datenschutzrechtlichen und IT-sicherheitstechnischen Auditierung der „Chronic Care Application - CCA“ in der Version 1.23 anhand der Datenschutzgütesiegelverordnung (DSGSVO) Schleswig-Holsteins[1] zusammengefasst.

2. Zeitraum der Prüfung

Die Begutachtung erfolgte vom 06.12.2013 bis 23.03.2015 und beinhaltete eine konzeptionelle Analyse der zur Verfügung gestellten Unterlagen, Besichtigungen des Systems und Tests des Authentisierungsvorgangs.

3. Antragstellerin

Antragstellerin des Datenschutz-Gütesiegels ist die

AstraZeneca GmbH
Tinsdaler Weg 183,
22880 Wedel

Ansprechpartner ist Herr Burkardt Tonagel.

Die CCA wurde im Auftrag der AstraZeneca GmbH durch die dr. heydenreich GmbH entwickelt. Herr Dr. Heydenreich, Geschäftsführer der dr. heydenreich GmbH, hat dieses Audit maßgeblich unterstützt.

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 Dr. Irene Karper (Recht). Ansprechpartner für diese Begutachtung sind Frau Dr. Irene Karper (Recht) und Herr Ralf von Rahden (Technik).

5. Kurzbezeichnung des IT-Produkts

Begutachtet wird das Produkt „Chronic Care Application - CCA“ in der Version 1.23, nachfolgend auch kurz als „CCA“ bezeichnet.

6. Beschreibung des IT-Produkts

Die CCA ist eine Server-basierte Web-Anwendung zur Unterstützung der medizinischen Patientenversorgung, welche unter chronischen Erkrankungen leiden, insbesondere dem Akuten Coronarsyndrom (ACS). Die CCA wird dabei im Rahmen von Selektivverträgen genutzt und übernimmt für Ärzte Steuerungs- und

[1] Landesverordnung über ein Datenschutzgütesiegel (Datenschutzgütesiegelverordnung – DSGSVO) v. 30.11.2013, *GVOBl.* Schl.-H. 2013, S.536ff. Konkretisiert wird die DSGSVO durch den Anforderungskatalog des ULD, der zum Zeitpunkt des Audits in der Version 1.2 vorlag. Die Kriterien sind abrufbar unter https://www.datenschutzzentrum.de/uploads/guetesiegel/guetesiegel-anforderungskatalog.pdf. Stand dieser und weiterer hier zitierter Webseiten ist März 2015.

Kommunikationsaufgaben bei der Behandlung. Typischer Anwendungsfall der CCA ist eine Arztpraxis oder ein Ärztenetz, in denen die CCA als Ergänzung zum Arztinformationssystem (AIS) installiert ist.

Haus- und Fachärzte übertragen medizinische Informationen im Rahmen einer Behandlung und mit schriftlichem Einverständnis der Patienten manuell oder aus dem AIS in die CCA. Die Informationen werden mittels der CCA gegen wissenschaftlich geprüfte und z.B. von der Bundesärztekammer empfohlene Behandlungshinweise (Leitlinien für Ärzte) geprüft. Das Ergebnis des Abgleichs bildet dann eine Entscheidungshilfe für die weitere Behandlung durch den Arzt.

Verantwortliche Stelle ist der behandelnde Arzt. Er und die in seinem Umfeld tätigen Personen, welche die CCA nutzen, werden nachfolgend Anwender genannt.

Die CCA wurde im Auftrag der AstraZeneca GmbH durch die dr. heydenreich GmbH entwickelt. Die medizinischen Inhalte wurden durch die sgh-consulting realisiert.

Der Anwender führt die Installation der CCA sowie ggf. spätere Updates eigenständig in seiner IT-Umgebung durch. Dadurch haben weder die AstraZeneca GmbH noch die dr. heydenreich GmbH oder die sgh-consulting Zugriff auf die CCA und sind daher *keine* Auftragsdatenverarbeiter i.S.d. § 11 BDSG bzw. § 17 LDSG SH.

Die CCA kann z.B. von Ärzten in öffentlich-rechtlich organisierten Krankenhäusern in Schleswig-Holstein genutzt werden. Die CCA ist damit auditierbar nach DSGSVO. **Hervorzuheben ist, dass im Rahmen dieses Audits nicht untersucht wurde, ob die CCA konform zum Medizinproduktegesetz aufgestellt ist.**

7. Tools, die zur Herstellung des Produkts verwendet wurden

Keine.

8. Zweck und Einsatzbereich

Kern der CCA ist der Abgleich der Behandlungshistorie mit medizinischen Behandlungsleitlinien. Der Abgleich unterstützt den Arzt bei der Auswahl der optimalen Behandlungsmethode. Hierfür bietet die CCA folgende fach-medizinische Funktionen:

- Unterstützung einer arztübergreifend abgestimmten, mehrdimensionalen Therapie der Haupterkrankung und der vorhandenen Komorbiditäten,
- Stratifizierung bzw. Gruppierung von Patienten bezüglich ihrer Haupterkrankung und Erzeugung von ICD-Kodierhinweisen,
- Unterstützung der Einschreibung von Patienten in einen Selektivvertrag,
- Regelbasierte Unterstützung der Diagnostik von Begleiterkrankungen,
- Erstellung individualisierter Behandlungsempfehlungen für nichtmedikamentöse Therapien und Arzneimitteltherapien
- Unterstützung von arztübergreifenden Behandlungsprozessen durch Therapieplanung und Terminmanagement für Hausarzt und Fachärzte
- Prozessuale Unterstützung vertragskonformer ärztlicher Konsultationen und deren Dokumentation

--- Patientenbezogene und patientenübergreifende Evaluation mit Berechnung von Qualitätsindikatoren

--- Bidirektionale Kommunikation zwischen Arzt-Informations-Systemen und CCA-Server.

--- Datenbankbasierte Speicherung von Verwaltungsdaten und patientenbezogenen medizinischen Informationen,

--- Reports zu Behandlungsverläufen durch den Hausarzt sowie durch alle mitbehandelnden Fach- und Krankenhausärzte.

