vogel—partner
RECHTSANWÄLTE

Rahmenbedingungen Cloud-basierter Krankenhausinformationssysteme

Wissenschaftliches Gutachten

von

Prof. Dr. sc. hum. Peter Haas

Dr. iur. Uwe K. Schneider

unter Mitarbeit von

David Heieck, LL.B., und Ref. iur. Nils Wiedemann

für das Projekt „KIS & Cloud“ des

Health Innovation Hub
des Bundesministeriums für Gesundheit

Version 1.3 vom 07.01.2021

Büro Stuttgart
Königsbau-Passagen
Königstraße 26
D-70173 Stuttgart
Fon +49 711 24 83 95 200
Fax +49 711 24 83 95 205
info@vogel-partner.eu

Büro Karlsruhe
Technologiepark Karlsruhe
Emmy-Noether-Straße 17
D-76131 Karlsruhe
Fon +49 721 78 20 27 0
Fax +49 721 78 20 27 27
info@vogel-partner.eu

BW Bank Karlsruhe
IBAN: DE74 6005 0101 0002 7431 45
BIC-Code: SOLADEST600

Vogel & Partner Rechtsanwälte mbB
Sitz Karlsruhe – AG Mannheim PR 700160

www.vogel-partner.eu

Vorwort

Dieses Gutachten entstand im Auftrag des „health innovation hub" (hih) des Bundesministeriums für Gesundheit im Zeitraum von Ende Oktober 2020 bis Anfang Januar 2021. Der hih ist Think Tank, Sparring Partner und Umsetzungsunterstützer für innovative Health-IT-Themen und die damit verbundene Digitalisierung im Gesundheitswesen in ihrer ganzen Breite.

In dieser Funktion hat der hih das Thema „Cloud-KIS" auf die Agenda gesetzt und mit der Auftragsvergabe den Impuls dafür gegeben, dass Potenziale, Anforderungen und Lösungsansätze in Bezug auf zukunftsorientierte Krankenhausinformationssysteme als initiale Diskussionsgrundlage zusammengestellt werden. Dezidiert adressierte die Ausschreibung auch das Spannungsverhältnis zwischen gesetzlich Erlaubtem und technisch Möglichem sowie die Fragestellung, was gesetzlich und technisch an Veränderungen und Migrationsprozessen in Deutschland anzugehen ist, um Cloud-KIS und ergänzend moderne digitale Ökosysteme im Gesundheitswesen zu ermöglichen. Entsprechend ist das Gutachten nach den Vorgaben des hih gegliedert und enthält nach einer Einführung zwei Kernteile jeweils zu rechtlichen und technischen Aspekten sowie darauf aufbauend die Kapitel „Vereinbarkeit von Recht und Technik" und – abschließend – „Lösungsvorschläge".

Einerseits ist es erstaunlich festzustellen, wie extrem heterogen die Rechtslage in Deutschland über zwei Jahre nach Geltung der DSGVO noch ist und wie wenig diese die Softwareindustrie motivieren kann, solche innovativen Ansätze wie Cloud-KIS zu verfolgen. Andererseits erstaunt auch, wie weit man technologisch in anderen Branchen beim Cloud-Computing schon ist und wie sich auch in diesem Feld das seit Jahrzehnten zu beobachtende mehrjährige Hinterherhinken der Krankenhaus-IT zeigt. Dabei muss herausgestellt werden, dass das Thema Cloud-KIS zwei mehr oder weniger unabhängige Facetten hat: Einerseits die der Bereitstellungsmodelle und die damit einhergehende „Verschiebung" der Ablaufumgebung für ein KIS von lokalem Betrieb zum Betrieb bei einem Cloud-Dienstleister, andererseits aber auch die Softwarearchitektur eines KIS als modulare Cloud Native Anwendung, mittels der eben nicht nur die Ausschöpfung der Potenziale von Skalierbarkeit, Elastizität und Verfügbarkeit einer Cloud-Infrastruktur möglich ist, sondern auch eine agile Entwicklung und ein zeitnahes Deployment sowie die Integration von Softwarebausteinen vieler Hersteller in Form von „KIS-Plugins". So ergeben sich Vorteile eines Cloud Native KIS auch beim lokalen Betrieb.

Am Ende ist es keine Frage des Ob, auch keine Frage des Wie, sondern eine Frage der radikalen Abkehr von alten Denk- und Technikstrukturen sowie eine Abkehr von Legacy-Geschäftsmodellen, bei denen im Zentrum die Abhängigkeit des Kunden von genau einer Software steht. Die Nutzung von Cloud-KIS in der Fläche ist allerdings auch eine Frage der Anpassung rechtlicher Rahmenbedingungen.

Den zuständigen Mitarbeitern beim hih, Dr. Philipp Kircher und Ecky Oesterhoff, danken wir für die kooperative Zusammenarbeit und die wertvollen Impulse für dieses Gutachten. Dank gebührt auch Kira Schroff für die redaktionelle Unterstützung bei der Anfertigung des Gutachtens, was in dem engen Zeitrahmen nicht immer einfach war.

Uwe Schneider Peter Haas

Inhaltsverzeichnis

1 Executive Summary ... 8
2 Sachverhalt und Fragestellung ... 15
2.1 Krankenhausinformationssysteme (KIS) ... 16
2.1.1 Topologie eines KIS – Verortung von Systemen ... 18
2.1.2 Prinzipielle logische Systemtypen ... 21
2.1.3 Wesentliche Funktionalitäten ... 23
2.1.4 Stand der KIS-Durchdringung in Deutschland ... 24
2.1.5 Datenkategorien in einem KIS ... 26
2.2 Cloud Computing – Historie, Stand und Perspektiven ... 27
2.2.1 Servicemodelle ... 31
2.2.2 Bereitstellungs- und Organisationsmodelle ... 34
2.3 Marktlage im Hinblick auf Cloud-Angebote im KIS-Umfeld ... 36
2.4 Herausforderungen und Motivationen ... 41
2.4.1 Herausforderungen und Motivationen aus der allgemeinen Situation und Entwicklung ... 41
2.4.2 Regulatorische Herausforderungen und Motivationen ... 42
2.5 Chancen und Risiken für Krankenhäuser ... 46
2.6 Fragestellungen des vorliegenden Gutachtens ... 47
3 Rechtliche Anforderungen bzgl. Datenschutz und Schweigepflicht ... 49
3.1 Anforderungen an Cloud-KIS nach der DSGVO ... 49
3.1.1 Anwendbarkeit der DSGVO auf Krankenhäuser ... 49
3.1.2 Cloud-Computing durch Auftragsverarbeiter nach Art. 28 DSGVO ... 50
3.1.3 Cloud-Computing in Drittländern nach Art. 44 ff. DSGVO ... 53
3.1.4 Cloud-Computing durch Anbieter im EWR mit Bezug zu unsicheren Drittländern ... 59
3.1.5 Technische und organisatorische Maßnahmen der Datensicherheit ... 62
3.2 Datenschutzrechtliche Anforderungen an Cloud-KIS nach Bundesrecht ... 64
3.2.1 Bundesdatenschutzgesetz (BDSG) ... 64
3.2.2 Die Regelungen der Sozialgesetzbücher (SGB) ... 64
3.3 Verhältnis von Datenschutzrecht und Schweigepflicht ... 66
3.3.1 Schweigepflicht der Heilberufe und Outsourcing an mitwirkende Personen ... 66

3.3.2 Datenschutz und Schweigepflicht als eigenständige Schranken für die Weitergabe von Patientendaten ... 74
3.3.3 Zusammenfallen von datenschutzrechtlicher Erlaubnis und Offenbarungsbefugnis in Sonderfällen ... 75
3.4 Datenschutzrechtliche Anforderungen an Cloud-KIS in den Bundesländern ... 76
3.4.1 Baden-Württemberg ... 77
3.4.2 Bayern ... 91
3.4.3 Berlin ... 96
3.4.4 Brandenburg ... 103
3.4.5 Bremen ... 107
3.4.6 Hamburg ... 111
3.4.7 Hessen ... 114
3.4.8 Mecklenburg-Vorpommern ... 117
3.4.9 Niedersachsen ... 121
3.4.10 Nordrhein-Westfalen ... 125
3.4.11 Rheinland-Pfalz ... 128
3.4.12 Saarland ... 132
3.4.13 Sachsen ... 138
3.4.14 Sachsen-Anhalt ... 141
3.4.15 Schleswig-Holstein ... 145
3.4.16 Thüringen ... 149
3.4.17 Überblick: Auf Krankenhäuser anwendbares Datenschutzrecht ... 152
3.4.18 Überblick: Anforderungen an die Auftragsverarbeitung für Krankenhäuser ... 158
3.4.19 Überblick: Technische und organisatorische Maßnahmen nach Landesrecht ... 163
3.5 Datenschutzrechtliche Anforderungen an Cloud-KIS in kirchlichen Krankenhäusern ... 164
3.5.1 Vorbemerkung zur Anwendbarkeit der kirchlichen Datenschutzregeln ... 164
3.5.2 Evangelische Kirche ... 165
3.5.3 Katholische Kirche ... 171
3.5.4 Zusammenfassende Bewertung ... 179
4 Technische Anforderungen ... 180
4.1 Befunde auf einen Blick ... 180
4.2 Einführung und Überblick ... 183
4.3 Architektonische Aspekte ... 187
4.4 Cloud-KIS ... 191

4.4.1 SaaS-Cloud-KIS und Ausgangssituation ... 191
4.4.2 Funktionale Modularisierung von KIS ... 194
4.4.3 Cloud-Migration von KIS ... 201
4.4.4 Fallbeispiele für CMSMs ... 205
4.4.5 Kandidaten und Vorgehen ... 210
4.4.6 Die besondere Rolle von Repositories ... 212
4.4.7 Contextmanagement und -handling ... 213
4.4.8 Resultierende Anforderungen ... 215
4.4.9 Konsequenzen und Fazit ... 217
4.5 Cloud-spezifische Anforderungskataloge, Standards und Zertifizierungen ... 219
4.6 Verfügbarkeit, Performance und Skalierbarkeit ... 221
4.6.1 Verfügbarkeit ... 221
4.6.2 Performance und Skalierbarkeit ... 223
4.6.3 Datenverfügbarkeit ... 224
4.6.4 Zusammenfassung und Maßnahmen ... 225
4.6.5 Technische Rahmenbedingungen ... 226
4.7 Datenschutz- und Datensicherheitsmechanismen ... 226
4.7.1 Einführung und Überblick ... 226
4.7.2 Authentifikations- und Berechtigungsmanagement ... 229
4.7.3 Vertraulichkeit gegenüber dem Provider ... 233
4.7.4 Datensicherheitsmechanismen ... 236
4.8 Integritätsaspekte in einem Cloud-KIS ... 237
4.8.1 Einführung ... 237
4.8.2 Datenintegrität ... 239
4.8.3 Entitäten-übergreifenden Patientenidentifizierung ... 241
4.8.4 Funktionsintegrität und Softwareintegrität ... 242
4.8.5 Parametrierungs- und Konfigurationsintegrität ... 243
4.8.6 Authentizität, Zurechenbarkeit und Kontext. ... 244
4.8.7 Integritätsaspekte Zusammenfassung ... 245
4.9 Semantische Interoperabilität ... 245
4.9.1 Einführung ... 245
4.9.2 Semantische Interoperabilität im Gesundheitswesen ... 247
4.9.3 Interoperabilitätserfordernisse für Cloud-KIS ... 248
4.10 Sonstige Aspekte und Anforderungen ... 252

