Prüfstelle für Fachprogramme
Dr. Uwe Schwochert

Kurzgutachten zum Datenschutzgütesiegel des ULD

IT-Produkt:

Medikationsplanserver des Modellvorhabens ARMIN Stufe 3

Programmversion: 1.0.2018.2.19

Prüfgrundlage:	Anforderungskatalog 2.0 vom 28.11.2014 des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein (ULD)
Gutachten-Version:	1.5
Stand:	22.05.2018
Projektnummer:	TB1309104530

A. Allgemeine Angaben zur Prüfung

A.1 Zeitpunkt der Prüfung

Das Prüfprojekt fand im Zeitraum von Juli 2013 bis Mai 2018 statt.

A.2 Adresse des Antragstellers

AOK PLUS
Sternplatz 7
01067 Dresden

A.3 Adresse des Sachverständigen

TRUSTBIT Prüfstelle für Fachprogramme
Dr.-Ing. Uwe Schwochert

Halankweg 15
01156 Dresden

Tel.: +49 (351) 4163820

A.4 Kurzbezeichnung des IT-Produktes

Medikationsplanserver

A.5 Detaillierte Bezeichnung / Abgrenzung des IT-Produktes

Bezeichnung

Medikationsplanserver des Modellvorhabens ARMIN Stufe 3

Der Medikationsplanserver (MPS) ist ein IT-Service der AOK PLUS (AOK) zur Unterstützung des Anlegens und der Verwendung gemeinsamer Medikationspläne eines Versicherten durch den ihn betreuenden Arzt und Apotheker.

Was ist Zertifizierungsgegenstand?

Der Prüfgegenstand MPS besteht aus mehreren für seinen Betrieb notwendigen Komponenten und Diensten. Im Detail bezieht sich die Zertifizierung auf:

- das Programm Medikationsplanserver MPS,
- das für das Einspielen von Daten zum MPS bereitgestellte Tool JOBS,
- das für den Test und behelfsweisen Zugang zum MPS bereitgestellte "RHEA Web Frontend" (RWF),
- die für die Teilnehmerverwaltung innerhalb des MPS bereitgestellte Software "RHEA Management UI" (RMU),
- die Anbindung von IT-Systemen der Ärzte und Apotheken (Primärsysteme, PS) an den MPS,
- die den MPS betreffenden Prozesse der AOK-Teilnehmerverwaltung AOK SELECT,
- den Betrieb des MPS (MPB, Management durch kubus IT, Server-Bereitstellung durch COLT).

Was ist nicht Zertifizierungsgegenstand?

Aus dem angebotenen Dienst MPS ergeben sich spezielle Anforderungen an benachbarte bzw. verbundene Systeme. Dies betrifft:

- allgemeine Betriebsprozesse bei den den Medikationsplan betreibenden Dienstleistern (Komponente MPB),
- allgemeine Prozesse des Versichertenmanagements bei der AOK (Komponente AOK SELECT),
- Sicheres Netz der Kassenärztlichen Vereinigung (Komponenten SNET, KV-Connect),
- Schnittstellen zum Datenaustausch (S3C, FIVERX),
- Praxisverwaltungssysteme in der Arztpraxis (PVS),
- Apothekenverwaltungssysteme (AVS).

Diese einzelnen technischen Komponenten existieren unabhängig vom zu prüfenden Medikationsplanserver und sind für sich selbst nicht Prüfgegenstand. Im Rahmen der Datenschutz-Begutachtung des Medikationsplanservers war jedoch anhand von Dokumentationen und Spezifikationen zu prüfen, ob diese Komponenten grundsätzlich geeignet sind, die sich aus dem Medikationsplanserver ergebenden Datenschutzauflagen umzusetzen.