--- Die CCA-Dokumentation verwendet leitliniengerechte Prozessmodelle. Hierbei handelt es sich um schulmedizinische Abläufe für Konsultationen und deren Dokumentation (Einschreibung, Abklärung, Behandlung, Ausschreibung). Für einen Prozess sind Aufgaben der Patientenbehandlung zugeordnet, die in einer vorgegebenen Abfolge abgearbeitet werden. Die konkreten wissenschaftlichen Grundlagen, welche die CCA zugrunde legt, können innerhalb des CCA Accounts jederzeit eingesehen werden. An dieser Stelle ist hervorzuheben, dass sich dieses Audit nicht mit den Leitlinien, Prozessen und Berechnungsmethoden beschäftigt, da diese nicht datenschutzrechtlich relevant sind. Sie werden durch die medizinische Wissenschaft vorgegeben.

8.1.1 Login-Funktion und Passwortregelung

Anwender der CCA loggen sich mit einem Benutzernamen und einem Passwort ein. Die CCA bietet alternativ eine 2-Faktor-Authentisierung. Unterstützt werden VPN-Zertifikate, OTP- oder RSA-Token und USB-Token, wobei der Einsatz von Client-Zertifikaten empfohlen wird.

Als Passwortkonvention gilt eine verbindliche Mindestpasswortlänge von 8 Zeichen und Verwendung von 3 Zeichenarten (Klein-, Großbuchstaben, Zahlen oder Sonderzeichen), welche ausreichend stark ist. Das Gültigkeitsalter der Passwörter muss konfiguriert werden. In einem Datenschutz- und Sicherheitskonzept wird der Anwender bzw. Administrator darauf sensibilisiert, dass eine kurze Gültigkeit zu wählen ist und keine Passwörter im Browser gespeichert werden dürfen. Letzteres wird im CCA-Anmeldeformular im Browser mit der Direktive autocomplete=off technisch auch unterstützt.

Nach erstem Login muss der Anwender die Nutzungsbedingungen des für den Anwender jeweils geltenden integrierten Vollversorgungsvertrages gemäß § 140a SGB V[2] anerkennen, die er im Account auch jederzeit einsehen kann.

Im Account stehen dem Anwender – je nach festgelegter Rolle – verschiedene Funktionen zur Verfügung. Es gibt die Anwender-Rollen:

--- Arzt

--- Praxisassistent

[2] Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch Artikel 1 des Gesetzes vom 11. August 2014 (BGBl. I S. 1346) geändert worden ist.

--- Chronic Care Manager
--- Auditor
--- Administrator
--- Nutzeradministrator.

8.1.2 Arzt als Benutzerrolle

Der Arzt sieht Informationen zu Patienten, bei denen er als Leistungserbringer eingetragen ist. Er hat das Recht zur Ein- oder Ausschreibung und zur Verwaltung (d.h. Lesen, Schreiben, Löschen) von Patienten- und Versicherungsdaten sowie Daten der medizinischen Dokumentation (Befunde, Diagnosen, Therapien). Ferner kann er medizinische Auswertungen durchführen und Termine planen. Als einschreibender Arzt eines Patienten kann er diesem andere Leistungserbringer (z.B. mitbehandelnde Ärzte) zuordnen, die dann die gleichen Rechte bekommen, wie er. Die mitbehandelnden Ärzte können allerdings keine weiteren Ärzte hinzufügen.

Dem Arzt stehen folgende Haupt- und Unterfunktionen zur Verfügung:

--- **Arbeitsplatz**
  --- Patienten
    - Basisdaten
    - Status
    - Kalender
    - Termine
    - Aktuelle Aufgaben
    - Befunde
    - Zielwerte
    - Diagnosen
    - Nichtmedizinische Maßnahmen
    - Verordnungen
    - Prozessdiagramm
    - Evaluation
  --- Aktuelle Termine
  --- Aktuelle Aufgaben
  --- Vertrag (Dokumente)
--- **Auswertungen**
  --- Evaluation
--- **Hilfe**
  --- Hilfe
  --- Über CCA
  --- Nutzungsbedingungen
  --- Updates
  --- Passwort ändern