4.10.1 Administration/Cloud-Management ... 252
4.10.2 Compliance-Aspekte ... 253
4.10.3 OH-KIS konforme Mandantentrennung ... 254
4.10.4 Versions- und Patchmanagement ... 256
4.10.5 Technische Revision ... 256
4.10.6 Datenübertragbarkeit ... 257
4.10.7 Migration und Migrationsunterstützung ... 258
4.10.8 Archivfunktion und Archive ... 258
4.11 Potenziale und Chancen durch Cloud-KIS ... 260
4.11.1 Modularisierung und Best of Breed-Ansatz ... 260
4.11.2 Förderung von Innovation und Wettbewerb ... 261
4.11.3 Wirtschaftliche Effekte ... 261
4.12 Digitale Ökosysteme ... 262
5 Vereinbarkeit von Recht und Technik ... 266
5.1 Einführung ... 266
5.2 Rechtliche Anforderungen und Herausforderungen ... 267
5.2.1 Herausforderungen durch unterschiedliche Anforderungen der Landeskrankenhausgesetze ... 268
5.2.2 Herausforderungen durch zusätzliche Anforderungen bei einem Bezug der Auftragsverarbeitung zu unsicheren Drittstaaten ... 269
5.2.3 Herausforderungen durch die Schweigepflicht der Heilberufe ... 271
5.2.4 Herausforderungen bzgl. der Übermittlung von Leistungsdaten nach dem SGB V ... 272
5.3 Resultierende technische Herausforderungen und Umsetzungsmöglichkeiten ... 272
5.3.1 Anonymisierung, Pseudonymisierung oder Verschlüsselung ... 272
5.3.2 Bare-Metal-Server ... 276
5.4 Bewertung der Vereinbarkeit der Anforderungen für den Krankenhaus-Bereich ... 278
5.4.1 Basisanforderungen nach Art. 28 DSGVO ... 278
5.4.2 Verschärfte Erforderlichkeitsprüfung gemäß der Schweigepflicht (§ 203 StGB) ... 278
5.4.3 Unsichere Drittstaaten und schwierige Bundesländer ... 279
6 Lösungsvorschläge ... 281
6.1 Vorschläge für Schaffung einer einheitlicheren und Cloud-freundlicheren Rechtslage ... 281
6.1.1 Angleichung der Regeln zur Auftragsverarbeitung in den Landeskrankenhausgesetzen ... 281

6.1.2 Vereinheitlichung der Regeln zur Auftragsverarbeitung im SGB V 282
6.1.3 Abschaffung von Öffnungsklauseln für Sonderregelungen der Kirchen 282
6.1.4 Rechtliche Vorgaben zur Interoperabilität von KIS und KIS-Modulen 283
6.1.5 Stimulierung der Cloudifizierung von KIS 285
6.2 Vorschläge zur Ausrichtung der technischen KIS-Architekturen auf die Cloud 286
6.3 Vorschläge für mehr Cloud-Souveränität in Deutschland und Europa 289
6.3.1 Entwicklung und Stärkung originär europäischer Cloud-Angebote 289
6.3.2 Cloud nach dem Treuhandmodell 289
7 Abkürzungsverzeichnis 292
8 Abkürzungen der Bundesländer 300
9 Glossar 301
10 Quellenverzeichnis 317

Es wird darauf hingewiesen, dass keine Gewähr dafür übernommen werden kann, dass sich Aufsichtsbehörden oder Gerichte in jedem Fall den im Gutachten vertretenen Rechtsauffassungen anschließen.

1 Executive Summary

Die IT-Welt wandelt sich, viele Unternehmen sind einerseits mit dem eigenständigen Betrieb der immer komplexer werdenden Infrastrukturen und Middleware-Software überfordert, andererseits wachsen eCommerce, elektronische Verkaufsplattformen und Enterprise Informationssysteme immer mehr zusammen. Die Zeit der Cloud-Systeme und -Anwendungen ist angebrochen. Die Legacy-Dinosaurier – also die großen softwaremonolithischen Altsysteme – sterben aus und machen Herden von agilen, intelligent kollaborierenden Software-Kleintieren – den Microservices – Platz. Systemgrenzen verschwimmen, IT-Ressourcen und Software werden nicht mehr gekauft, sondern bedarfsgerecht bezogen und wieder abgestoßen. Kapitalbindung war gestern. Das Vor-Ort-Personal kann sich auf die strategischen und anwendungsbezogenen Aspekte konzentrieren, die Betreuung und technologische Weiterentwicklung der Infrastruktur und Software übernimmt der Servicepartner. Mit kalkulierbaren laufenden Kosten orientiert an der Ressourcennutzung oder der betrieblichen Wertschöpfung (z.B. Anzahl abgewickelter Vorgänge, Fälle) erhält man die neuesten Innovationen zeitnah ins Unternehmen.

Die Vorteile des Cloud-Computings für ein Unternehmen, aber auch die Möglichkeit des Aufbaus Cloud-basierter regionaler, nationaler oder weltumspannender digitaler Ökosysteme, sind auch im Krankenhauswesen von großem Interesse, wenngleich hier eher in einem regionalen Kontext. Dies sowohl für die einzelnen Krankenhäuser, deren IT-Personal durch die sich schnell wandelnden Technologien und die große Themenvielfalt zunehmend überfordert wird, als auch für die Hersteller von Krankenhausinformationssystemen (KIS), bei denen die Größe und Komplexität der Legacy-Software zu abnehmender Handhabbarkeit, zunehmendem Innovationstau und damit sinkender Wettbewerbsfähigkeit führt, und für die Dienstleistungsrechenzentren, die heute Legacy-KIS im Auftrag von Krankenhäusern betreiben. Cloud-Computing für Krankenhäuser bildet sich in Form der Nutzung von Cloud-KIS ab.

Ein Cloud-KIS ist die Summe aller über eine Cloud beziehbaren Plattform- und Software-Ressourcen zur Verarbeitung aller notwendigen Daten zur Unterstützung aller administrativen, logistischen und medizinischen Vorgänge bis hin zum Controlling, dem Qualitätsmanagement sowie dem strategischen Management von Krankenhäusern.

Der Einsatz von Cloud-KIS hat für Krankenhäuser vielfältige Vorteile; hierzu zählen u.a. die Hochverfügbarkeit, das hohe Sicherheitsniveau, die passgenau Orchestrierung der Anwendungsumgebung, ressourcennutzungs- oder wertschöpfungsorientierte Kostenmodelle, die sukzessive Hinzunahme von Funktionalitäten, die Möglichkeit aus verschiedenen alternativen Modulen zu wählen, die Schaffung von Freiräumen für das Vor-Ort-IT-Personal für die Konzentration auf fachliche und strategische Belange der IT im Krankenhaus, der Abbau von Herstellerabhängigkeit, Wegfall der Notwendigkeit zur Installationen und zum Management von Clients sowie die einfache Integration von „Fremdsoftware" in Form von "KIS-Plugins" und Eigenentwicklungen.

Für Cloud-KIS können vor dem Hintergrund bestehender Cloud-Plattformen und -Technologien zwei wesentliche Fragekomplexe adressiert werden:

1. Wie sollte die Software-technische Architektur eines Cloud-KIS beschaffen sein, um die Vorteile des Cloud-Computings ausschöpfen zu können, ab wann könnten Cloud-KIS verfügbar sein? Welche weiteren technischen Aspekte spielen eine Rolle?
2. Welche Regelungen zum Datenschutz sind hierbei zu beachten? Welche Folgerungen ergeben sich aus der ärztlichen Schweigepflicht? Ermöglichen diese rechtlichen Rahmenbedingungen bestimmte Einsatzszenarien oder wird die Nutzung von Cloud-KIS durch sie eingeschränkt?

Damit verbunden ist dann auch die Frage, inwieweit gewisse Bereitstellungmodelle auf Basis weitergehender technischer Absicherungen möglich sind. Diese Fragen werden im Detail in der vorliegenden Expertise behandelt. Wesentliche Befunde sind nachfolgend zusammengefasst:

Zu 1.: Architektur von Cloud-KIS und technische Aspekte

a) Im weitesten Sinne ist der Betrieb von Legacy-KIS des alten Stils auf skalierbaren Infrastrukturen oder Plattformen auch schon Cloud-Computing.

b) Legacy-KIS sind in der Regel keine Webanwendungen, sondern klassische Client-Server-Anwendungen. Bei RZ-Betrieb durch einen Servicepartner erfolgt die Verarbeitung der „fetten Clients" auch im Rechenzentrum und die Benutzung wird mittels Terminalserver bzw. virtualisiertem Desktop auf die Arbeitsrechner gebracht.

c) Legacy-Anwendungen können die skalierenden Infrastruktur- und Plattform-Potenziale des Cloud-Computing nur in eingeschränktem Maße ausschöpfen, zudem handelt es sich um große Software-Monolithen.

d) Aufgrund des technologischen Wandels und der schwindenden Verfügbarkeit alter Technologien werden Legacy-KIS zunehmend verrotten; dieser Prozess hat bereits begonnen.

e) Die Zielprojektion für ein Cloud-KIS ist es, dass für Krankenhäuser bzw. stationäre Einrichtungen jeglicher Art ein skalierbares Set an domänenspezifischen Software-Funktionalitäten zur Verfügung gestellt wird, die je nach Einrichtung und Bedarf bezogen und genutzt werden können.

f) Ein modulares Cloud-KIS ist eine Cloud Native Anwendung, also eine spezifisch für die Cloud entwickelte Anwendung. Ein solches Cloud-KIS stellt eine nutzer- und nutzenzentrierte webbasierte Softwarelandschaft bestehend aus domänenspezifischen, voneinander weitgehend unabhängigen fachlichen und systemtechnischen Microservice-Modulen dar, die von verschiedensten Softwareherstellern stammen können und mittels semantischer Interoperabilität auf Basis geeigneter Mechanismen zusammenarbeiten. Dies bedeutet eine radikale Abkehr von heterogenen, aus abgeschlossenen minimal-interoperablen proprietären Informationssystemen bestehenden, nicht skalier- und orchestrierbaren KIS, wie sie heute allerorten betrieben werden.

g) Cloud-KIS können Basis zur Entwicklung von regionalen digitalen Ökosystemen im Gesundheitswesen sein und auch die einrichtungsübergreifende Leistungsabstimmung und Kooperation sowie die Abwicklung einrichtungsübergreifender Behandlungsprozesse unterstützen. Auf jeden Fall sind sie zentrale Elemente eines solchen Ökosystems.

h) Eine schrittweise Migration von Legacy-KIS hin zu Cloud Native Anwendungen bzw. Cloud Native KIS ist gut möglich. So können neue Funktionalitäten als Cloud Native Anwendungen entwickelt und interoperabel mit dem Legacy-KIS betrieben werden. Der Einbau entsprechender Aufrufschnittstellen in die Legacy-Systeme ist einfach zu bewerkstelligen und eine Notwendigkeit für den Migrationsprozess.

i) Mit dem Krankenhauszukunftsgesetz (KHZG) wurde eine große Chance dahingehend geschaffen, dass für die im neuen § 19 Krankenhausstrukturfonds-Verordnung (KHSFV) benannten Fördergegenstände die Legacy-KIS um Cloud Native Module erweitert werden und damit die ersten Schritte in Richtung Migration erfolgen können.

j) Bei Förderprogrammen zur Digitalisierung im Krankenhaus sollten zukünftig Förderkriterien die Pflicht zur Implementierung als Cloud-fähige Lösung beinhalten, Krankenhäuser sollten bei Ausschreibungen auf die Perspektiven und Planungen des Herstellers bezüglich der „Cloudifizierung" dessen Legacy-Systems achten.

k) Ein großes Potenzial für eine „Cloudifizierung" von digitalen Lösungen bzw. der Realisierung von Cloud Native Anwendungen liegt im Krankenhaus- bzw. Gesundheitswesen in den über viele Jahrzehnte entwickelten Interoperabilitäts- und Semantikstandards – hier vor allem den Standards von HL7 und IHE und DICOM und SNOMED. So kann der HL7-Standard FHIR bzw. die im Rahmen dessen spezifizierten Ressourcen direkt auch für Entwurf und Interoperabilität von Microservices eingesetzt werden, CDA-Dokumente als Persistenzobjekte können als strukturierte und formalisierte Dokumente für die justitiable Dokumentenspeicherung und den Austausch dienen, ebenso für Aggregationsobjekte wie z.B. Gesundheitspässe, Medikationsplan, Impfbuch usw.

l) Die Kenntnisnahme der hoch schutzwürdigen medizinischen Daten durch den Provider ist so weit wie technisch praktikabel zu verhindern bzw. zu erschweren. Gleichzeitig sind hierzu auch vertragliche Regelungen zu treffen und deren Umsetzung regelmäßig zu überprüfen. Kryptographische Verfahren, verteilte Geheimnisse und Trennung der Verwaltung von identifizierenden und medizinischen Daten in verschiedene Anbieter-Plattformen sind mögliche Ansätze. Hier besteht aber weiterer Forschungsbedarf.

m) Wissensgewinnung und Wissensentwicklung können in der Medizin zunehmend nur noch gemeinsam und multizentrisch erfolgen. Cloud-KIS bieten die Chance, Community-Plattformen aufzubauen, die verzahnt mit Cloud-KIS einen solchen gemeinsamen Wissensentwicklungsprozess und ein gemeinsames Wissensmanagement ermöglichen – bei gleichzeitiger direkter kontextsensitiver Aufrufbarkeit und Integration des Wissens in die Cloud-KIS-Funktionalitäten.