A.6 Tools, die zur Herstellung des IT-Produktes verwendet wurden

Medikationsplanserver:

- Visual Studio 2013
- git (Versionskontrollsystem)
- Microsoft SQL-Server 2012
- Programmiersprache C#

Kommunikationsplattform für die Kommunikation mit den **PS** und für die Web-Anwendung

- Microsoft IIS 8.x
- KV-Connect (REST-Schnittstelle und PKI)

A.7 Zweck und Einsatzbereich des IT-Produktes

A.7-1 Zweck des Medikationsplanservers (MPS)

Zweck der Bereitstellung des Medikationsplanservers (MPS) ist es, ein systematisches und dokumentiertes Medikationsmanagement unter Einbeziehung des Hausarztes und der Stammapotheke eines Versicherten zu ermöglichen. Das Medikationsmanagement dient der Verbesserung der Arzneimitteltherapiesicherheit und der Therapietreue bei multimorbiden Versicherten der AOK. Der Medikationsplanserver soll dazu das gemeinsame detaillierte Erfassen und Bereitstellen der Medikationspläne mit einer geeigneten und sicheren IT-Infrastruktur unterstützen.

A.7-2 Einsatzbereich

Einsatzbereich des betrachteten Services ist die Medikamentenversorgung von Krankenversicherten im Zusammenspiel Versicherter-Arzt-Apotheker-Krankenkasse. Damit kommen die zum Medikationsplanserver gehörenden Softwarekomponenten bei der AOK, bei Ärzten und bei Apotheken zum Einsatz. Dem Modellcharakter des Projektes entsprechend wird eine Anwendung dieser Lösung in verschiedenen Krankenkassen, Regionen und Patientenbetreuungssituationen (z. B. auch Klinik, Pflegeeinrichtung) avisiert und ist damit grundsätzlich auch für öffentliche-rechtliche Träger der medizinischen Versorgung in Schleswig-Holstein relevant (Anbindung entsprechend autorisierter Zugriffe über SNET ist auch in Schleswig-Holstein möglich).

A.7-3 Projekteinordnung

Der Medikationsplanserver der AOK (MPS) ist eingebettet in die "Arzneimittelinitiative Sachsen-Thüringen", kurz ARMIN. ARMIN ist ein Modellvorhaben nach [SGB V] § 63 und wird unter www.arzneimittelinitiative.de detaillierter vorgestellt.

Im Rahmen von Stufe 3 dieses Vorhabens ist vorgesehen, die technischen Voraussetzungen für ein Medikationsmanagement zu schaffen, indem den einen Patienten betreuenden Ärzten

und Apothekern eine Möglichkeit zur gemeinsamen Speicherung von Medikationsplänen gegeben wird. Das Vorhaben bietet dazu eine in die Primärsysteme der Leistungserbringer (PVS, AVS) integrierte serverbasierte Lösung, um den Anspruch der Versicherten nach [SGB V] § 31a (Einführung durch das E-Health-Gesetz auf Papierbasis) auf einen Medikationsplan einzulösen.

A.7-4 Übersicht Ablauf Medikationsmanagement

Das Projekt ARMIN Stufe 3 wird Ärzten und Apotheken (Leistungserbringer) über ihre Verbände als Vertrag angeboten. Die eingeschriebenen Leistungserbringer erhalten in einem ersten Schritt von der AOK über den MPS Informationen zum Programm sowie Vorschlagslisten für das Medikationsmanagement. Diese enthalten eine Auflistung der Versichertennummern der Versicherten, die eine Vielzahl von Medikamenten einnehmen und die beim jeweiligen Arzt in hausärztlicher Betreuung sind bzw. in der jeweiligen Apotheke die Mehrzahl ihrer Verordnungen einlösen. Mit der Aufnahme auf eine solche Vorschlagsliste wird dem Leistungserbringer signalisiert, dass für den jeweiligen Versicherten das Anlegen eines Medikationsplans sinnvoll sein könnte, um die Arzneimitteltherapiesicherheit zu verbessern.

Im zweiten Schritt spricht der Leistungserbringer den Versicherten an, informiert über das Projekt und bietet ihm das Anlegen eines Medikationsplans an. Willigt der Versicherte in das Aufstellen eines Medikationsplans und die damit verbundene Datenverarbeitung ein, wird dies vertraglich in einer Teilnahme- und Einwilligungserklärung vermerkt, welche vom Arzt, Apotheker und vom Patienten unterzeichnet wird.