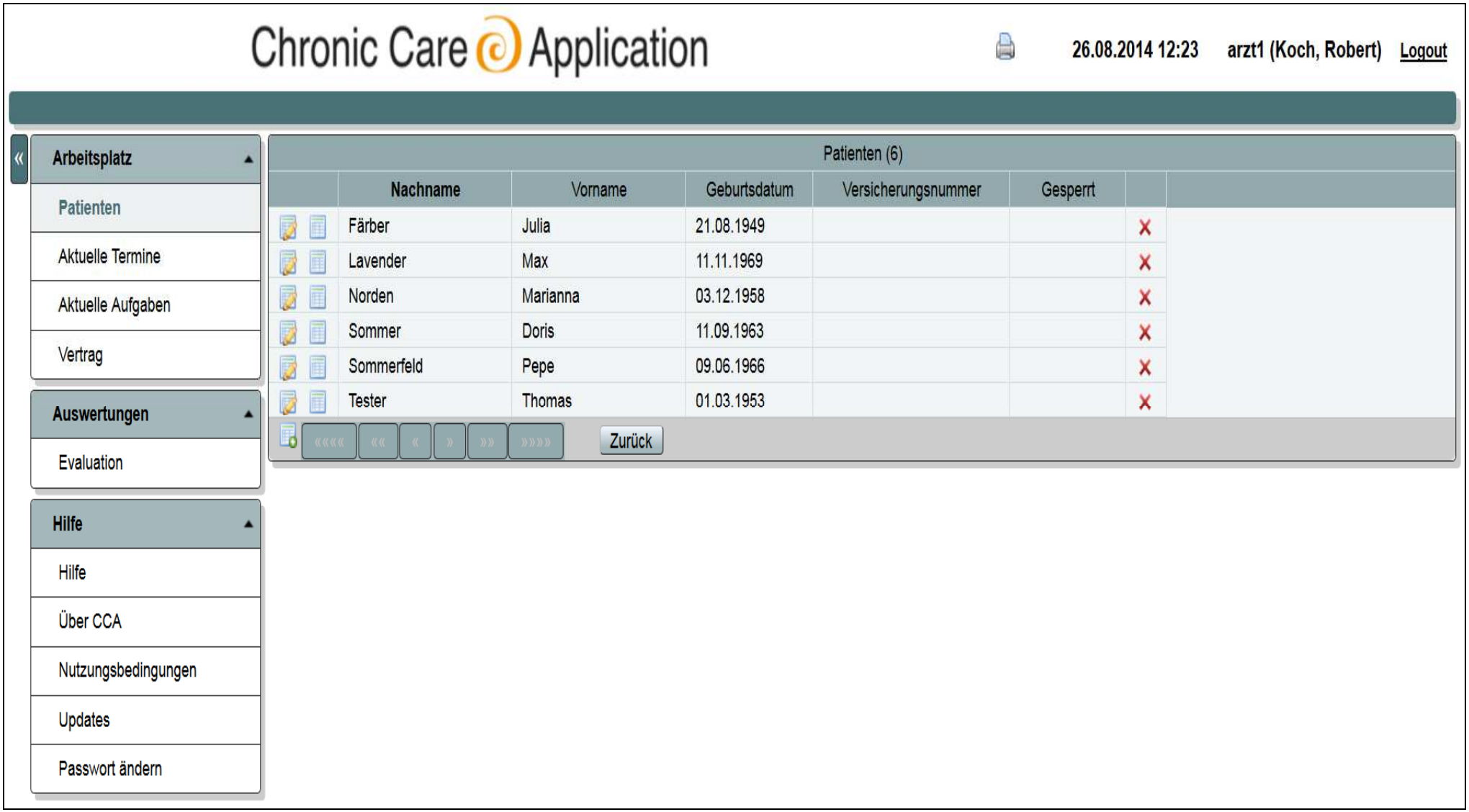

Abbildung 1 Arbeitsplatzübersicht der CCA für Ärzte - Startseite

Im Bereich „Patient“ erhält der Arzt eine Übersicht mit Basisdaten aller teilnehmenden Patienten sowie in weiteren Unterbereichen den aktuellen Status, eine Kalenderübersicht, eine Übersicht mit aktuelle Aufgaben für diesen Patienten, Befunde, Zielwerte, Diagnosen, nichtmedizinische Maßnahmen, Verordnungen, Prozessdiagramme und Ergebnisse einer Evaluation.

Bei der Einschreibung eines Patienten müssen Basisdaten in die CCA übergeben werden. Die Eingabe der Daten erfolgt manuell oder durch Übertragung aus den AIS. Einschreibungen können nur erfolgen, wenn für diesen Patienten eine Patientenerklärung vorliegt. Sie wird innerhalb der CCA als Muster zur Verfügung gestellt. Die Erklärung enthält eine Teilnahmeerklärung, eine Einwilligung, über Termine per Telefonanruf oder E-Mail an informiert zu werden, eine datenschutzrechtliche Einwilligungserklärung sowie eine Erklärung zur Entbindung des Arztes von der Schweigepflicht und eine Erläuterung der verschiedenen Nutzerrollen innerhalb der CCA.

Voraussetzung einer Einschreibung ist ferner, dass der Patient vertraglich in die integrierte Vollversorgung der jeweiligen Krankenkasse einbezogen ist.

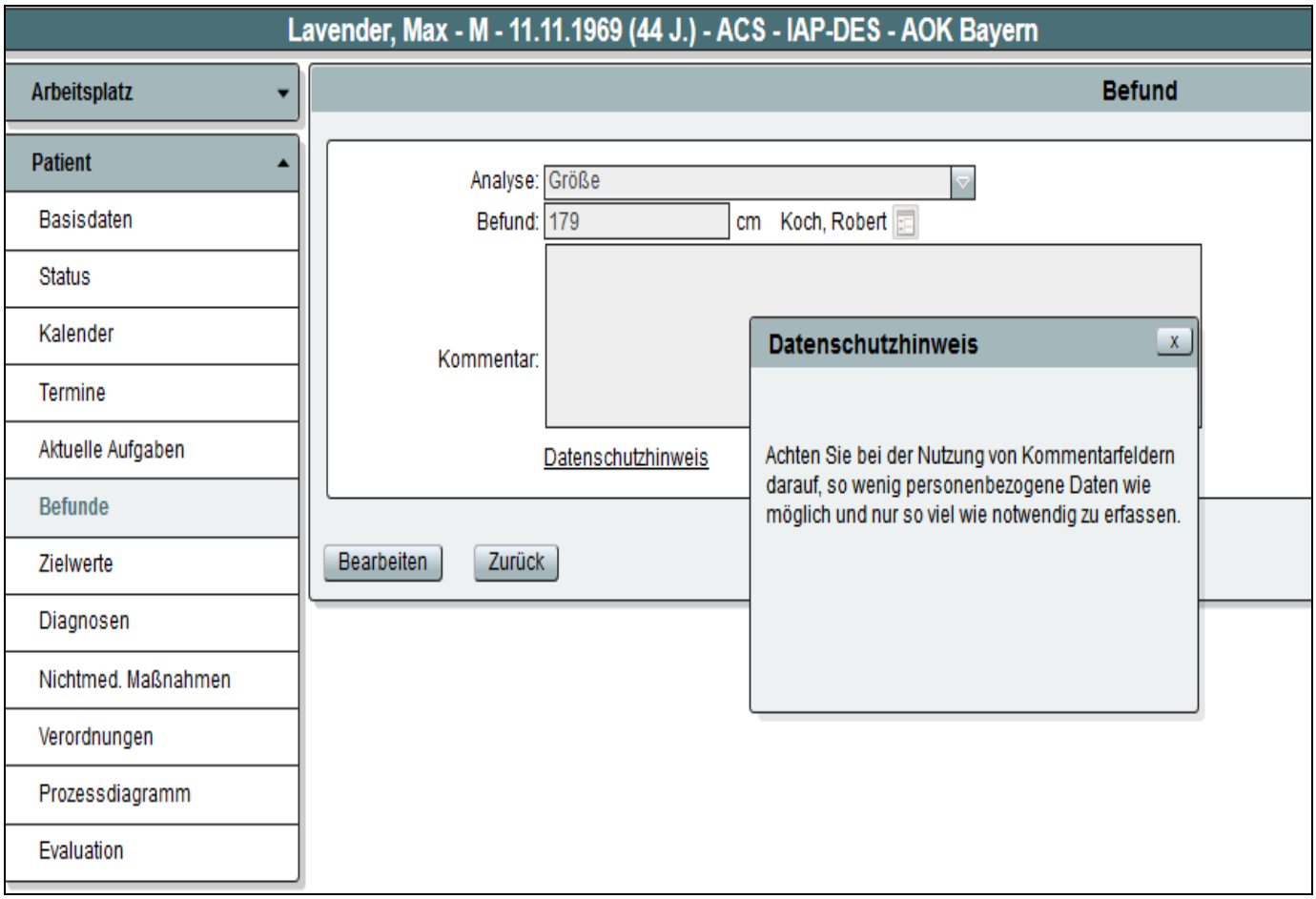

Abbildung 2 Arbeitsplatzübersicht der CCA für Ärzte

Über den Bereich „Auswertung“ erhält der Arzt eine Übersicht über Evaluationsergebnisse, die sich auf den Vollversorgungsvertrag beziehen.