Zu 2.: Anforderungen bzgl. Patientendatenschutz und ärztlicher Schweigepflicht

a) Patientendaten geben Auskunft über Gesundheit und Krankheit eines Menschen. Sie bilden einen elementaren Teil seines Schicksals in der Vergangenheit ab und bestimmen auch sein Schicksal in der Zukunft mit. Es ist von elementarer Bedeutung, dass diese Patientendaten zurzeit und am Ort der Behandlung verfügbar sind, dass sie authentisch auf einen oder mehrere Urheber zurückgeführt werden können und unverfälscht (integer) sind. Der Datenschutz erfasst neben diesen Schutzzielen der Verfügbarkeit, Authentizität und Integrität

insbesondere auch noch das der Vertraulichkeit. Denn Patienten müssen grundsätzlich auch darauf vertrauen können, dass ihre Daten nur zur Behandlung genutzt werden und ausschließlich ihren behandelnden Ärzten und – soweit erforderlich – dem Personal, das diese unterstützt, zur Kenntnis gelangen. Bei Preisgabe entsprechender Daten an Stellen außerhalb dieses Behandlungskontextes könnten Diskriminierung am Arbeitsplatz, bei Versicherungen oder im gesellschaftlichen Leben drohen. Auch innerhalb des Medizinbetriebes ist es wichtig und legitim, dass Patienten Zugriffe steuern können, um z.B. eine unbefangene Zweitmeinung sicherzustellen, bei welcher der Arzt, der um die Zweitmeinung gebeten wurde, möglicherweise die Befunde, nicht aber die Diagnosen und Behandlungsvorschläge des bislang behandelnden Arztes kennt.

b) Mittels eines KIS werden keine Schrauben oder sonstige Artikel verwaltet, sondern menschliche Schicksale – abgebildet in den Elektronischen Patientenakten der Krankenhäuser, die einem KIS zugrunde liegen. Dies zeigt die große Verantwortung, welche mit dem Betrieb entsprechender Systeme einhergeht, was auch beim Bezug von KIS aus der Cloud zu beachten ist. Denn KIS enthalten mit die sensibelsten Daten in einer Informationsgesellschaft.

c) Die Nutzung einer Cloud kann viele Vorteile mit sich bringen, sowohl was die leichtere technische Wartbarkeit betrifft, welche zudem Sicherheitsrelevanz haben kann, als auch was die Wirtschaftlichkeit angeht. Gerade im Hinblick auf den Datenschutz besteht jedoch auch die Gefahr, dass sich die Verantwortung für die Verarbeitung sensibler Patientendaten in der Cloud verliert und im Netz Daten diffundieren. Dem ist in jedem Fall durch eine klare und verbindliche Aufgabenteilung zwischen verantwortlichem Krankenhaus und weisungsgebundenem Cloud-Anbieter, durch Transparenz im rechtlichen Sinne, also die Sichtbarkeit und Verortbarkeit von Verarbeitungsvorgängen und Datenspeicherungen auch für das Krankenhaus, sowie durch Abschottung gegenüber unberechtigten Dritten Rechnung zu tragen. Die technischen und organisatorischen Maßnahmen der Datensicherheit müssen dem Stand der Technik entsprechen und den hohen bis sehr hohen Schutzbedarf der Patientendaten und die besonderen Bedrohungen in einer Cloud angemessen widerspiegeln.

d) Entsprechende Maßgaben finden sich auch in der EU-Datenschutz-Grundverordnung (DSGVO), dort u.a. in Art. 32 zur Sicherheit der Verarbeitung, welcher auch Anwendung findet, wenn das Krankenhaus selbst eine „private" Cloud betreibt.

e) Beauftragt das Krankenhaus einen externen Cloud-Anbieter, liegt eine sogenannte Auftragsverarbeitung nach Art. 28 DSGVO vor, der ebenfalls solche Maßgaben enthält. Das Krankenhaus bleibt auch dann im Außenverhältnis, sei es zu Patienten oder Aufsichtsbehörden, vollumfänglich für die Einhaltung des Datenschutzes verantwortlich. Im Innenverhältnis kann das Krankenhaus als Auftraggeber jedoch die Ausführung der Verarbeitung und die Gewährleistung der Datensicherheit nach dem Stand der Technik weitgehend auf den Cloud-Anbieter als weisungsgebundenen Auftragsverarbeiter delegieren. Das Krankenhaus muss den Cloud-Anbieter jedoch sorgfältig im Hinblick auf dessen Garantien für den Datenschutz auswählen und mit ihm klare vertragliche Regelungen gemäß Art. 28 Abs. 3 DSGVO treffen.

f) Befindet sich der Cloud-Anbieter bzw. seine Server jedoch in Drittstaaten, die aus Sicht der EU über kein angemessenes Datenschutzniveau verfügen, weil der Datenzugriff dortiger

Behörden über das nötige Maß hinausgeht, sind weitere Maßnahmen zu treffen. Nach der Aufhebung des Privacy Shield-Beschlusses durch den Europäischen Gerichtshof (EuGH), kann dieser nicht mehr als Grundlage für Datenübermittlungen in die USA genutzt werden. Das stellt eine große Herausforderung für die Nutzung von Cloud-Diensten dar, denn die bislang größten Cloud-Anbieter haben alle ihren Hauptsitz in den USA. Allein ein Vertrag über die Auftragsverarbeitung, auch in Form von Standardvertragsklauseln, wie sie die EU-Kommission genehmigt hat, genügt hierfür nicht mehr. Der Europäische Gerichtshof verlangt zusätzlich, dass Exporteur und Importeur von Daten sowie bei Bedarf die Datenschutzaufsicht prüfen, ob diese Klauseln im Drittstaat auch wirklich eingehalten werden (können). Wenn dies gerade wegen der ausufernden Datenzugriffsmöglichkeiten durch Behörden des Drittstaates, wie nach dem EuGH in den USA, nicht der Fall ist, müssen zusätzliche Maßnahmen ergriffen werden. Dann empfiehlt der Europäische Datenschutzausschuss, in dem alle Aufsichtsbehörden der EU vertreten sind, technische Methoden anzuwenden, die ausschließen, dass personenbezogene Daten im Klartext in den betreffenden „unsicheren" Drittstaat gelangen. Dies bedeutet, dass Maßnahmen wie eine Ende-zu-Ende-Verschlüsselung oder Pseudonymisierung bereits im Krankenhaus angewendet werden müssten und in der Cloud Patientendaten nicht im Klartext verarbeitet werden. Das schränkt die Möglichkeiten, ein KIS oder einzelne Module in eine entsprechende Drittstaats-Cloud auszulagern, merklich ein. Der Betrieb eines kompletten Cloud-Native-KIS in einer entsprechenden Drittstaaten-Infrastruktur ist damit nach dem Stand der Technik nicht möglich. Möglich ist jedoch die Anwendung einer Ende-zu-Ende-Verschlüsselung auf einzelne KIS-Subsysteme wie ein radiologisches Bilddatenarchiv (PACS), das dann auch in eine entsprechende Cloud ausgelagert werden könnte. Gleiches gilt für einen Service aus der Cloud, der Krankenhäuser bei der Generierung pseudonymer Befundtexte unterstützt.

g) Ähnliche Herausforderungen ergeben sich, wenn Patientendaten in eine Cloud in Deutschland oder der EU ausgelagert werden, die von einem Unternehmen mit engen Beziehungen zu unsicheren Drittstaaten betrieben werden. Dies gilt insbesondere für die großen Cloud-Anbieter aus den USA, welche dem dortigen „Clarifying Lawful Overseas Use of Data Act" (kurz: U.S. CLOUD Act) unterliegen. Denn dieses Gesetz gibt öffentlichen Stellen in den USA das Recht, gemäß den dortigen gesetzlichen Vorschriften von Cloud Providern unter ihrer Jurisdiktion Daten anzufordern, auch wenn sich die Daten in anderen Staaten befinden. Eine Zustimmung der Staaten, in denen die Daten sich befinden, ist dabei im Gegensatz zu Rechtshilfeersuchen nicht notwendig. Und der Jurisdiktion der USA unterfallen nach den dortigen Gesetzen v.a. auch Tochterunternehmen von Konzernen mit Hauptsitz in den USA. Damit droht auch hier auf Anordnung öffentlicher Stellen eine Übermittlung in einen unsicheren Drittstaat – und zwar (u.a. entgegen Art. 28 Abs. 3 Unterabs. 1 Buchstabe a DSGVO) unabhängig von einer Weisung oder Zustimmung des Krankenhauses oder von einer gesetzlichen Verpflichtung nach dem Recht der EU oder ihrer Mitgliedstaaten. Dies stellt gerade vor dem Hintergrund des nach deutschem Recht für Patientendaten bestehenden Beschlagnahmeschutzes (§ 97 StPO) ein nicht unerhebliches Risiko dar, so dass ergänzende Maßnahme wie bei einer Drittstaatsübermittlung getroffen werden sollten. Neben einer Ende-zu-Ende-Verschlüsselung oder Pseudonymisierung kommt hier aber auch ein sogenanntes Datentreuhandmodell in Betracht, bei dem ein rein oder schwerpunktmäßig europäisches Unternehmen als Treuhänder der Patientendaten auf der in Europa belegenen

technischen Infrastruktur fungiert, auf welcher Cloud-Plattformen von US-Anbietern laufen. Als Datentreuhänder müsste dieses Unternehmen im Auftrag des Krankenhauses sämtlichen Zugriffe auf diese Infrastruktur von Seiten des Cloud-Anbieters kontrollieren und ggf. restringieren, v.a. was Datenabflüsse in die USA angeht.

h) Zudem müssen Krankenhäuser die Schweigepflicht nach § 203 StGB beachten. Ohne gesonderte Vorschriften, die gerade ein Offenbaren von Patientendaten durch Ärzte oder anderes in die Behandlung involviertes Personal erlauben, dürfen Patientendaten demnach nur dann sonstigen mitwirkenden Personen, wie Cloud-Anbietern, offengelegt werden, wenn dies für die Auslagerung einer Tätigkeit erforderlich ist (§ 203 Abs. 3 S. 2 StGB). Wenn nun ein komplettes KIS in die Cloud ausgelagert werden soll und lokal nur noch "Thin Clients", z.B. in Form von Browsern, vorgehalten werden sollen, wird man nach dem Stand der Technik in der Regel davon ausgehen können, dass diese Offenlegung erforderlich ist. Sollen lediglich Subsysteme oder einzelne Funktionalitäten wie z.B. AMTS-Prüfungen eines KIS in die Cloud outgesourct werden, kann sich dies anders darstellen, da hier dann nach wie vor eine Ende-zu-Ende-Verschlüsselung oder eine Pseudonymisierung in der ohnehin noch vorhandenen IT-Infrastruktur des Krankenhauses vor Ort möglich und zumutbar sein kann. In jedem Fall ist der Cloud-Anbieter bzw. sein Personal gemäß § 203 Abs. 4 StGB vom Krankenhaus auf die Schweigepflicht zu verpflichten; ein Verstoß auch durch das Personal des Cloud-Anbieters wäre für dieses strafbar.

i) Das SGB V enthält teilweise auch für Leistungserbringer in der GKV Vorschriften zur Auftragsverarbeitung bei der Übermittlung von Leistungsdaten zur Abrechnung mit der GKV. Dies gilt bspw. auch für Krankenhäuser zur Abrechnung ambulanter Notfälle mit der Kassenärztlichen Vereinigung (§ 295a Abs. 3 SGB V). Für die Abrechnung stationäre Fälle durch Krankenhäuser nach § 301 SGB V fehlt es jedoch an einer entsprechenden Regelung, was das Outsourcing von Abrechnungsmodulen in die Cloud rechtlich im Unklaren lässt.

j) In rechtspolitischer Hinsicht sollte der Bundesgesetzgeber daher im SGB V eine einheitliche Befugnis zur Auftragsverarbeitung bei der Übermittlung von Abrechnungsdaten für alle Leistungserbringer in der GKV schaffen.

k) Überdies ist nach geltendem Recht das jeweilige Landeskrankenhausgesetz (LKHG) des Bundeslandes zu prüfen, in welchem das Krankenhaus seinen Sitz hat. Hier zeigt sich ein sehr heterogenes Bild, was die Anforderungen an die Auftragsverarbeitung angeht. Rheinland-Pfalz lässt die Auftragsverarbeitung für Krankenhäuser z.B. in seinem LKHG explizit unter den Voraussetzungen des Art. 28 DSGVO zu, was somit auch eine eigenständige Offenbarungsbefugnis im Sinne von § 203 Abs. 1 StGB darstellen dürfte, so dass keine Erforderlichkeitsprüfung nach § 203 Abs. 3 S. 2 StGB nötig ist. Andere Bundesländer, wie z.B. Bayern, erlauben das Outsourcing von Patientendaten zu Behandlungszwecken nur an andere Krankenhäuser, nicht jedoch an professionelle Cloud-Anbieter, was dazu führt, dass dies in Bayern allenfalls unter Verwendung der bereits beschriebenen zusätzlichen Schutzmaßnahmen wie Ende-zu-Ende-Verschlüsselung oder Pseudonymisierung bereits im Krankenhaus möglich ist.

l) Abschließend sei darauf hingewiesen, dass die Bundesländer in legislatorischer Hinsicht die Vorschriften zur Auftragsverarbeitung in ihren LKHG angleichen sollten, damit ein einheitlicher und effizienter Markt für Cloud-KIS in Deutschland entstehen kann, der es unter klaren rechtlichen Rahmenbedingungen ermöglicht, die Vorteile des Cloud-Computing auch für Krankenhäuser zu erschließen. Die Bundesländer sollten dabei auch ihre bisher teils in den LKHG existierenden Öffnungsklauseln für Regelungen der Kirchen zum Datenschutz streichen, da der Patientendatenschutz in kirchlichen Krankenhäusern keine innere Angelegenheit der Kirchen ist und auf diese Weise die rechtliche Komplexität im Sinne einer klaren Rechtslage und stringenten Rechtsdurchsetzung reduziert wird.