Diese Erklärung wird in Schritt Drei an das "Fallmanagement" bei der AOK geleitet, wo daraus die Teilnehmerinformationen für den MPS aufbereitet werden. Von hier aus wird auch die Erzeugung eines (leeren) Medikationsplans für den betroffenen Versicherten auf dem MPS eingeleitet. Weiterhin werden zu diesem Medikationsplan Abrechnungsdaten der AOK bereitgestellt.

Im vierten Schritt erfolgt eine Erstaufnahme der Gesamtmedikation des Versicherten beim Apotheker. Dafür stehen nun seitens des MPS die Abrechnungsdaten der AOK aus dem letzten halben Jahr zur Verfügung. Die Aufnahme konkreter Medikationen in den Medikationsplan erfolgt aber grundsätzlich einzeln durch einen Leistungserbringer. Dabei werden auch Selbstmedikationen des Versicherten, die nicht verschreibungspflichtig sind, auf Grundlage seiner Angaben eingetragen.

Mit diesem Schritt ist das Anlegen des Medikationsplans beendet, dieser wird erst jetzt für den beteiligten Arzt freigegeben, so dass der Medikationsplan nun wechselseitig durch Arzt und Apotheker weiter gepflegt werden kann. Vergangene Medikationen werden gelöscht (sofern nicht aus Verträglichkeits- oder anderen medizinischen Gründen noch relevant), neue eingetragen. Der Patient erhält nach jeder Änderung den Medikationsplan ausgehändigt.

In jeder Bearbeitungsstufe hat der Versicherte verschiedene Eingriffsmöglichkeiten. Neben der regulären Angabe von Selbstmedikationen für den Eintrag in den Medikationsplan kann er auch Widerspruch zu einzelnen Angaben einlegen oder der weiteren Speicherung seines Medikationsplans widersprechen. Dabei gelten auf Grund der getrennten Bearbeitung verschiedene Ansprechpartner: Während hinsichtlich der einzelnen Eintragungen auf dem Medikationsplan immer der betreuende Arzt und die Apotheke zuständig sind, werden Widersprüche zur Vertragsteilnahme insgesamt sowie zur Bereitstellung von Daten für den Medikationsplan durch die AOK (Vorschlagslisten, Abrechnungsdaten) direkt an die AOK gerichtet.

A.7-5 Vertragliche Sicht

Mit dem Projekt ARMIN sind vielfältige vertragliche Beziehungen zwischen den Beteiligten verbunden. Kernbestandteil ist die

"Teilnahme- und Einwilligungserklärung",

ein Vertrag zwischen dem Versicherten, der AOK PLUS, dem betreuenden Arzt und dem Apotheker, der die Grundlage für das Anlegen eines konkreten Medikationsplans bildet. Dieser Vertrag ist eingebettet in den Rahmenvertrag

"Vertrag zu einem Modellvorhaben nach § 63 SGB V zur Optimierung der Arzneimittelversorgung in Sachsen und Thüringen (Arzneimittelinitiative Sachsen-Thüringen - ARMIN)"

der zwischen der **AOK** und den Kassenärztlichen Vereinigungen sowie den Apothekerverbänden in Sachsen und Thüringen abgeschlossen wurde. In ihm sind die Vorlagen für Einzelverträge mit Ärzten, Apotheken und Versicherten enthalten. Dieses Vertragswerk enthält aus Datenschutzsicht wichtige Vorgaben an die Leistungserbringer und ihre Informations- und Betreuungspflichten gegenüber den Versicherten.