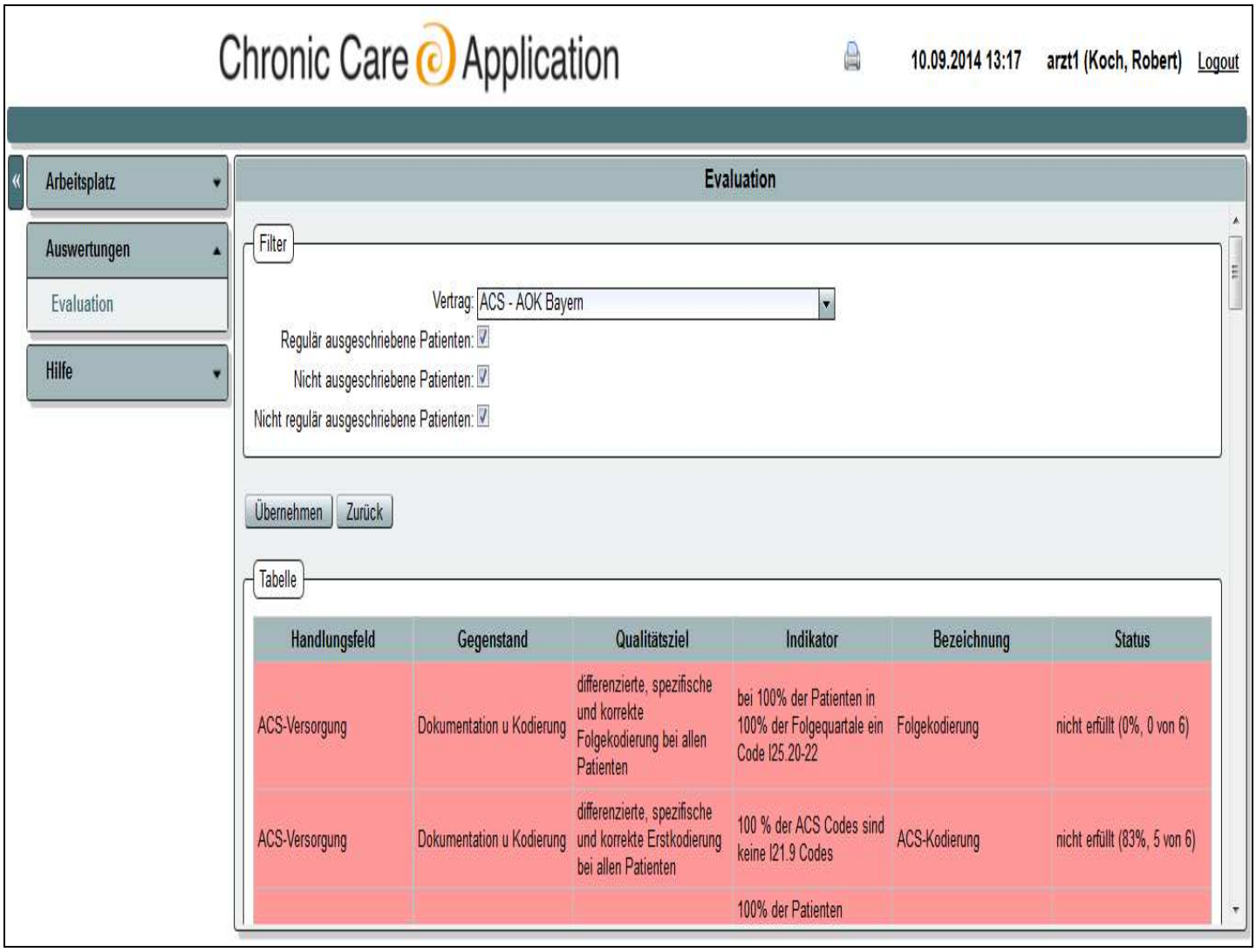

Abbildung 3 Bereich Auswertung für Ärzte

Im „Hilfebereich“ erhält der Anwender z.B. das Anwenderhandbuch als pdf, die aktuelle Versionsnummer, eine Erklärung wesentlicher Funktionen der CCA, die Nutzungsbedingungen, einen Überblick über Updates sowie die Funktion, das Passwort zu ändern.

8.1.3 Praxisassistenz als Benutzerrolle

Der Praxisassistent (PA) ist eine vom Arzt definierte Person. Er sieht den Bereich der Patientenakten und führt arztunterstützende Tätigkeiten durch, kann aber z.B. keine Patienten ein- und ausschreiben oder andere Ärzte hinzuziehen. Er kann auch keine Diagnose- oder Therapiedokumentation oder patientenübergreifenden Auswertungen einsehen oder durchführen.

8.1.4 Chronic Care Manager als Benutzerrolle

Der Chronic Care Managers ist eine Person im Umfeld des behandelnden Arztes. Er plant die integrierte Vollversorgung und hat hierfür Zugriff auf Patienten- und Vertragsdaten. Er wertet diese aus, um die nächsten Behandlungsschritte zu terminieren und um den Patienten oder den Arzt zu erinnern.

8.1.5 Auditor zur Qualitätskontrolle als zusätzliche Benutzerrolle

Ferner kann ein Auditor zur Qualitätskontrolle tätig werden. Der erhält lediglich Einblick in die Fallakte eines Patienten, jedoch keine Rechte für Veränderungen oder Löschen von Daten. Er kann die Historie der Daten und Datenveränderungen einsehen und qualitätssichern.

8.1.6 Installation, Administration, Berechtigungskonzept

Die CCA wird mit den Rollen Administrator und Nutzeradministrator ausgeliefert. Dem **Administrator** obliegt die Verwaltung (d.h. Lesen, Schreiben, Löschen) von Umgebungsdaten. Er verwaltet die Stammdaten der Ärzte, Vertragspartner-Krankenkassen und Ärztenetze. Die Nutzerverwaltung kann er sehen, hat aber keine Schreibrechte darauf. Er hat keinen Zugriff auf patientenbezogene Daten. Der **Nutzeradministrator** kann Nutzer anlegen, Rollen zuordnen, Nutzerdaten verändern und Nutzer löschen. Auch er hat keinen Zugriff auf patientenbezogene Daten.