Der Einsatz von Cloud-Computing hat viele Vorteile, die in Zukunft für Krankenhausinformationssysteme erschlossen werden sollten. Auch können Cloud-KIS ein wichtiger Bestandteil zukunftsorientierter digitaler Ökosysteme im Gesundheitswesen sein. Eine Modernisierung sowie Harmonisierung der rechtlichen Rahmenbedingungen des Bundes und der Länder, um die entsprechenden Chancen besser nutzen, gleichzeitig aber Risiken minimieren zu können, ist vor diesem Hintergrund dringend anzuraten.

2 Sachverhalt und Fragestellung

Bessere Informationen und bessere Informationssysteme sind die Grundlage für Verbesserung von Effektivität, Effizienz, Qualität und Patientensicherheit – auch im Krankenhaus.

In allen Industrienationen ist man daher bemüht, die Informatisierung im Gesundheitswesen und im für die Versorgung wichtigen stationären Sektor voranzutreiben – zum Teil mit Förderprogrammen oder Strafzahlungen bei Nichterfüllung gewisser Kriterien oder Fähigkeiten. So hat das Bundesministerium für Gesundheit mit verschiedenen Gesetzen – unter anderem mit dem Krankenhauszukunftsgesetz (KHZG) – wichtige Entwicklungen angestoßen und Impulse gesetzt. Krankenhäuser und die von ihnen betriebenen Legacy-Systeme sehen sich zunehmend neuen Anforderungen und Herausforderung bezüglich der Interoperabilität und neuer innovativer Funktionalitäten konfrontiert, nicht nur aufgrund der Gesetzeslage, sondern auch aufgrund der technologischen Fortschritte und Möglichkeiten, Prozess und Dokumentation aber auch direktes medizinisches Handeln umfassend digital zu unterstützen bzw. durchzuführen.

Krankenhäuser sind in ihrer Komplexität ein Mikrokosmos der gesamten Gesundheitsversorgung. In ihrer Breite und Differenziertheit hinsichtlich Organisation und Dokumentation sowie der komplexen rechtlichen und finanzierungstechnischen Rahmenbedingungen sind sie kaum mit irgendeinem anderen Wirtschaftsbetrieb ähnlicher Größenordnung zu vergleichen. Dementsprechend sind die Anforderungen an die gesamtbetrieblichen Informationssysteme für ein Krankenhaus – allgemein als Krankenhausinformationssysteme (im Folgenden mit KIS abgekürzt) bezeichnet – extrem hoch, da Breite und Tiefe der KIS-Funktionalitäten sowie die Anforderungen an Datenschutz und -sicherheit sehr hoch sind. Man denke allein schon an die unzähligen medizinischen Formulare selbst in kleinen Krankenhäusern, die digital adäquat abzubilden sind oder an die komplexen Abrechnungs- und Nachweispflichten. Auch die zu unterstützenden Prozesse sind komplex und nicht – wie z.B. in der Industrie – für jeden „Stückprozess" vollständig standardisierbar, da jeder Patient ein Individuum mit besonderer individueller bio-psycho-sozialer Situation und Behandlungserfordernissen ist. Medizinische Behandlungen am Fließband sind weder medizinisch noch ethisch vertretbar. Mit dieser Variantenvielfalt auch beim Prozessmanagement müssen unterstützende KIS ebenso adäquat umgehen können.

Die letzten 25 Jahre haben gezeigt, dass die heterogenen und auf einzelnen Client-Server-Systemen basierenden KIS hinsichtlich Entwicklung, Wartung, Betrieb und Vor-Ort-Betreuung sowie Integrationsmanagement an ihre Grenzen stoßen und die Innovationsgeschwindigkeit stetig abnimmt. In vielen anderen Branchen wurde inzwischen aus diesen Gründen der Weg zu komponentenbasierten serviceorientierten Architekturen und Webanwendungen vollzogen.

„Mit Verbreitung moderner und leistungsfähiger Browser sowie schneller Internetverbindungen lohnt sich der Einsatz einer Client-zentrierten Webanwendung. Durch ihre performante und komfortable Interaktion mit den Anwendern lösen sie immer häufiger auch leistungsfähige lokal installierte Anwendungen ab, die aufwändig installiert und nur mittels Updates aktuell gehalten werden können. Durch ihre geringen technischen Voraussetzungen sind Client-zentrierte Webanwendungen ferner häufig das Mittel der Wahl, um plattformunabhängige Cloud-Anwendungen zur Verfügung zu stellen. Zudem reduziert die Verlagerung der Prozesslogik, weg vom Server hin zum Client, die Anforderungen an einen Server. Dies ermöglicht es,

bei gleichem Funktionsumfang Anwendungen kostengünstiger zu betreiben bzw. besser auf steigende Nutzerzahlen zu reagieren."[1]

Damit können heute einrichtungsübergreifende Bestell-, Produktions- und Lieferketten effektiv und transparent abgewickelt werden. Die Bürger erleben und erfahren dies jeden Tag. So sind inzwischen auch die betriebsinternen Enterprise Systeme vielerorts verteilte Systeme mit hoher Skalierbarkeit und Komponier- bzw. Orchestrierbarkeit. Große Branchensoftware-Hersteller gründen ihren Erfolg auf diesen Ansatz bzw. die Migration ihrer ehemals proprietären softwaremonolithischen Systeme in komponenten-/modulbasierte serviceorientierte Systeme, die wahlweise lokal oder teilweise oder ganz in der Cloud betrieben werden können. Manche seit vielen Jahren allgemein benutzte Client-Software im Bürobereich oder für das eLearning wird heute schon nur noch als Cloud-Anwendung angeboten. Gegenüber anderen Branchen finden sich Webanwendungen und Cloud-Lösungen aber im Gesundheitswesen bisher eher selten und überhaupt nicht als Enterprise-Lösungen z.B. für Krankenhäuser, sondern lediglich einzelne Subsysteme sind inzwischen auch als Webanwendungen und Cloud-fähig verfügbar.

In diesem Sinne dürfte der Krankenhausbranche ein Paradigmenwechsel bevorstehen, der sich mit einer Verzögerung von 10 Jahren zu anderen Branchen auch für KIS vollziehen könnte, da die Web- und Cloud-basierter Lösungen in vielerlei Hinsicht große Vorteile haben.

2.1 Krankenhausinformationssysteme (KIS)

Krankenhausinformationssysteme sind gesamtbetriebliche Informationssysteme für Krankenhäuser zur **Unterstützung aller administrativen, logistischen und medizinischen Vorgänge** bis hin zum Controlling und dem Qualitätsmanagement – und dies für Krankenhäuser jeglicher Größe und Art. In diesem Sinne gehören auch viele Medizintechnikgeräte zum KIS, die zunehmend auch digital sind, integriert werden und einen Datenaustausch unterstützen.

Dabei können vielfältige strategische und operative Ziele für ein KIS sowie resultierende Nutzenpotenziale angegeben werden.[2]

Moderne, effektive und qualitativ hochwertige Patientenversorgung und Krankenhausmanagement sind ohne Informatik-Unterstützung nicht mehr denkbar. Neben der Effektivierung der vielfältigen abteilungsinternen und abteilungsübergreifenden Prozesse steht gleichrangig die zeitnahe Transparenz der Patientensituation und -befunde auf Basis einer KIS-integrierten institutionellen Elektronischen Patientenakte im Mittelpunkt, um die Qualität, den Outcome und die Patientensicherheit zu verbessern. Nachgeordnete Verwendungszwecke der klinischen Daten für das Controlling und die Abrechnung sind ebenfalls von hoher Bedeutung.

Ein KIS umfasst neben den Datenübertragungsnetzen und den notwendigen Servern mit den entsprechenden Betriebssystemen auch die Middleware wie z.B. Datenbanken und die stationären und mobilen Endgeräte sowie die Anwendungssoftware. Während man verkürzt also mit „KIS" nur oft alle informationstechnischen Ressourcen in einem Krankenhaus meint, gehen am

[1] Bitkom e.V., Entwicklung erfolgreicher Webanwendungen. 2015. S. 8

[2] Eine Zusammenstellung von Zielen und Potenzialen eines KIS findet sich bei Haas/Kuhn: Krankenhausinformationssysteme: Ziele, Nutzen, Topologie, Auswahl; in: Kramme (Hrsg.) Informationsmanagement und Kommunikation in der Medizin, Kap. 2.2, S. 21 f.

Menschen orientierte Definitionen darüber hinaus und betrachten Informationssysteme als soziotechnische Systeme. Hier umfasst dann ein betriebliches Informationssystem zusätzlich alle organisatorischen Regelungen und die das IT-System nutzenden Menschen – die personellen und maschinellen Aufgabenträger machen also in Summe das funktionierende betriebliche Informationssystem aus.[3]

Die sehr differenzierte Aufbau- und Ablauforganisation in Krankenhäusern – aber auch die komplexen Finanzierungs- und Abrechnungsspezifika – erfordern sehr komplexe Informationssysteme mit vielfältigen und vielschichtigen Funktionalitäten. Dabei hat sich historisch mit Blick gerade auf diese differenzierte Komplexität der Funktionalitäten z.B. für einzelne Teilbereiche wie medizinische Institute oder Fachabteilungen aber auch spezielle administrative Aufgaben gezeigt, dass nicht ein einziger Softwarehersteller alle diese Funktionalitäten in der notwendigen Breite und Tiefe herstellen und pflegen kann, sodass sich neben den **Kernsystem-Anbietern** auch **Spezialsystemanbieter** für bestimmte Abteilungen oder sehr spezielle betriebliche Aufgaben etabliert haben. So haben heute die Krankenhäuser mit zunehmender Größe und Komplexität mehrere bis viele meist auf Basis des internationalen Standards HL7[4] interoperierende Informationssysteme im Einsatz, wobei es sich zumeist um eine nachrichtenbasierte *lose Kopplung* handelt. Man spricht dann von einem „heterogenen KIS", welches alle Merkmale eines verteilten Systems[5] hat. In der Regel gibt es aber herausgehoben ein **administratives und ein klinisches Kernsystem**, um die sich dann die einzelnen sogenannten **Subsysteme** anordnen und mit den Kernsystemen je nach Erfordernissen interoperieren. Historisch wird der strategische Ansatz, einen optimalen – aber auch minimalen – Mix unterschiedlicher Systeme zur bestmöglichen Unterstützung der einzelnen Aufgabenbereiche einzusetzen, als „Best of Breed"-Ansatz bezeichnet.

Aufbau und Betrieb eines heterogenen Informationssystems stellen hohe Anforderungen an die fachliche Breite und Tiefe des Know-how des IT-Personals. Hier stoßen kleine bis mittlere Krankenhäuser immer mehr an ihre Grenzen, da die Vielfalt der Themen, Technologien und Komplexität ständig zunimmt.

Daneben bringt der Einsatz mehrerer Systeme mit sich, dass bestimmte Daten – vor allem die Patientenstamm- und Falldaten, aber auch medizinische Daten und Befunde – redundant in diesen Systemen gehalten und in geeigneter Weise gegenseitig synchronisiert werden müssen. Diese Synchronisation erfolgt heute meist mittels klassischem Nachrichtenaustausch, z.B. mittels HL7-Nachrichten auf Basis einer zentralen Nachrichtenaustauschinfrastruktur („Kommunikationsserver"). Ein Trend zur Serviceorientierung, z.B. mittels des ebenfalls von der Normierungsorganisation HL7 herausgegebenen Standards FHIR, ist jedoch erkennbar. Dieses Integrationsmanagement stellt hohe Anforderungen an die IT-Abteilungen. Letztendlich müssen viele Stammdaten in allen diesen Systemen auch manuell redundant gepflegt werden.