Hinsichtlich der technischen Umsetzung gibt es folgende Verträge:

- Vereinbarungen zur Nutzung des Sicheren Netzes der Kassenärztlichen Vereinigungen (SNK) für die Bereitstellung der Dienste des MPS,
- eine Auftragsdatenverarbeitung seitens der kubus IT (ausgelagerter IT-Dienstleister der AOK PLUS und AOK Bayern) gegenüber diesen AOKn,
- eine Auftragsdatenverarbeitung seitens Colt Technology Services GmbH (COLT) gegenüber dem AOK Bundesverband (AOK BV).
- Eine vertragliche Vereinbarung über die Entwicklung und Bereitstellung von Software für den MPS mit Element 44 GmbH (E44).

Die vertragliche Situation wurde bei den entsprechenden Prüfkriterien des Prüfgutachtens konkret betrachtet.

A.7-6 Komponentensicht

Zur Funktion des Medikationsplanservers ist das Zusammenwirken verschiedener Komponenten erforderlich. Ein Überblick ist mit dem Diagramm in Abschnitt ➔ A.9 gegeben.

Der MPS selbst wird als Anwendung bei COLT gehostet. COLT hat dabei aber nur die Verantwortung für die Bereitstellung einer sicheren Systemumgebung (inkl. Backups), das Management des MPS erfolgt durch den Auftraggeber. Die MPS Datenbestände liegen bei COLT nur verschlüsselt vor, können von dort aus also nicht zugegriffen werden. Eine kurzeitige unverschlüsselte Verarbeitung ist dabei jedoch nicht vermeidbar. Die konkrete Betreuung der Anwendung MPS erfolgt durch kubus IT im Auftrag der AOK.

Im Rahmen der Betreuung der Anwendung werden durch kubus IT die vom Entwickler E44 bereitgestellten Softwarekomponenten eingespielt.

Die grundsätzliche Verwaltung der an ARMIN teilnehmenden Versicherten erfolgt im AOK Fallmanagement (AOK FM). Hier gehen die Einschreibungen der Leistungserbringer und Versicherten ein, wobei spezielle Software der AOK zum Einsatz kommt (AOK SELECT). Die Teilnehmerverzeichnisse, Vorschlagslisten und Abrechnungsdaten (aus R300) werden hier als Dateien vorbereitet und der kubus IT zum Einspielen auf den MPS bereitgestellt (Komponente JOBS).

Für die Verwaltung der Teilnehmer auf dem MPS durch AOK FM kommt RHEA Management UI zum Einsatz, für das Einspielen der Daten zum MPS durch kubus IT das Kommandozeilenprogramm JOBS.