	Admin	Nutzer-Admin	Leistungs-erbringer		CCM	Auditor
			Arzt	PA		
Administrative Daten ohne Patientenbezug	S L	- L	- L	- L	- L	(H)
Nutzerverwaltung	- L	S L	- -	- -	- -	(H)
Patientenverwaltung						
- Patientenstammdaten	- -	- -	S L *)	S L *)	S L	(H)
- Versicherungsdaten	- -	- -	S L *)	S L *)	S L	(H)
- Einschreibung	- -	- -	S L *)	- L *)	S L	(H)
- Zuordnung Leistungserbringer	- -	- -	S L *)	- L *)	S L	(H)
- Behandlungsprozess, Terminkalender	- -	- -	S L *)	S L *)	S L	(H)
- Ausschreibung	- -	- -	S L *)	- L *)	S L	(H)
Medizinische Dokumentation						
- Befunddokumentation	- -	- -	S L *)	S L *)	- L	(H)
- Diagnosedokumentation	- -	- -	S L *)	- L *)	- L	(H)
- Therapiedokumentation	- -	- -	S L *)	- L *)	- L	(H)
Medizinische Auswertungen						
- patientenbezogen	- -	- -	S L *)	S L *)	S L	
- patientenübergreifend	- -	- -	S L *)	- - *)	S L	

S – Schreiben (Anlegen, Ändern, Löschen)
L – Lesen
(H) – Sicht auf die Historie der Daten, für die der Auditor durch seine anderen Rollen berechtigt ist

*) Betrifft nur die Daten der Patienten, die dem Leistungserbringer zur Behandlung zugeordnet wurden.

Abbildung 4 Berechtigungskonzept der CCA

8.1.7 Sperrung, Löschung und Anonymisierung

Nach Beendigung eines Vertragsfalles werden die mit dem Vertragsfall verbundenen Daten zunächst gesperrt. Drei Monate danach werden die Daten anonymisiert und bleiben zu Evaluierungszwecken anonymisiert erhalten. Die Anonymisierung erfolgt durch Löschung des Patientenbezuges und aller identifizierenden Patientendaten einschließlich der Bezugsdaten zu verschiedenen AIS der beteiligten Ärzte. Von den Patientenstammdaten bleiben nur das Geschlecht und die behandlungsrelevanten Altersgruppen bei Vertragseintritt erhalten.

8.1 Komponenten

Die CCA hat folgende Komponenten:

--- CCA Application Server

--- CCA-AIS-Connector

--- Web-User Client.

Der **CCA Application Server** verwaltet Software und Datenbank und stellt die Funktionen des Webanwendungsservers zur Verfügung. Die CCA Java-EE-Anwendung wird in einem JBoss Application Server ausgeführt. Die Kommunikation des CCA Application Server mit einem AIS erfolgt über den Connector mit einem REST-konformen Web Service, der AIS-GDT-Dateien empfängt und mit JAXB-generierte CCA-XML-Dateien versendet. Auch diese Kommunikation basiert auf https. Der Application Server kapselt Funktionsaufrufe in Transaktionen und organisiert die automatische Datenbankspeicherung von Änderungen an Entity Beans. Die Prozessmodelle für die Behandlungsprozesse, für die Konsultationen und die Dokumentationen steuert die CCA mit Hilfe von JBoss Drools mit den Komponenten jBPMN und Rules. Für die Datenhaltung wird eine eingebettete H2 Database Engine verwendet.

Der CCA Application Server kann Patientendaten aus dem AIS empfangen und Verordnungs- und Diagnosedaten an das AIS übertragen. Der Datenaustausch erfolgt bidirektional über einen **CCA-AIS-Connector**. Der Connector ist ein Java-Programm, das auf dem AIS-PC des Nutzers installiert sein muss. Der Connector authentisiert den Nutzer bzw. sein AIS gegenüber dem CCA-Server und wickelt den Datentransport zwischen beiden Systemen mit SSL-Verschlüsselung ab.

Beim Aufruf des CCA Servers muss der Arzt seine Login-Daten eingeben. Alternativ können die Login-Daten im AIS-System hinterlegt sein und an den AIS-Connector übergeben werden. Das Hinterlegen der Login-Daten im AIS muss sicher geschehen, z.B. indem sie durch den AIS-Zugang geschützt werden.

Die XML-Kommunikation wird über einen Link im CCA-Programm initialisiert. Der AIS-Connector empfängt Daten und übergibt sie an das AIS. Der Arzt hat dann die Möglichkeit, diese Daten in seine AIS-Akte zu übernehmen und auf Grundlage der Verordnungsempfehlungen tatsächliche Verordnungen zu erstellen.

Die Anwender können die gängigen aktuellen Internet Browser nutzen. Der Zugriff auf die CCA erfolgt per SSL/https. Der **CCA-Web-Client** läuft im Internet Browser auf jedem aktuellen PC. JavaServer Faces und RichFaces generieren HTML-Sichten mit JavaScript-Unterstützung und AJAX-Datenübertragung. Daher muss im Browser JavaScript zu-gelassen sein.

8.2 Schnittstellen

Die Anwender können neben dem Internet Browser eine Kommunikations-Schnittstelle zum AIS verwenden. Existiert ein Patient noch nicht in der CCA-Patientenverwaltung, kann er auf Grundlage der übertragenen Stammdaten als Vertragsfall angelegt werden. Patientendaten der CCA können ferner an das AIS übergeben werden.

8.3 Verschlüsselung und Schnittstellen

Zum Schutz der Patientendaten ist ein verteiltes Keymanagement implementiert. Es gibt für jeden Patienten einen Patientenschlüssel, mit dem die Felder mit personenbezogenen Daten verschlüsselt werden. Dieser Schlüssel wird mit dem öffentlichen Schlüssel des behandelnden Arztes und weiterer leseberechtigten Personen verschlüsselt in der Datenbank hinterlegt. Nur mit Besitz des privaten Schlüssels lässt sich auf die Patientendaten zugreifen. Darüber hinaus wird die Datenbank noch verschlüsselt, um unbefugte Zugriffe auf das Backup zu verhindern.

Der CCA Application Server ist für die Verwendung von SSL vorkonfiguriert, und der http-Port ist deaktiviert. In der ausgelieferten web.xml ist die Kommunikation über sichere Kanäle für die gesamte Anwendung eingestellt. Voraussetzung ist ein von einem Trustcenter ausgestelltes, gültiges SSL-Server-Zertifikat. Im Administrations-handbuch wird darauf hingewiesen, dass die Sicherheit weiter erhöht werden kann, wenn sich nur Client-Rechner mit dem Server verbinden können, auf denen auch Client-SSL-Zertifikate installiert sind.