[3] Siehe bei Gabriel zum Begriff des Informationssystems in der Enzyklopädie der Wirtschaftsinformatik Online Lexikon unter https://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/uebergreifendes/Kontext-und-Grundlagen/Informationssystem/index.html.

[4] HL7: Digitale Standards im Gesundheitswesen. https://hl7.de/.

[5] Coulouris/Dollimore/Kindberg: Verteilte Systeme, S. 17 ff.

2.1.1 Topologie eines KIS – Verortung von Systemen

Für Krankenhausinformationssysteme ergibt sich eine System- bzw. eine Anwendungslandschaft, für die topologisch bzw. mit Blick auf die logische Systemsicht – also unabhängig von der technischen Implementierung z.B. in verschiedenen Servern, virtuellen Maschinen oder in einem technischen System - im Grunde **vier Sichtweisen** eingenommen werden können:

- Verortung eines Systems bzw. eines Softwaremoduls in der Informationssystempyramide nach Scheer[6]
- Verortung eines Systems bzw. eines Softwaremoduls in der logischen Krankenhausorganisationsstruktur
- Verortung eines Systems bzw. eines Softwaremoduls nach betrieblicher Ebene
- Klassifikation nach dem Charakter: horizontal, teilhorizontal oder vertikal.

Dabei spielt es einerseits eine Rolle, welche Systeme eher kooperieren oder eher aufeinander aufbauen und andererseits was der *betriebliche Gegenstandsbereich* eines Systems ist.

Sichtweise 1: Verortung in der Informationssystempyramide

Schon 1995 formulierte Scheer: „Management-Informationssysteme setzen Dispositionssysteme voraus, die die Datenbasis erzeugen, auf die dann entsprechende Verdichtungsprozeduren zur Ermittlung von Führungsinformationen zugreifen."[7] Vor diesem Hintergrund skizzierte Scheer die Informationssystempyramide, ein Schichtenmodell, das einerseits verdeutlicht, wie Systeme aufeinander aufbauen, andererseits aber auch, wie die operative Bedeutung der einzelnen Systeme „von unten nach oben" abnimmt, und gegenläufig die strategische Bedeutung zunimmt. Informationssysteme auf einer höheren Ebene können in der Regel aber ohne jene auf der unteren Ebene nicht sinnvoll betrieben werden, da sie auf die Daten der darunter liegenden Systeme angewiesen sind. In Anlehnung an Scheer ergibt sich für ein Krankenhaus die nachfolgend gezeigte Informationssystempyramide.

[6] S. Scheer: Wirtschaftsinformatik

[7] Scheer: Wirtschaftsinformatik Referenzmodelle für industrielle Geschäftsprozesse. 1995

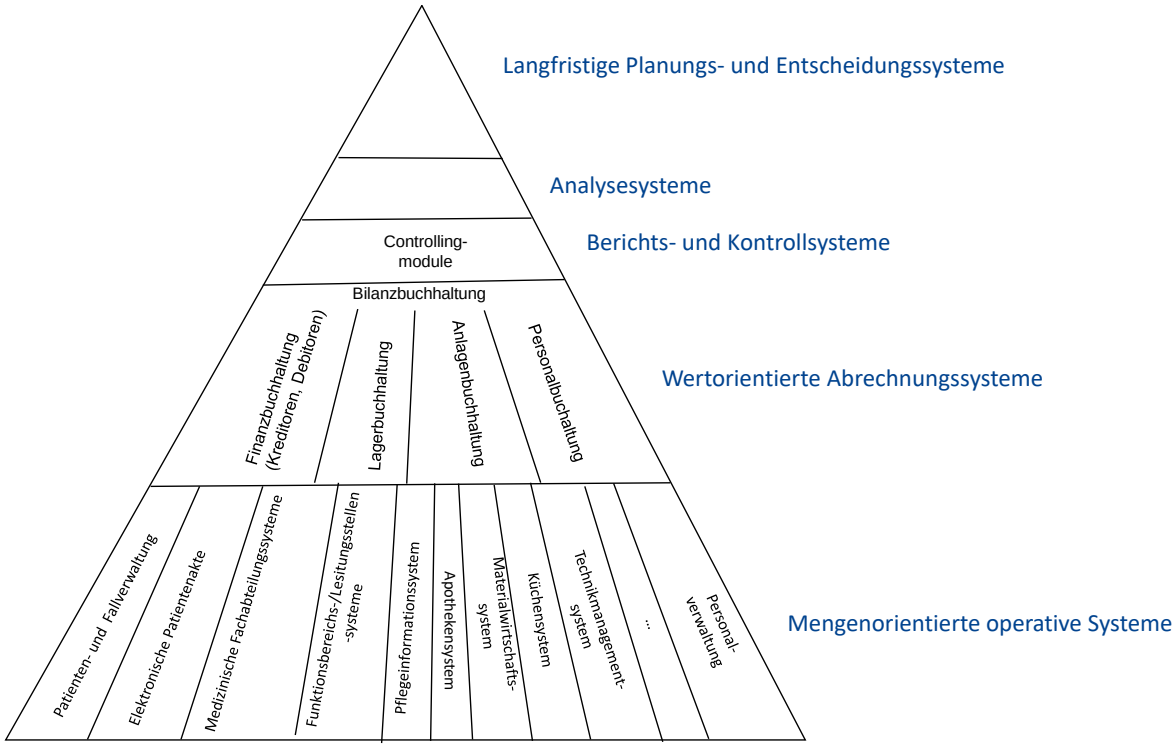

Abbildung 2-1: Informationssystempyramide nach Scheer adaptiert für das Krankenhaus

Sichtweise 2: Verortung nach Krankenhausabteilungen

Mit Blick auf die verschiedenen betrieblichen Bereiche im Krankenhaus kann die nachfolgend gezeigte Topologie angegeben werden. Hier zeigt sich, wo Systeme für welche betrieblichen Bereiche eingesetzt werden.

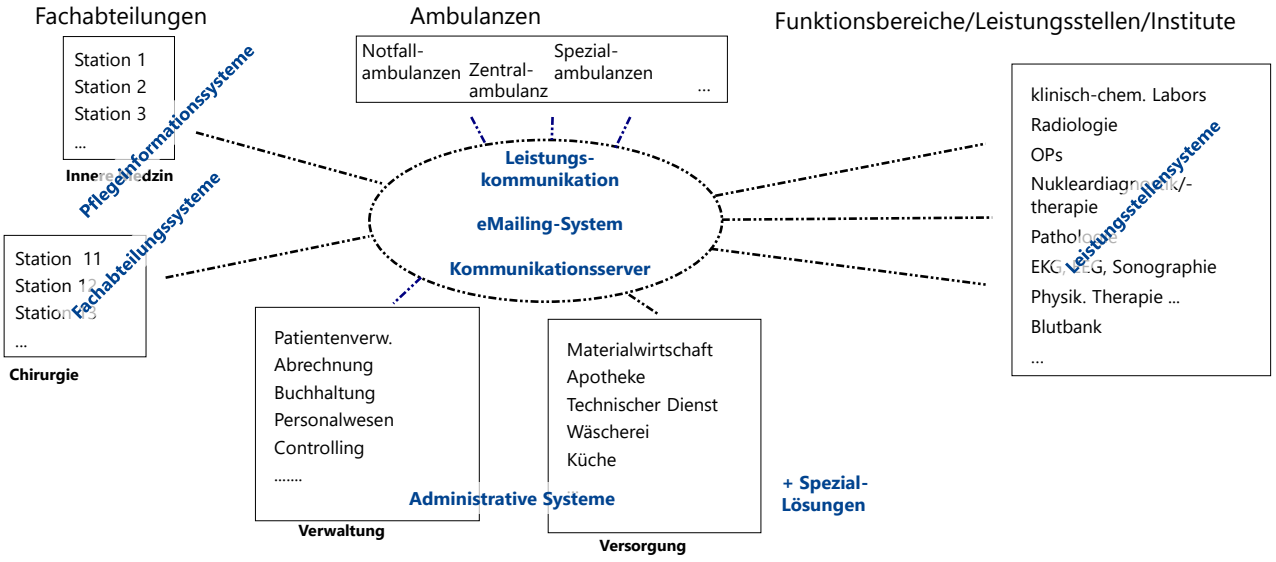

Abbildung 2-2: Logische Krankenhausorganisation und typisierte Topologie eines KIS[8]

[8] In Anlehnung an Haas/Kuhn: Krankenhausinformationssysteme: Ziele, Nutzen, Topologie, Auswahl; in: Kramme (Hrsg.) Informationsmanagement und Kommunikation in der Medizin, Kap. 2.2, S. 29.

Sogenannte *Subsysteme* – d.h. in sich gekapselte und autonom betreibbare spezialisierte Informationssysteme kommen vor allem in größeren Leistungsstellen/Funktionsbereichen und für spezielle administrativ-/logistische Abteilungen zum Einsatz. Ansonsten bieten die KIS-Kernsysteme ebenfalls Grundfunktionalitäten für die einzelnen Fachabteilungen und Funktionsbereiche. Subsysteme müssen in geeigneter Weise mit dem Kernsystem und gegebenenfalls anderen Systemen interoperieren können.

Sichtweise 3: Verortung nach betrieblichen Ebenen

Neben dieser an den globalen Aufgabenbereichen orientierten Betrachtung können aber auch die betrieblichen Ebenen wichtig sein, denn manche Software- bzw. Anwendungssysteme sind auf der Arbeitsplatzebene angesiedelt, andere ganz oben auf Unternehmensebene.

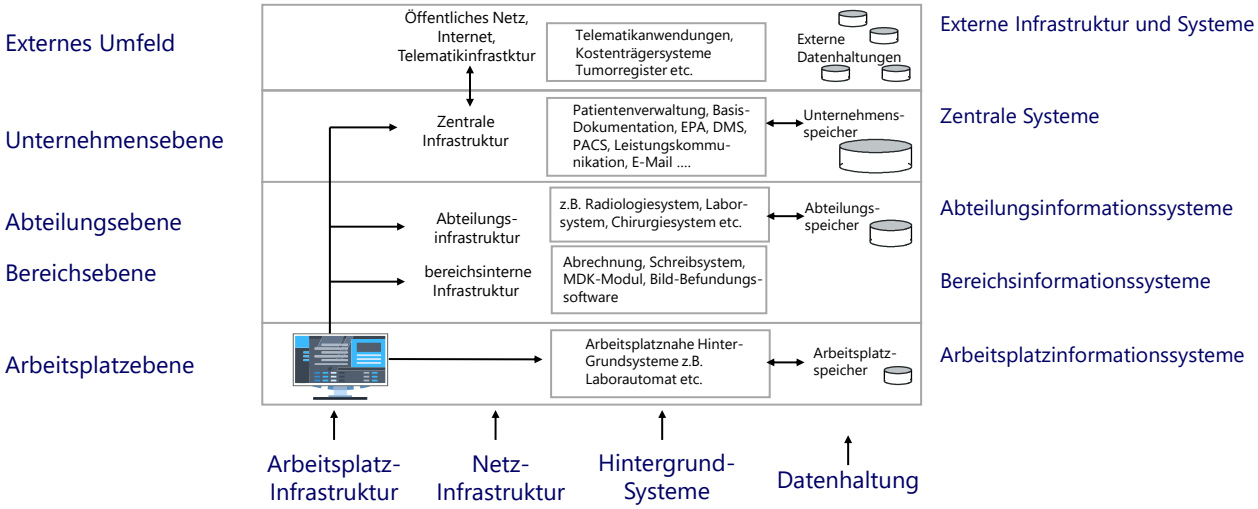

Abbildung 2-3: Verortung von Systemen nach betrieblicher Ebene

Vorangehende Abbildung macht deutlich, dass Abteilungsinformationssysteme selbst wieder aus Software/Systemen für Arbeitsbereiche oder Arbeitsplätze oder die ganze Abteilung bestehen können. Dabei müssen in der Regel auch hier – wie bei der Pyramide nach Scheer – Systeme der unteren Ebenen in jenes der darüberliegenden Ebene integriert werden. Bereichsinformationssysteme, sind dabei selten eigene Systeme, sondern Module im entsprechenden Abteilungsinformationssystem.