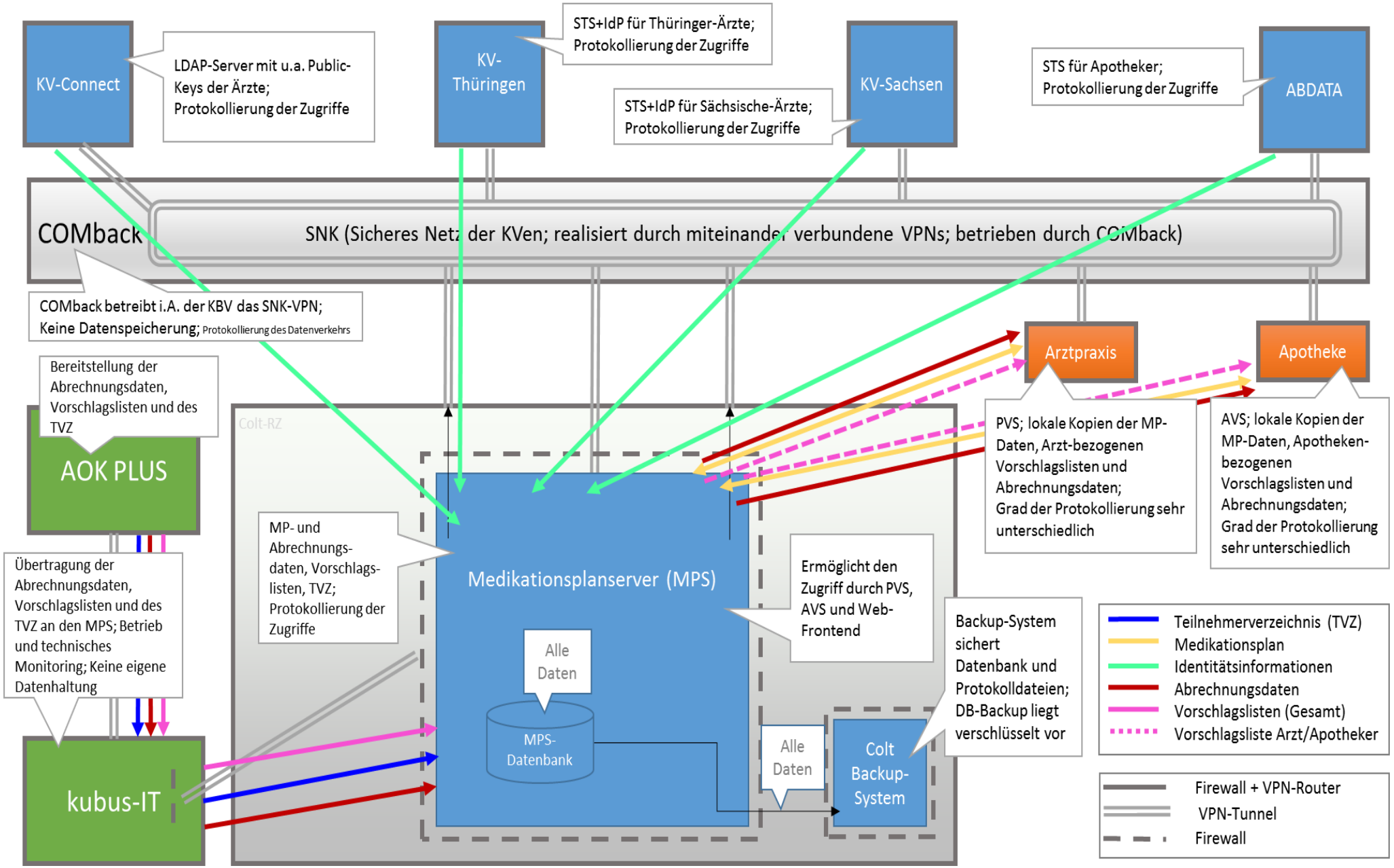
Für die Übertragung der Informationen zu den Leistungserbringern kommt das SNK über die Zugangsvariante KV-SafeNet (=SNET) zum Einsatz. Die durch das SNET gegebene Sicherheit wird durch eine MPS-spezifische Verschlüsselung ergänzt, welche auf der PKI des SNET aufsetzt. Um neben den ohnehin eingebundenen Ärzten auch die Apotheker einzubinden, wurde das SNK für Apotheken geöffnet. Außerdem unterstützt der MPS neben dem Schnittstellenstandard der Arztsysteme (S3C) auch den der Apothekensoftware (FIVERX).

In der Arztpraxis kommt ein Praxisverwaltungssystem (**PVS**) zum Einsatz. Dieses muss bestimmte, von der GEVKO GmbH spezifizierte und kontrollierte Standards erfüllen, damit der Arzt am ARMIN Programm (und auch an anderen Sonderprogrammen) teilnehmen kann. Die

für ARMIN benötigten Funktionen werden durch E44 als Entwickler des MPS umgesetzt. Die Gewährleistung eines hohen Datenschutzniveaus ist Teil dieser funktionalen Anforderungen.

Auf Apothekenseite kommen ebenfalls durch verschiedene Entwickler bereitgestellte Apothekenwarenwirtschaftssysteme zum Einsatz. Auch diese müssen zur korrekten Unterstützung von ARMIN mit seinen Datenschutzauflagen spezielle Anforderungen erfüllen. Diese werden im Rahmen eines Konformitätsverfahrens mit Herstellererklärung überwacht.

A.9 Modellierung des Datenflusses



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

Anforderungskatalog 2.0 vom 28.11.2014 des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein (ULD).