Die Administrationsschnittstelle ist per Remote Desktop Protocol auf der Basis von IPSec mit gegenseitiger Authentisierung mit Hilfe von Zertifikaten realisiert. Damit wird garantiert, dass nur zugelassene Administrations-Clients eine Verbindung zum Server aufbauen können.

8.4 Verarbeitung von Primär- und Sekundärdaten

Mittels der CCA werden folgende Daten verarbeitet:

- Patientenverwaltung
  - Patienten-Stammdaten (Name, Vorname, Geburtsdatum, Geschlecht, Größe)
  - Versicherungsdaten (Krankenkasse, Kassen- u. Versicherungsnummer)
  - CCA-Vertragsfall-ID,
  - Patienten-ID des Arzt-Informations-Systems
  - Einschreibedaten (Datum, Einwilligung, Status)
  - Ausschreibedaten (Datum, Status)
  - Beteiligte Leistungserbringer (Hausarzt, Fachärzte)
- Medizinische Dokumentation
  - Befunddaten (z.B. Blutdruck, Körpergewicht, Körpergröße)
  - Zielwerte für ausgewählte Befunddaten, z.B. Körpergewicht
  - Diagnosen (Haupterkrankung, Begleiterkrankungen)
  - Soziale Angaben (Alkoholkonsum nach Standards der WHO, Raucherstatus, Soziale Situation, Betreuungssituation)
  - Therapiedaten

- Medikamentöse Therapie, Wirkstoffempfehlungen
- Nichtmedikamentöse Behandlungen

--- Behandlungsprozess und Terminkalender

--- Planaufgaben bzw. -aktivitäten

--- Plantermine bzw. Planterminintervalle

--- Hausarzt/Facharzt-Konsultationen

In Freitextfeldern können ggf. personenbezogene Kommentare erfasst werden. Das Datenschutz- und Sicherheitskonzept sensibilisiert den Anwender auf die Einhaltung der Grundsätze der Zweckbindung, Datenvermeidung und Datensparsamkeit.

Ferner werden personenbezogene Daten der CCA-Administration verarbeitet:

--- Leistungserbringer (Hausärzte, Fachärzte)

--- Betriebsstätten-Nr.

--- Arztnummer

--- Fachrichtung

--- Name, Vorname

--- Adressdaten

--- Nutzerverwaltung

--- Login, Passwort (verschlüsselt)

--- Zugeordnete Rollen

--- Zuordnung eines Nutzers zu einem Leistungserbringer.

Sodann entstehen durch die Logging- und Protokollmechanismen Sekundärdaten. Auf dem CCA Application Server fallen access.log, nutzererror.log, server.log, boot.log und shutdown.log an. Standardmäßig werden die Logging-Dateien nicht gelöscht. Durch ein Batch-Script und eine zeitgesteuerte geplante Aufgabe, wie im Administrationshandbuch beschrieben, wird der Anwender aber aufgefordert, täglich automatisiert alle Logging-Dateien, die älter als 24 Stunden sind, zu löschen.

Beim Hibernate Envers werden in der Datenbank Tabellen eingerichtet, welche die Tabellen mit den aktuellen Daten ergänzen. Envers legt darin Informationen über die Historie der Originaldaten ab, die der CCA Auditor sehen kann. Beim Anonymisieren werden alle zu löschenden Daten inklusive ihrer Historie gelöscht.

Die CCA unterdrückt ein Browser Caching durch zentrale no-cache und no-store Metaanweisungen. Da Browser diese Anweisungen ignorieren können, werden den Anwendern nur Browser empfohlen, in denen das Caching deaktiviert werden kann, und es werden Hinweise zum Ausschalten des Caching gegeben. Außerdem wird der Anwender im Datenschutz- und Sicherheitskonzept sowie in einem Datenschutzhinweisblatt darauf hingewiesen, dass die Funktion der Browserseitigen Passwortspeicherung nicht genutzt werden darf.

8.5 Transparenz und Sicherheit der Einsatzumgebung

Die CCA wird in einer IT-Systemlandschaft des Anwenders eingesetzt und ist von den dort getroffenen Sicherheitsanforderungen abhängig. Hervorzuheben ist, dass die AstraZeneca GmbH ein Datenschutz- und Sicherheitskonzept mit zahlreichen Empfehlungen für eine angemessene Umsetzung des Datenschutzes und der

Datensicherheit bei der CCA ausgibt. Ein Datenschutzhinweisblatt informiert dabei im Speziellen über die Einhaltung des Datenschutzes. Alle Dokumente stehen im Account der CCA zur Verfügung.

8.6 Abgrenzung des Auditgegenstands

Die Chronic Care Application - CCA umfasst folgende Komponenten:

--- CCA Application Server

--- CCA-AIS-Connector

--- Web-User Client.

Nicht auditiert wurden andere Leistungen der AstraZeneca GmbH oder der Dienstleister, medizinische Leitlinien oder Behandlungsprozesse und dahinter stehende Berechnungsmethoden sowie das Medizinprodukt als solches, Verschlüsselungs- und Backupmechanismen.

Nicht Auditgegenstand ist ferner die Einsatzumgebung des Anwenders der CCA inklusive eingesetzter Tablets, Apps oder Smartphones. Auch gehört keine Cloud-Lösung der CCA zum Auditgegenstand.

8.7 Rechtliche Anforderungen

Der rechtliche Rahmen zur Entwicklung eines Anforderungsprofils gemäß der Datenschutzgütesiegelverordnung Schleswig-Holstein besteht in dem Landesdatenschutzgesetz Schleswig-Holstein (LDSG S-H), der Datenschutzverordnung (DSVO)[3], dem Bundesdatenschutzgesetz (BDSG)[4] sowie den bereichsspezifischen Bestimmungen des Gesundheitswesens. Die Auslegung dieser Rechtsnormen wird konkretisiert durch Rechtsprechung und durch Mitteilungen der Datenschutzaufsichtsbehörden.