Sichtweise 4: Verortung nach Art

Sind Informationssysteme nicht speziell für eine bestimmte betriebliche Organisationseinheit zugeschnitten (vertikale Systeme), sondern stellen Funktionalitäten in gleicher Weise für viele verschiedenartige oder alle Organisationseinheiten zur Verfügung, spricht man auch von Querschnittsanwendungen bzw. horizontalen Systemen[9]. Die Betrachtung vertikal und horizontal kann auch auf der Granularitätsstufe der betrieblichen Ebene aus der zuvor geschilderten Sichtweise erfolgen. Beispiele: Textverarbeitungssysteme und E-Mailing sind horizontale Systeme

[9] „Als horizontale Standardsoftware wird diejenige Standardsoftware bezeichnet, die unabhängig von einer aufbauorganisatorischen Zuordnung an Arbeitsplätzen eingesetzt werden kann. Hierzu gehören bspw. Systeme zur Textverarbeitung, Tabellenkalkulation, Grafikerstellung, DTP (Desktop-Publishing) oder Dateiverwaltung (Office Software)." Quelle: http://einkauf.oesterreich.com/IV2_SS05/bestehendehp%FCberarbeitet/Horizontale_standardsoftware.htm.

auf Arbeitsplatzebene, die Bildbefundungssysteme vertikale Systeme für die radiologische Bildbefundung. Gerade im Krankenhaus kann es aber auch sein, dass Systeme „teilhorizontal" sind, d.h. sie stellen Funktionalitäten für einige verschiedenartige Abteilungen zur Verfügung, aber nicht für alle. So ist ein Picture Archiving and Communication System (PACS) für alle betrieblichen Bereiche nutzbar, in denen durch bildgebende Verfahren Bilder und Videos entstehen. In der Regel müssen horizontale Systeme in die vertikalen Systeme eingebunden bzw. damit interoperabel gemacht werden. So müssen z.B. die durch eine horizontal genutzte Textverarbeitung entstandenen Texte natürlich in die Dokumentation des im Kontext genutzten Abteilungssystems integriert werden.

2.1.2 Prinzipielle logische Systemtypen

Als Konsequenz können daher verschiedene **Informations-/Softwaresystemtypen** angegeben werden, die heute den vielfältigen Markt an Software / Anwendungssystemen für Krankenhäuser kennzeichnen und die je nach Ausprägung dann ein konkretes heterogenes KIS in einem Krankenhaus ausmachen[10]:

Kernsysteme

- **Administratives Kernsystem** mit stationärer Patientenstamm- und Falldatenverwaltung, stationärer Abrechnung, und ggf. ambulanter Abrechnung, mit allen werteorientierten Systemen und Kontroll- und Analysesystemen, oftmals integriert
- **Medizinisches Kernsystem** mit Order-Entry/Result-Reporting, klinische Patientenakte mit Formulargenerator/-tool, Patiententerminbuchung/-management und ggf. Pflegeinformationssystem

Daneben gibt es in der Regel Spezialsysteme für bestimmte Abteilungen und (Funktions-)Bereiche (oft als Abteilungsinformationssysteme bezeichnet) oder für bestimmte Spezial-Aufgaben. Hierbei können wieder solche für Administration und Logistik von jenen für den medizinischen Bereich unterschieden werden.

Administrative und versorgungsbezogene Abteilungsinformationssysteme

Neben den Modulen des administrativen Kernsystems haben sich auch dedizierte Subsysteme für einige Verwaltungsabteilungen bzw. zentrale Abteilungen etabliert. Hier sind vor allem Materialwirtschaftssysteme, Apothekeninformationssysteme, Küchensysteme, Blutbanksysteme und Instandhaltungsmanagementsysteme zu nennen.

Medizinische (Fach-)Abteilungsinformationssysteme

Fachabteilungssysteme unterstützen in spezialisierter Weise die fachärztliche Organisation und Dokumentation sowie die dieser nachgeordneten Verwendungszwecke wie Qualitätsmanagement, Nachweispflichten, Abrechnung usw. innerhalb der medizinischen Fachabteilungen. Zunehmend unterstützen diese auch ein Behandlungsmanagement und integrieren entscheidungsunterstützende Funktionalitäten. Beispiele sind Chirurgieinformationssysteme, Anästhesieinformationssysteme, Gynäkologieinformationssysteme und Urologieinformationssysteme.

[10] Eine Übersicht von Produktgruppen z.B. für Software für das Krankenhaus findet sich im Produktgruppenverzeichnis der Leitmesse DMEA unter https://www.virtualmarket.dmea.de/de/produkte-produktgruppen.

Neben der Dokumentation unterstützen sie den ärztlichen Entscheidungsprozess durch die schnelle Verfügbarmachung neuester Befunde auf Basis des krankenhausweiten Leistungskommunikationssystems und der institutionellen EPA (iEPA), ermöglichen aber auch zunehmend den Zugriff auf an das KIS angekoppelte Wissensbasen und elektronische Lehrbücher. Mittels eines Behandlungsplanungsmoduls erlauben sie fachabteilungsspezifisch, problem- oder diagnosebezogene Behandlungsstandards in Form von klinischen Pfaden zu hinterlegen und bei konkreten Behandlungen als Planungsgrundlage zu nutzen.

Oftmals werden die notwendigen Funktionalitäten im Rahmen der Ausgestaltung spezieller Dokumentationsmasken mit einem Formulardesigner innerhalb des medizinischen Kernsystems realisiert und zur Verfügung gestellt, womit es sich dann eher um Module des Kernsystems denn um eigene Subsysteme handelt.

Eine besondere Stellung nimmt hier das **Pflegeinformationssystem** ein, das im Grunde als „teilhorizontales System" für eine bestimmte Berufsgruppe über alle Fachabteilungen hinweg betrachtet werden kann, da in der Regel in allen Fachabteilungen das gleiche System zum Einsatz kommt. Mittels dem Pflegeinformationssystem werden die Pflegeplanung, Pflegedokumentation und die Kurvenführung und das pflegerische Qualitätsmanagement unterstützt.

Medizinische Funktionsbereichs-/Leistungsstellensysteme

Funktionsbereichssysteme unterstützen in integrierter Weise die Organisation, Dokumentation und Kommunikation in Leistungs- Funktionsstellen oder Instituten; einerseits durch spezielle Dokumentationsfunktionalitäten und die effektive Abwicklung der speziellen Workflows, andererseits aber auch durch die Einbindung spezieller bereichsspezifischer medizintechnischer Komponenten wie z. B. die Online-Anbindung von Laboranalysegeräten an das (Laborinformationssystem) LIS oder der bildgebenden Modalitäten an das Radiologieinformationssystem (RIS) bzw. das PACS mit Integration mit dem RIS. Leistungsstellen, in denen direkt Patienten untersucht werden, benötigen auch ein effektives Terminmanagement, sodass diese Systeme auch oft eine Terminkalenderverwaltung haben.

Beispiele für Systeme die Terminkalender bzw. Termin-Arbeitsplatzlisten beinhalten können sind das Laborinformationssystem, Radiologieinformationssystem, Operationsdokumentationssystem, Pathologieinformationssystem (PathIS), Anästhesieinformationssystem und OP-Informationssystem.

Arbeitsplatzsoftware/-systeme

- Diagnosen-Codiersoftware
- Bildbetrachtungs-/Befundungssoftware
- Büro-Software
- Spracherkennungssoftware
- Spezielle Auswertungssoftware für arbeitsplatzbezogene Aufgaben
- KAS – Klinisches Arbeitsplatzsystem

Spezialsoftware

- Tumordokumentationssystem
- Data Warehouse für Controlling und Analyse

- DRG-Grouper – Software für die Abrechnung zur Ermittlung von Diagnosis Related Groups aus den medizinischen Daten
- AMTS-Software – Software zur Überprüfung der Arzneimitteltherapiesicherheit
- MDK-Modul – Software für die Dokumentation von Aspekten für und Kommunikation mit dem Medizinischen Dienst der Krankenkassen
- Patientenportal – Software zur Ermöglichung der Patientenpartizipation in vielfältiger Weise

Horizontale allgemeine Systeme

Horizontale Systeme unterstützen in generischer Weise bestimmte Aspekte und können durch Parametrierung an das spezifische Einsatzumfeld angepasst werden. Beispiele hierfür sind Dokumentenmanagementsysteme (DMS), Archivsysteme, Picture Archiving and Communication Systems , Spracherkennung, eMailing/Kommunikationssysteme, Wissensmanagementplattformen, die Rote Liste, ggf. Terminplanungsmodule.

Technisches Integrationssystem: Der Kommunikationsserver

Ein besonderes Anwendungssystem ist der Kommunikationsserver, der eine Middleware darstellt, um die Integration der verschiedenen Systeme bzw. deren semantische Interoperabilität zu vereinfachen und auch im laufenden Betrieb die technisch-/logische Kommunikation zwischen den Systemen zu überwachen. Über diesen laufen alle Datenaustausche zwischen den Systemen, wobei dabei auch Protokollumsetzungen oder Semantikübersetzungen vorgenommen werden können. Auch ist ein „Multicasting" möglich, das heißt eine Nachricht kann an mehrere Empfänger geschickt werden. So ist es heute üblich, dass nach Aufnahme eines neuen Patienten seine demographischen Daten und die zugehörigen Falldaten an die wesentlichen medizinischen Subsysteme wie z.B. LIS und RIS übermittelt werden.

2.1.3 Wesentliche Funktionalitäten

Die Summe der einzelnen Anwendungssysteme, die für ein Krankenhaus das gesamtbetriebliche KIS ausmachen, stellen eine große Zahl an Einzelfunktionalitäten zur Verfügung. Wie Abbildung 1 zeigt, sind es vor allem die mengenorientierten Systeme, die die Grundlage für die weitere Verarbeitung und das Krankenhausmanagement liefern. Dabei geht es sowohl im administrativen wie im medizinischen Bereich erste einmal um vielfältige Dokumentationsfunktionalitäten, sodann aber auch um Funktionalitäten für die Verarbeitung der dokumentierten Daten, für die Organisationsunterstützung (z.B. Bestellwesen, Terminmanagement, Workflowmanagement), die Kommunikationsunterstützung und die Entscheidungsunterstützung.

Tabelle 2-1: *IT-Unterstützungsdimensionen und beispielhafte KIS-Funktionalitäten*[11]

Unterstützungsdimension	Beispiele
Verarbeitungsunterstützung	▪ Lohn- und Gehaltsabrechnung ▪ Kosten-/Leistungsrechnung ▪ Administrative Auswertungen ▪ Ermittlung der abrechenbarer DRG ▪ Ermittlung fallbezogener Prozesskosten

[11] In Anlehnung an Haas/Kuhn: Krankenhausinformationssysteme: Ziele, Nutzen, Topologie, Auswahl; in: Kramme (Hrsg.) Informationsmanagement und Kommunikation in der Medizin.

Unterstützungsdimension	Beispiele
Verarbeitungsunterstützung	▪ Kalkulation von Deckungsbeiträgen ▪ Berechnung diagnosegruppenbezogener Kostenverteilungen ▪ (Fortwährende) Berechnung wesentlicher statistischer Maßzahlen wie mittlere Verweildauer, Auslastung usw. ▪ DRG-Ermittlung ▪ Erstellung von (gesetzlich vorgeschriebenen) Statistiken und Nachweisen ▪ Berechnung medizinischer Scores ▪ Medizinische Statistiken ▪ Bestrahlungsplanung ▪ AMTS-Prüfungen
Dokumentationsunterstützung	▪ Bestellungen und Liefereingänge ▪ Beschäftigungsverhältnisse und Mitarbeiterstammdaten ▪ Patientenfälle nach Fallarten ▪ abrechnungsorientierte Diagnosen- und Prozedurdokumentation (DRG-Dokumentation) ▪ klinische Diagnosedokumentation ▪ Dokumentation der durchgeführten Maßnahmen mit zugehörigen Befunden so z.B. auch die Operationsdokumentation, Anästhesiedokumentation, Laborwertdokumentation, Bestrahlungsdokumentation u.v.a.m. ▪ Symptomdokumentation ▪ Dokumentation wesentlicher Vorfälle und Vorkommnisse ▪ Medikationsdokumentation ▪ Arztbriefschreibung, Epikrisendokumentation … integriert in einer Elektronischen Krankenakte
Organisationsunterstützung	▪ Terminpläne/Ressourcenbelegungsplanung in Ambulanzen und Funktionsbereichen ▪ Bettenbelegungsplanung auf Station ▪ OP-Planung ▪ Workflowmanagement zur Unterstützung der Abwicklung von Untersuchungsaufträgen und der Dokumenten-/Befunderstellung ▪ Anwendung von klinischen Pfaden und Behandlungsstandards ▪ Überwachung der Vollständigkeit und Zeitnähe der Abrechnungsdokumentation ▪ Wiedervorlage-Organisation
Kommunikationsunterstützung	▪ gebundene betriebliche Kommunikation in Form der Leistungsanforderung und Ergebnisrückmeldung (Leistungskommunikation, „order entry/result reporting“) ▪ Übermittlung von Falldaten an Krankenkassen gemäß §301 SGB V ▪ Übermittlung von Entlassbriefen an die einweisenden Ärzte ▪ interne betriebliche Email-Kommunikation
Entscheidungsunterstützung	▪ kontextsensitiver Zugriff auf Fakten- und Wissensbasen ▪ klinische Erinnerungsfunktionen („Reminder“) und Warnhinweise ▪ kontextsensitive patientenzentrierte Checklisten ▪ AMTS-Prüfung ▪ Prüfung von verordneten Maßnahmen auf Kontraindikationen ▪ kontextsensitive Laborwertwertüberwachung ▪ Bild- und Signalauswertung und Bewertung

Weitere Betrachtungen zur funktionalen Zergliederung finden sich in Kapitel 4.4.2.