A.11 Zusammenfassung der Prüfergebnisse

Allgemeines

Der MPS der AOK stellt eine komplexe Serviceleistung der AOK in einem durch verschiedene Beteiligte sicherzustellenden informationstechnischen Umfeld dar. Entsprechend lag der Schwerpunkt der Begutachtung bei der Betrachtung des korrekten und datenschutzgerechten Zusammenspiels der verschiedenen Beteiligten. Maßgaben zur Gewährleistung des Datenschutzes erstrecken sich auch auf benachbarte Systeme. Dabei wurde neben den Vorgaben der AOK als Betreiber des Service an diese Beteiligten auch deren dokumentierte Umsetzung der Vorgaben geprüft.

Dies betraf neben der Auftragsdatenverarbeitung durch die beiden Dienstleister COLT und kubus IT auch die Sicherstellung der Umsetzung von Sicherheits- und Datenschutzvorgaben durch die eingebundenen Ärzte und Apotheker. Eine große Rolle spielten dabei die jeweiligen Verbände, also die Kassenärztlichen Vereinigungen und die Apothekerverbände.

Zusammenfassend kann festgestellt werden, dass nicht zuletzt durch die detaillierten Spezifikationen der GEVKO und ihre Umsetzung durch den eingebundenen Softwareentwickler E44 diese Überprüfung erfolgreich verlaufen ist. Die Vorgaben an alle Beteiligten sind klar und ausführlich dokumentiert und werden entsprechend dokumentiert umgesetzt.

Rechtliche Grundlagen

Der MPS ist Bestandteil des Modellvorhabens "ARMIN" nach [SGB V] § 63. Es war nachzuweisen, dass in den Verträgen zu diesem Modellvorhaben der Zweck hinreichend klar beschrieben ist, so dass auch ein notwendiger Umfang der zu speichernden und zu übermittelnden personenbezogenen Daten abgeleitet werden konnte.

Mit dem (nachgewiesenen) Status als Modellprojekt besteht grundsätzlich eine Ermächtigung zur Speicherung der Daten. Hinsichtlich der konkreten Ausgestaltung des Modellprojektes und der damit verbundenen Speicherung konkreter Gesundheitsdaten einzelner Versicherter muss jedoch beim einzelnen Betroffen eine spezielle Einwilligung eingeholt werden.

Im Verlauf der Begutachtung wurden die verschiedenen Aspekte dieser Einwilligung, insbesondere die ausreichende Information des Versicherten und seine Eingriffsmöglichkeiten, detailliert geprüft. In zahlreichen Dokumenten, Informationsbroschüren und Dokumentationen werden nicht nur der Versicherte sondern auch der ihn betreuende Arzt und Apotheker sowie auch deren Softwareentwickler über die mit dem Schutz der Versichertendaten verbundenen Maßgaben informiert.

Spezielle Aufmerksamkeit galt der arbeitsteiligen Zuständigkeit für die Wahrnehmung von Betroffenenanliegen. Im Rahmen der Begutachtung wurde nachgewiesen, dass diese Arbeitsteilung (Trennung der Speicherung nach Zuständigkeiten) nicht zu einer unübersichtlichen Situation für den Betroffenen wird und er jederzeit weiß, wie und bei wem er seine Rechte durchsetzen kann.

Technische Umsetzung

Hinsichtlich der technischen Umsetzung stand die Begutachtung des Zusammenspiels und klarer Vorgaben für die einzelnen Dienstleister im Vordergrund. Dabei mussten auch in etablierten Dienstleistungssituationen (COLT als Rechenzentrumsdienstleister, kubus IT als IT-Servicestelle der AOK, KBV als Betreiber des Datennetzes und ABDATA als Rechenzentrumsdienstleister der Apotheken) nachgewiesen werden, dass der neue Service MPS datenschutz-

gerecht gehandhabt wird. Nicht zuletzt wurde auch überwacht, dass der eingebundene Softwareentwickler E44 einen verlässlichen und sicheren Betrieb des MPS ausreichend unterstützt.