Die Vorgaben des **SGB V** waren für die Auditierung nicht von Relevanz. Die CCA dient zwar dazu, die Versorgungsqualität im Rahmen von integrierten Vollversorgungsverträgen gemäß § 140a SGB V[5] zu unterstützen, indem sie Behandlungsleitlinien und Entscheidungshilfen bietet. Da dieser Vertrag zwischen dem Arzt und der Krankenkasse geschlossen wird, bildet er allerdings keine Rechtsgrundlage für die Verarbeitung von Patientendaten in der CCA. Die Teilnahme der Versicherten an den integrierten Versorgungsformen der § 140a ff. SGB V ist freiwillig und wird mit einer widerruflichen Einverständniserklärung gegenüber der Krankenkasse erklärt. Auch diese Einverständniserklärung bildet keine Rechtsgrundlage der Patientendatenverarbeitung in der CCA. Die CCA dient zudem weder einer gemeinsamen Dokumentation gemäß § 140b Abs. 3 SGB V noch einer der Abrechnung von Leistungen gemäß § 295a SGB V. Die Krankenkassen selbst haben keinen Zugriff auf die CCA. Ferner können über die CCA keine Patientendaten an die Krankenkassen übermittelt werden.

---

[3] Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten v. 05.12.2014, GVOBl Schl.-H. 2013, S. 554ff.

4 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).

[5] Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch Artikel 1 des Gesetzes vom 11. August 2014 (BGBl. I S. 1346) geändert worden ist.

Die Pflicht zum ordnungsgemäßen Umgang mit Patientendaten ergibt sich für den Arzt allerdings aus einer Vielzahl von bereichsspezifischen Rechtsvorschriften. Dies folgt aus § 10 der (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (**MBO-Ä**)[6] bzw. den nahezu gleichlautenden landesgesetzlichen Ausprägungen der Berufsordnungen[7]. Wesentlich ist die ärztliche Schweigepflicht, welche eine der ältesten bekannten Datenschutzbestimmungen darstellt[8]. Sie gilt gemäß **§ 203 Strafgesetzbuch** (StGB)[9] in Verbindung mit § 9 MBO-Ä für das gesamte Behandlungsverhältnis. Im Zuge der Datenverarbeitung mittels der CCA darf das Patientengeheimnis weder innerhalb von Praxisgemeinschaften, noch gegenüber dem Chronic Care Manager, dem Auditor sowie den Administratoren und Nutzeradministratoren rechtswidrig offenbart werden, sofern diese Rollen nicht zugleich einem behandelnden Arzt zuzuordnen sind. Ebenfalls dürfen die Patientendaten der CCA nicht den ggf. einbezogenen IT-Dienstleistern rechtswidrig offenbart werden. Um eine rechtswidrige Offenbarung im Zuge der Nutzung der CCA zu verhindern, kommt es daher auf die Rechtsgrundlage des **individuellen Behandlungsvertrages** zwischen Patient und Arzt in Verbindung mit einer schriftlichen **Patientenerklärung** an, in welcher der Patient nach vorheriger Aufklärung über die Datenverarbeitungszwecke in die Datenverarbeitung jederzeit widerruflich einwilligt und den Arzt von seiner Schweigepflicht entbindet. Den Anwendern der CCA wird daher eine solche Patientenerklärung bereitgestellt.

Die CCA kann ferner Teil bzw. Subsystem eines Krankenhausinformationssystems (KIS) sein. Demnach sind die Auslegungshilfen der „**Orientierungshilfe Krankenhausinformationssysteme**“, Version 2.0 aus März 2014 der Unterarbeitsgruppe Krankenhausinformationssysteme der Arbeitskreise Gesundheit und Soziales sowie Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder[10] anwendbar. Für die CCA wurden die Hersteller-seitigen Vorgaben der OH KIS betrachtet. Da die CCA lediglich ein Subsystem eines KIS darstellt, wurden die obligatorischen Regelungen der OH KIS zudem nur dann als anwendbar betrachtet, soweit sich diese nicht auf die reine elektronische Patientenakte beziehen.

Hervorzuheben ist, dass es sich bei der CCA um keinen Telemediendienst im Sinne des **Telemediengesetzes** (TMG)[11] handelt, welcher online für eine offene Benutzergruppe über das Internet erreichbar ist. Vielmehr wird die CCA ausschließlich in der geschlossenen Einsatzumgebung des Anwenders eingesetzt. Die CCA ist zudem eine individuelle Softwareentwicklung der dr. heydenreich GmbH für die AstraZeneca GmbH und wird als solche weder auf den Webseiten dieser beiden Unternehmen noch anderer Stellen beworben.

---

[6] MBO-Ä 1997 in der Fassung der Beschlüsse des 114. Deutschen Ärztetages 2011 in Kiel.
[7] Z.B. Berufsordnung (Satzung) der Ärztekammer Schleswig-Holstein vom 3. Februar 1999 in der Fassung vom 08. Mai 2012, ABl. Schleswig-Holstein v. 29. Mai 2012.
[8] Zurückgehend auf den Hippokratischen Eid, ca. 400 v. Chr.: „Was immer ich sehe und höre bei der Behandlung oder außerhalb der Behandlung im Leben der Menschen, so werde ich von dem, das niemals nach draußen ausgeplaudert werden soll, schweigen, indem ich alles Derartige als solches betrachte, das nicht ausgesprochen werden darf“.
[9] Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 1 des Gesetzes vom 23. April 2014 (BGBl. I S. 410) geändert worden ist.
[10] Z.B. Abrufbar unter http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=13016&article_id=95681&_psmand=48.
[11] Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692) geändert worden ist.

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

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 die CCA kam es daher auf die Prüfung der Dokumentationen, Tests und Freigabeverfahren an.

9. Modellierung des Datenflusses

Die nachfolgende Abbildung illustriert die Komponenten und den Datenfluss der CCA. Sie zeigt links die Kommunikation zwischen dem CCA Application Server und den CCA-Nutzern Arzt, Chronic Care Manager (CCM) und dem Administrator. Diese Rollen nutzen einen Web Browser als User Client. Weiterhin zeigt die Abbildung rechts den Datenaustausch zwischen dem CCA Application Server und dem CCA-AIS-Connector:

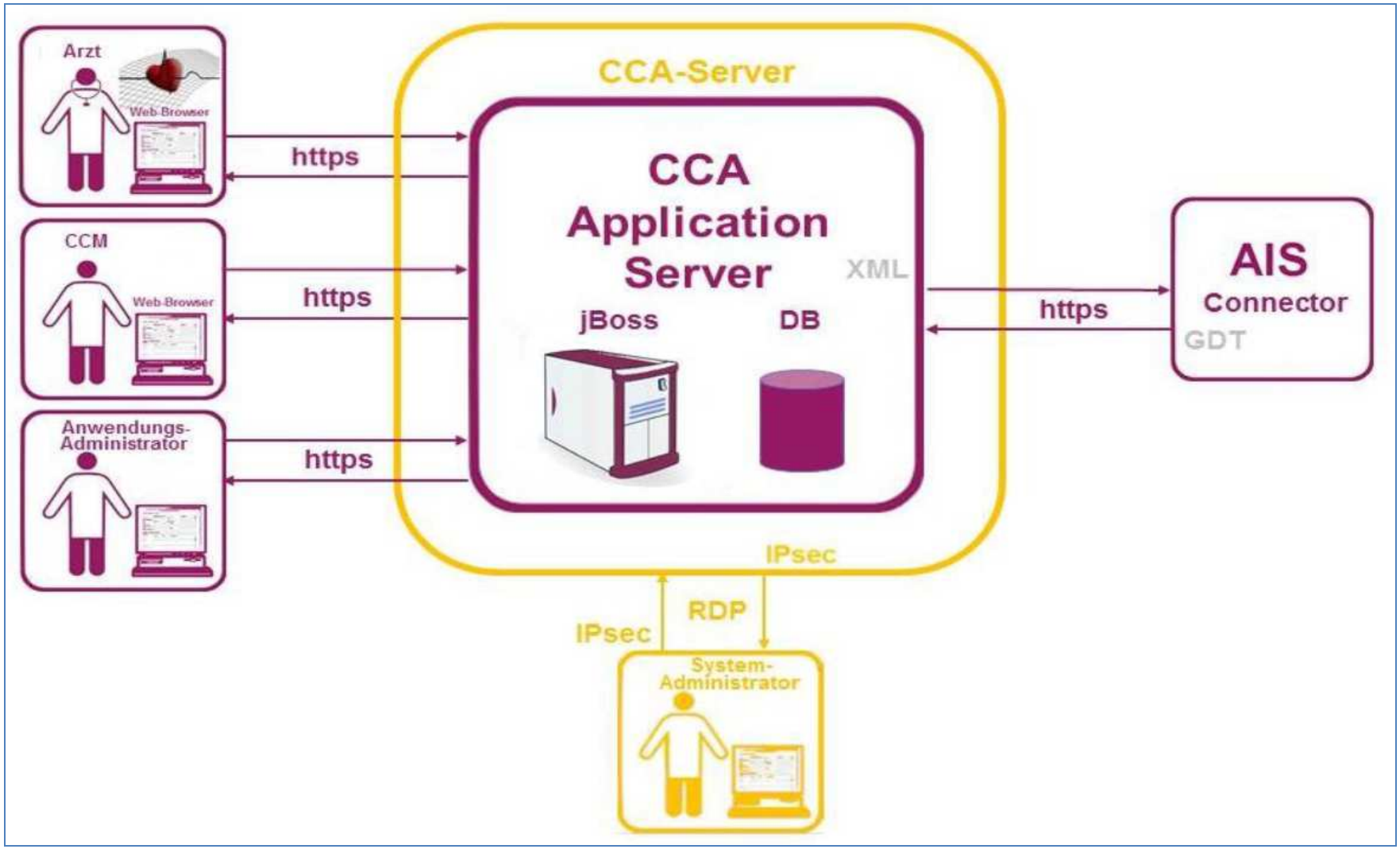

Abbildung 5 Datenfluss

10. Version des Anforderungskatalogs

Version 1.2

11. Zusammenfassung der Prüfergebnisse

Die Prüfergebnisse im Einzelnen werden wie folgt zusammengefasst:

Nr.	Anforderungsprofil	Bewertung / Kommentar
Datenart A: Medizinische Daten (Primärdaten)		
A1	Produktbeschreibung	verständlich und aussagekräftig, in vollem Umfang sichergestellt
A2	Datensparsamkeit, Pseudonyme	in adäquater Weise sichergestellt
A3	Zulässigkeit der Datenverarbeitung	Zulässig
A4	Authentizität der Nutzer	in vollem Umfang sichergestellt
A5	Authentizität des Servers	in vollem Umfang sichergestellt
A6	Vertraulichkeit der übertragenen Daten	in vollem Umfang sichergestellt
A7	Vertraulichkeit der auf dem Server gespeicherten Daten	in vollem Umfang sichergestellt
A8	Integrität der übertragenen Daten	in vollem Umfang sichergestellt
A9	Integrität der auf dem Server gespeicherten Daten	in vollem Umfang sichergestellt
A10	Verfügbarkeit der Daten	in vollem Umfang sichergestellt
A11	Revisionsfähigkeit	in vollem Umfang sichergestellt
A12	Betroffenenrechte	in vollem Umfang sichergestellt
Datenart B: Protokolldaten (Sekundärdaten)		
B1	Produktbeschreibung	verständlich und aussagefähig, in vollem Umfang sichergestellt
B2	Zulässigkeit der Verarbeitung	Zulässig
B3	Vertraulichkeit der Protokolldaten	im vollem Umfang sichergestellt
B4	Integrität der Protokolldaten	in vollem Umfang sichergestellt
B5	Verfügbarkeit der Protokolldaten	im vollem Umfang sichergestellt

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

Das IT-Produkt fördert den Datenschutz auf Vielfältige Weise:

--- Bei der Konfiguration der Verbindungsverschlüsselung per SSL wird der Anwender deutlich auf die Notwendigkeit einer sicheren Konfiguration hingewiesen.

--- Bereits im Rahmen der Entwicklung der CCA wurden Aspekte des Datenschutzes und der Datensicherheit vor dem Hintergrund des besonderen Schutzbedarfs von Patientendaten berücksichtigt und flossen in das Gesamtkonzept ein. Der Anwender wird verständlich und vorbildlich für die Einhaltung des Datenschutzes und der Datensicherheit sensibilisiert

--- Durch das Verschlüsselungskonzept werden Primärdaten gezielt einzelnen Nutzern und nicht Nutzergruppen freigegeben. Diese Freigaben können auf einfache Weise entzogen werden, indem Schlüsseldateien gelöscht werden. Diese klare Lösung unterstützt die Vermeidung von fehlerhaften Freigaben.

13. Votum der Auditoren

Das IT-Produkt Chronic Care Application, Version 1.23, setzt insgesamt die Anforderungen an den Datenschutz angemessen um. Die Auditoren haben daher der Zertifizierungsstelle die Gütesiegelvergabe empfohlen.

Bremen, den 23. März 2015

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

Ralf von Rahden
datenschutz cert GmbH