2.1.4 Stand der KIS-Durchdringung in Deutschland

Die Geschichte der Krankenhaus-IT begann in den 70er-Jahren des vorigen Jahrhunderts im Rahmen des Förderprogrammes DOMINIG der Bundesregierung. Erste administrative Verfahren entstanden zu dieser Zeit. Die Umstellung auf kaufmännische Buchführung 1978 zwang viele Krankenhäuser zur ersten Einführung von KIS-Modulen. Ab Mitte der 80er-Jahre entstanden dann die ersten dedizierten Subsysteme und lokal betreibbare „autonome“ Krankenhaussysteme. Zur Beschreibung des Durchdringungsgrades von Krankenhäusern mit IT haben sich

weltweit zwei Assessments etabliert: einerseits das Electronic Medical Record Adoption Model (EMRAM), ein Stufenmodell[12] der Healthcare Information and Management Systems Society (HIMSS), einer Non-Profit-Organisation; und andererseits das "Digital Health most wired Survey"[13], das ursprünglich von der American Hospital Association (AHA) entwickelt wurde und nun vom College of Healthcare Information Management Executives (CHIME) gepflegt wird. Beide Modelle verfolgen verschiedene Ziele und haben unterschiedliche Kriterien, die jedoch auf den Nutzungsgrad bestimmter KIS-Funktionalitäten aufsetzen.

In 2017 ergab sich für die deutschen Krankenhäuser folgendes Bild[14], wobei sich deutliche Unterschiede zwischen kleinen Krankenhäusern unter 200 Betten mit einem Mittelwert von 1,3 und Häusern über 500 Betten mit einem Mittelwert von 3,4 zeigten.[15]

Tabelle 2-2: Reifegrad KIS in deutschen Krankenhäusern 2017 nach EMRAM Stufenmodell

Stufe	Kriterien	Anteil der KH in D [%]
7	Lückenlose elektronische Patientenakte integriert in alle klinischen Bereiche (z. B. Ambulanz, Intensivstation, Notaufnahme), die alle (medizinischen) Papierakten ersetzt; Einsatz von Standards zum Datenaustausch für die integrierte Versorgung; Data Warehouse als Basis für klinische und betriebliche Analysen.	0,0
6	Klinische Dokumentation interagiert mit intelligenter klinischer Entscheidungsunterstützung (basierend auf diskreten Datenelementen) UND Vorhandensein eines IT-gestützten, geschlossenen Medikationsprozesses (closed loop medication).	1,2
5	Integrierte Bildmanagementlosung (z. B. PACS) ersetzt alle filmbasierten Bilder.	18,0
4	Elektronische Verordnung mit klinischer Entscheidungsunterstützung in mindestens einem klinischen Bereich und für Medikation.	5,4
3	IT-gestützte klinische Dokumentation sowie Einsatz elektronischer Verordnungen durch Ärzte bzw. Pflegepersonal. Dies beinhaltet auch die Dokumentation der Medikamentengabe (eMAR).	9.0
2	Eine elektronische Patientenakte (bzw. ein Clinical Data Repository) ermöglicht die Zusammenfassung und Normalisierung von Daten aus verschiedenen klinischen Quellen im gesamten Krankenhaus.	26,9
1	Informationssysteme für die großen diagnostischen und versorgenden Abteilungen (Labor, Radiologie, Apotheke) sind installiert.	1,2
0	Informationssysteme für die großen diagnostischen und versorgenden Abteilungen (Labor, Radiologie, Apotheke) sind **nicht** installiert.	38,3
	N	167
	EMRAM-Mittelwert	2,3

Inzwischen wurde das EMRAM-Modell noch arrondiert, wobei weiterhin die Granularität der Kriterien inhomogen ist und von ganzen Subsystemen bis zu einzelnen speziellen Funktionalitäten reicht.

[12] S. https://www.himssanalytics.org/emram.

[13] S. https://chimecentral.org/chime-most-wired-2/.

[14] Klauber et al: Krankenhaus-Report 2019. Springer open 2019, S. 23.

[15] Die EMRAM-Stufen bilden an sich eine Ordinalskala, d.h. einen nur näherungsweise quantifizierten Gradmesser der Digitalisierung im Krankenhaus: je höher die Stufe, desto höher der Digitalisierungsgrad. Anders als bei Intervallskalen kann man allerdings nicht davon ausgehen, dass zwischen den Skalenpunkten (Stufen) quantitativ exakt gleiche Abstände herrschen. Von daher eignen sich die EMRAM-Stufen streng genommen nicht oder allenfalls bedingt für die Bildung eines Mittelwertes. Ein anteilsgewichteter Mittelwert wird hier wie auch in anderen Publikationen gleichwohl zur annähernden Veranschaulichung des durchschnittlichen Digitalisierungsgrades angegeben.

2.1.5 Datenkategorien in einem KIS

In einem KIS werden sehr verschiedene Datenkategorien verwaltet. Dies geschieht in den zuvor beschriebenen Systemen – zum Teil auch redundant. So werden Laborergebnisse sowohl im Laborinformationssystem gespeichert als auch im klinischen Kernsystem und dort in der Patientenakte.[16] Ist das Pflegeinformationssystem ein eigenes Anwendungssystem, so werden wesentliche Parameter auch dort nochmals gespeichert.

Beispielhafte Datenkategorien sind:

- Demographische und kontextuelle Angaben zum Patienten (Stammdaten zum Patienten, Angehörige, behandelnde Ärzte usw.)
- Falldaten zu den stationären oder ambulanten Behandlungsfällen
- Abrechnungsdaten abgeleitet aus den medizinischen Daten oder originär erfasste für die stationäre und ambulante Abrechnung mit gesetzlichen Kassen oder Privatpatienten.
- Granulare medizinische Behandlungsdaten wie Diagnosen, Symptome, durchgeführte Maßnahmen, Behandlungsziele, medizinische Scores
- Daten zur psycho-sozialen Situation des Patienten
- Daten zu verschiedenen Assessments (pflegerische, indikationsbezogene)
- Vielfältige Erhebungs- und Befunddokumente von den verschiedenen Anamnesen über Befunde aus den Funktionsbereichen wie Laborbefunde, Röntgenbefunde bis hin zu OP-Berichten und Entlassbriefen.
- Daten über die Pflege des Patienten von der Pflegeanamnese über die Pflegeeinstufung bis hin zu konkreten Pflegemaßnahmen
- Behandlungspfade
- Systemstammdaten zu Organisationen wie Kostenträgern, Arztpraxen, Krankenhäusern, Sozialdiensten u.v.a.m.
- Systemstammdaten zu Krankenhausstruktur und Organisation.
- Daten zu den Beschäftigten (Personaldaten)
- Apothekenartikelstamm- und -bewegungsdaten
- Materialstamm- und -bewegungsdaten
- Finanzdaten, Buchhaltungsdaten
- Daten zu technischen Geräten und Anlagen
- Vielfältige Semantikkataloge sowohl medizinischer als auch administrativer Art, so z.B. ICD und OPS aber auch viele andere bereichs-/systemspezifische attributbezogene Kataloge und Wertelisten

Je nach Heterogenitätsgrad des KIS werden diese Daten dediziert in verschiedenen Systemen oder in den Kernsystemen verwaltet und gehalten. Oftmals müssen die Daten auch in verschiedenen Systemen redundant gehalten werden. So sind z.B. die Laborergebnisse sowohl im Laborinformationssysteme als auch im medizinischen Kernsystem vorhanden.

[16] Zu den Datenkategorien bzw. Informationsobjekten in einem eEPA-System: Haas, Elektronische Patientenakten. 2017.S. 120 ff.

Mit Blick auf die vorangehende Liste wird deutlich, dass es sich zum Großteil um Gesundheitsdaten, also um besondere Kategorien von Daten im Sinne der DSGVO handelt, die auch besonders zu schützen sind und deren Offenbarung großes Schadenspotential für die Betroffenen in sich bergen.

Mit Blick auf die Vielfältigkeit der Daten, Systeme und Benutzergruppen und Benutzer kommt einem differenzierten *Zugriffsrechtemanagement* besonders hohe Bedeutung zu, damit alle Beschäftigten nur jene Daten einsehen bzw. eingeben und ändern dürfen, die sie für die betriebliche Aufgabenerfüllung brauchen. Umfangreiche Anforderungen an Datenschutzmechanismen wurden vom Arbeitskreis Gesundheit und Soziales sowie Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet und in der sogenannten Orientierungshilfe Krankenhausinformationssysteme (OH-KIS) niedergelegt.[17]

2.2 Cloud Computing – Historie, Stand und Perspektiven

Der Einsatz von Informatik-Technologien zur Unterstützung und zur (Teil-)Automatisierung von Vorgängen ist heute in allen Lebensbereichen präsent – sei es im betrieblichen als auch privaten Umfeld. Kämpfte man z.B. bei der Programmierung vor 40 Jahren noch um jedes Bit, stehen heute technische IT-Ressourcen auf allen Ebenen schier unermesslich zur Verfügung. Die **Miniaturisierung** aller Komponenten bei gleichzeitiger **Leistungs- und Durchsatzsteigerung aller Komponenten** – seien es Prozessoren, Speichermedien und Netzwerkkomponenten für Fest- und Mobilnetze – hat zu einem „Second Machine Age" geführt, vergleichbar mit der industriellen Revolution durch die Dampfmaschine.[18] Dabei können mit Blick auf die technische Entwicklung und Ausgestaltung von Systemen und die betriebliche Datenverarbeitung in den Unternehmen genau genommen drei Entwicklungs-Phasen unterschieden werden:

1. Mit Verfügbarkeit von **Großrechner-Systemen**, die von wenigen Technologiekonzernen gefertigt wurden, zogen Systeme in die Betriebe ein, deren Software vollständig auf diesen ausgeführt und über Terminals durch die Benutzer genutzt wurden. Auch der Einzug der sogenannten „mittleren Datentechnik" änderte daran wenig. Krankenhäuser betrieben erste Systeme für die Krankenhausverwaltung (KOLK, MAIK) basierend auf den Ergebnissen des DOMINIG -Förderprogrammes[19] der Bundesregierung in Rechenzentren, vor allem in den damals für diesen Bereich vorherrschenden kommunalen Rechenzentren.
2. Im August 1981 brachte IBM den ersten Personal Computer auf den Markt, 1983 folgte die LISA von Apple und mit Maus und WYSIWYG-Prinzip[20] brach ein neues Zeitalter für die ergonomische Benutzung von Softwareanwendungen an. Nach und nach erkannte

[17] Zu finden u.a. unter https://www.datenschutzzentrum.de/artikel/1107-OH-KIS-Orientierungshilfe-Krankenhausinformationssysteme.html. Diese Arbeiten, welche zur OH KIS der Datenschutzkonferenz führten, wurden u.a. durch ein Urteil des Europäischen Gerichtshofes für Menschenrechte (EGMR) gegen Finnland initiiert (EGMR, Urt. v. 17.07.2008 – 20511/03 (I. ./. Finnland)); s. dazu auch Schneider, Einrichtungsübergreifende elektronische Patientenakten, S. 255 ff.

[18] Vgl. Brynjolfsson/McAfee: The Second Machine Age. 2018. S. 19.

[19] Zum Hintergrund siehe Schneider/Schönberger: Datenverarbeitung im Gesundheitswesen. 1976. S. 7 ff.

[20] Grafische Benutzeroberfläche nach dem Prinzip: „What You See Is What You Get".

auch die Informatik-Industrie die Vorteile von Arbeitsplatzrechnern vor allem für benutzernahe und aufgabenangemessene Software und das – auch für KIS heute noch vorherrschende – Konzept der **Client-Server-Systeme** entstand und wurde zum vorherrschenden Paradigma für betriebliche Informationssysteme. Neben den Großrechnern wurden nun auch Server verfügbar, die von Firmen und öffentlichen Einrichtungen lokal betrieben werden konnten. In diesem Zusammenhang entstanden auch die ersten sogenannten „autonomen Krankenhausinformationssysteme" die nun nicht mehr in Rechenzentren, sondern nun auch in Krankenhäusern vor Ort betrieben wurden.