Begutachtungszeitpunkt

Die Begutachtung fand vor dem Start und während der Einführungsphase des Projektes statt. Einzelne Aspekte der Begutachtung konnten zu diesem Zeitpunkt noch nicht abschließend geprüft werden. Dort, wo eine konkrete Umsetzung noch nicht prüfbar ist (z. B. Evaluation der Ergebnisse des Modellvorhabens, längerfristige Löschung von Protokollen) werden entsprechende Konzepte und Überwachungsmechanismen geprüft. Insbesondere die Evaluation soll im Anschluss bzw. gegen Ende des Projektes auch Art der Nutzung der Medikationspläne betrachten, deshalb werden auch bestimmte Protokolldaten mitbetrachtet. Die Einhaltung der sich datenschutzrechtlich ergebenden Vorgaben an die Evaluation wird durch den Datenschutzbeauftragten der AOK überwacht.

Die Erprobungsphase ergab eine ausreichende Verfügbarkeit (bzw. eine kurzfristige Wiederherstellung der Verfügbarkeit) der MPS-Daten. Unberechtigte Zugriffsversuche oder die Offenlegung von Daten des MPS konnten nicht festgestellt werden.

Es wird empfohlen, der initialen Zertifizierung des Medikationsplanservers zeitnah eine Nachzertifizierung vor dem Hintergrund der praktischen Umsetzung weiterer Projektphasen folgen zu lassen.

A.12 Sofern das Produkt einen Teil der Anforderungen nur unzureichend erfüllt: Beschreibung, wie dies ausgeglichen wird

Wie festgestellt, befindet sich das Projekt "Medikationsplanserver" in der Einführungsphase, wodurch einzelne Aspekte zur Sicherstellung eines datenschutzgerechten Betriebs noch nicht vollständig und mit Praxisbezug beschrieben sind. Aus diesem Grund erreichen mehrere Kriterien nur den Status "adäquat" statt "vorbildlich", auch wenn der Datenschutz auf "vorbildlichem" Niveau konzipiert ist.

Als unzureichend wird jedoch betrachtet, dass der betroffene Patient zu den ihn betreffenden Zeilen eines Medikationsplanes keine direkte Information zu deren Herkunft erhält. Er kann also nicht direkt erkennen, ob eine Medikationsplanzeile aus (alten) Abrechnungen des Versicherers, aus eigenen Eintragungen des Arztes oder Apothekers oder aus Eintragungen, die er selbst initiiert hat, stammt.

Dem muss der Patient organisatorisch abhelfen, indem er sich den aktuellen Medikationsplan immer direkt bereitstellen lässt und somit erkennen kann, wem die jeweils letzten Änderungen zuzuordnen sind. Zu diesem Aspekt wurde ein separater Punkt in die Patientenbroschüre aufgenommen.

A.13 Beschreibung, wie das IT-Produkt den Datenschutz fördert

Der Medikationsplanserver stellt eine komplexe IT-Serviceleistung dar, die mehrere grundlegende IT-Strukturen des Gesundheitssektors berührt. In den entsprechenden Datenaustausch werden sowohl Praxisverwaltungssysteme der Ärzte (PVS) als auch Apothekenverwaltungssysteme (AVS) einbezogen, zur Anwendung kommt auch das zentreale Datenaustauschsystem der Ärzte, das KV SafeNet (Hier: SNET).

Somit wird im Rahmen der Begutachtung anhand einer an zentraler Stelle positionierten Anwendung nachgewiesen, dass die datenschutzgerechte Umsetzung prüfbar ist. Es ist zu erwarten, dass damit neue Maßstäbe für eine kontrollierbar datenschutzgerechte Umsetzung von IT-Projekten im Bereich der medizinischen Versorgung gesetzt werden. Dieses Gutachten zeigt, dass das trotz der Komplexität der Strukturen, auf die ein medizinisches IT-Produkt aufsetzt, möglich ist.

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Dresden, den 07.05.2018

Dr. Uwe Schwochert