3. Die Internettechnologie und Softwareframeworks zur Entwicklung von funktionalen Websites und hochfunktionalen **Web-Anwendungen und Web-Systemen** haben ab dem Jahr 2005 zunehmend zur Implementierung von Softwareprodukten geführt, deren Merkmal zwar noch die Client-Server-Architektur ist, bei denen der Client aber nur noch zur Darstellung der Benutzeroberfläche dient bzw. nun auch wieder zunehmend zur Ausführung bestimmter Oberflächen-bezogener Logik auf Basis von HTML5 und JavaScipt – mit clientseitiger Verarbeitungslogik dann auch als Rich Internet Applications (RIA) oder Client-zentrierte Webanwendung bezeichnet. Architekturansätze für Webanwendungen folgen derzeit der 3-Schichten- oder 4-Schichten-Architektur[21]
4. Ab dem Jahr 2012 wurde im größeren Rahmen das Konzept von Microservice-basierten Systemen diskutiert und befördert durch Virtualisierung und die Containerisierung von kapselbaren Funktionalitäten und die Idee des Domain Driven Design und verfügbarer Plattformen zunehmend umgesetzt.

„Durch ihre geringen technischen Voraussetzungen sind Client-zentrierte Webanwendungen ferner häufig das Mittel der Wahl, um plattformunabhängige **Cloud-Anwendungen** zur Verfügung zu stellen."[22]

Die wertvollsten Firmen der Welt sind heute IT-Technologie- bzw. Plattform-Unternehmen, deren Erfolg aus dem Einsatz von Webanwendungen in der Cloud auf Basis beliebig skalierbarer Infrastrukturen resultiert.

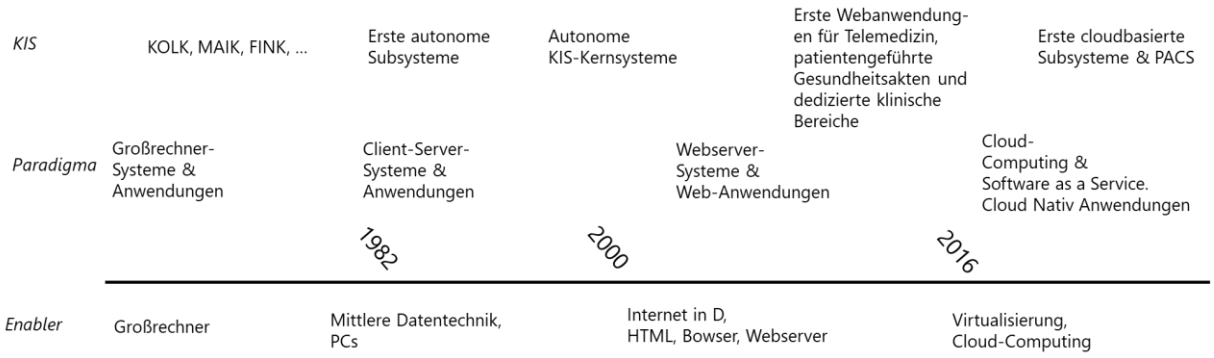

Abbildung 2-4: Die 4 Phasen der betrieblichen Datenverarbeitung zur Cloud hin

Mit Web-Anwendungen und den Virtualisierungstechnologien wird es für Unternehmen der IT-Branche attraktiv, Cloud Computing und Software als Service dem Markt anzubieten bzw.

[21] Bitkom: Entwicklung erfolgreicher Webanwendungen. 2015. S. 6.

[22] Bitkom: Entwicklung erfolgreicher Webanwendungen Leitfaden Webentwicklung 2015. S. 8.

zur Verfügung zu stellen. Für die Kunden wird der ggf. belastungsadaptierte Bezug von Ressourcen und Software ebenso immer attraktiver, da die wachsenden Anforderungen an Rechenleistungen und Speicherkapazitäten aber auch an die Funktionalitäten immer weniger durch lokale inflexible Infrastrukturen abgebildet werden können. Auch die Kooperation mit Partnern und Kunden kann durch Webanwendungen und Cloud-Lösungen besser und agiler bewerkstelligt werden. Vor diesem Hintergrund formulierte der damalige Bitkom-Präsident bereits im Jahr 2013:

„Ungeachtet aller Herausforderungen wird sich Cloud Computing, davon bin ich fest überzeugt, in der Breite durchsetzen. Die technischen und wirtschaftlichen Vorteile sind einfach zu groß."[23]

Mell und Grance[24] haben 2011 eine allgemeine Definition vorgelegt, die weitgehend akzeptiert ist: „**Cloud computing** is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models".

Ebenso benennen Mell und Grance als wesentliche Charakteristika, in diesem Sinne auch Vorteile: On-demand self-service, Broad network access, Resource pooling, Rapid elasticity und Measured service.

„Durch scheinbar unendliche IT-Ressourcen, die auf Abruf bereitgestellt oder auch wieder „zurückgegeben" werden können, entsteht für Unternehmen eine äußerst flexible und skalierbare Hard- und Softwareinfrastruktur."[25]

Für Web-Anwendungen als Basis für Software as a Service ergeben sich weitere Vorteile, wie

- Cross-Device Kompatibilität
- Funktionalität der Software überall und jederzeit verfügbar
- Einfache Installation, keine Client-Installationen notwendig
- Einfacher und kostengünstiger Rollout in der Fläche
- Skalierbarkeit
- Kostengünstige Entwicklung durch freie Verfügbarkeit vielfältiger Frameworks und Bibliotheken
- Aufwandsarmes Deployment von Softwareänderungen (BugFixes, Releases, Weiterentwicklungen)
- Updates können im laufenden Betrieb benutzerunabhängig eingespielt werden
- Benutzer erhalten/haben immer die aktuellste Version der Software
- Absicherungsmaßnahmen (Datenschutz & Datensicherheit) der Software können vom Hersteller/Betreiber übernommen werden

[23] Bitkom-Präsident Prof. Kempf in Wie Cloud Computing neue Geschäftsmodelle ermöglicht. Bitkom 2013, S. 8.

[24] Mell/Grance: The NIST Definition of Cloud Computing. 2011, S. 2.

[25] Hentschel/Ley: Cloud Computing: Status quo, aktuelle Entwicklungen und Herausforderungen, in: Reinheimer: Cloud Computing. 2016. S. 3.

- Reduzierung der Wartungsaufwände allgemein (nur Serverwartung statt Wartung aller Clients)
- Einfaches, kollaboratives, zeitgleiches Zusammenarbeiten an Texten, Vorgängen etc.

Daneben entwickeln sich Webframeworks nachfragegetrieben rasant[26] und enthalten inzwischen auch Funktionalitäten für Sicherheitsaspekte, sodass sich Entwickler nur noch begrenzt um solche Implementierungsaspekte kümmern müssen.

Im Allgemeinen wird davon ausgegangen, dass Cloud-Computing der wesentliche Lösungsansatz ist, um die Bewältigung des technologischen Fortschritts zu meistern bzw. die Nutzbarmachung moderner Technologien und Anwendungen in der Fläche für Unternehmen jeglicher Größe zu ermöglichen. So können heute neben den großen Unternehmen auch besonders vom Ein-Mann-Unternehmen über kleinere Handwerksbetriebe bis hin zu kleinen und mittelständischen Unternehmen von diesem Ansatz profitieren und Funktionalitäten nutzen, die ihnen beim Betrieb lokaler Client-Server-Anwendungen eher verbaut wären.

Hin zur Entwicklung von Cloud-Anwendungen gab und gibt es aber zwei weitere wesentliche technische Enabler:

Serviceorientierte bzw. Microservice-basierte Architekturen und daraus zusammengesetzte komponentenbasierte Systeme für gesamte Softwaresysteme („Service-orientierte Architekturen, kurz SOA), sind das abstrakte Konzept einer Software-Architektur, in deren Zentrum das Anbieten, Suchen und Nutzen von Diensten über ein Netzwerk steht. Diese Dienste werden plattformübergreifend von Applikationen oder anderen Diensten genutzt. Ein wesentlicher Vorteil einer SOA ist die Unabhängigkeit von der jeweiligen Implementierung. Dies ermöglicht eine funktionale Zerlegung der Anwendungen und erleichtert eine prozessorientierte Betrachtungsweise. Teilprozesse oder Dienste können über das Netzwerk angesprochen werden. Im Idealfall ist sogar eine einfache Integration ganzer Anwendungen möglich."[27] Für funktional skalierbare Software as a Service-Angebote und für eine innovative und sich rasch entwickelnde Anwendungssystemlandschaft sind SOA bzw. Microservices unabdingbarer Nährboden. Dabei ist die Modularisierung von Anwendungen beliebig granular umzusetzen, wirr aber zunehmen mit Blick auf kapselbare Anwenderfunktionalitäten auf Basis von maximaler Kohäsion und loser Kopplung umgesetzt.

Virtualisierung: Auch die Virtualisierung und Containerisierung hat die vergangenen 20 Jahre einen Siegeszug durchlaufen, im Rahmen dessen verfügbare Virtualisierungssoftware und Management-Instrumente immer perfekter und teilweise frei verfügbar wurden. Damit ist eine Entkopplung von Anwendungssystemumgebungen von der technischen Serverbasis gegeben, was in jeder Hinsicht die Modularisierung von Systemlandschaften und deren Betrieb und Management erleichtert. Trotzdem kann eine virtuelle Komponente genutzt und wie ein physisches Pendant betrachtet werden. Im Grunde können große Systeme und Anwendungslandschaften wie eine Menge von Containern betrachtet werden, die beliebig und dynamisch zu in sich funktionierenden Gesamtgebilden assembliert werden können.

[26] Eine Liste findet sich unter https://de.wikipedia.org/wiki/Liste_von_Webframeworks.

[27] Melzer: Service-orientierte Architekturen mit Web Services. 2010, S. 9.

Daneben sind weitere Treiber für modaler und responsive Anwendungen die Entwicklungen bei den mobilen Endgeräten, das Web 2.0 und leistungsfähige Browser sowie breitbandiges Internet zu nennen. Responsive Anwendungen, die auf jedem Gerät vom stationären Großbildschirm bis zum kleinen Handy optimal genutzt werden können, sind heute das Mittel der Wahl für moderne Softwareanwendungen und zur Zurverfügungstellung von Funktionalitäten in allen betrieblichen Bereichen und Situationen.

Die Nutzung von Cloud-Computing kann die Agilität und Flexibilität von Unternehmen ganz erheblich verbessern und ermöglicht den raschen Auf- und Abbau betrieblicher Funktions- bzw. Servicebereiche. Daneben ist auch bei entsprechender Standardisierung von Schnittstellen – hier Services – auch eine Skalierbarkeit der Beauftragung des Betriebs von Teilen der oder der gesamten eigenen Infrastruktur an verschiedene Dienstleister nach dem Prinzip der Kosten-/Nutzen-Bewertung möglich, ohne Abstriche bei der Leistung der Summe der Teile hinnehmen zu müssen.

Für das Cloud-Computing werden verschiedene Service- und Bereitstellungmodelle angegeben.

2.2.1 Servicemodelle

Servicemodelle beschreiben, welche Art von Ressourcen von einem Dienstleister als Service angeboten werden. Allgemein gesehen können dabei sehr verschiedene Aspekte als Service angeboten werden, in einer Literaturanalyse zeigen Duan et. al. die verschiedenen vielfältigen Ausprägungen[28] und nehmen eine Klassifizierung der verschiedenen aaS-Konzepte vor. Deutlich wird dabei die inflationäre Nutzung der „aaS"-Begrifflichkeiten – auch für Leistungen, die ehemals einfach Miet- oder Leasingmodelle waren.

Im Folgenden sollen nur noch „aaS"-Modelle betrachtet werden, die eng verbunden mit dem Betrieb von Anwendungssystemen und Anwendungssystemlandschaften sind. Hierzu stellt sich im Grunde die Frage, welche physikalischen und softwaretechnischen Artefakte eines Anwendungssystems bzw. einer Anwendungssystemlandschaft, die sich aus der Summe der Anwendungssysteme eines Unternehmens ergibt, in welcher Granularität in die Cloud verschoben werden können. Die Beantwortung dieser Frage kann vor dem Hintergrund der Schichten eines Anwendungssystems bzw. des IT-Stacks erfolgen.

[28] Duan et. al.: Various „aaS" of Everything as a Service. https://www.researchgate.net/publication/285236871_Various_%27aaS%27_of_everything_as_a_service

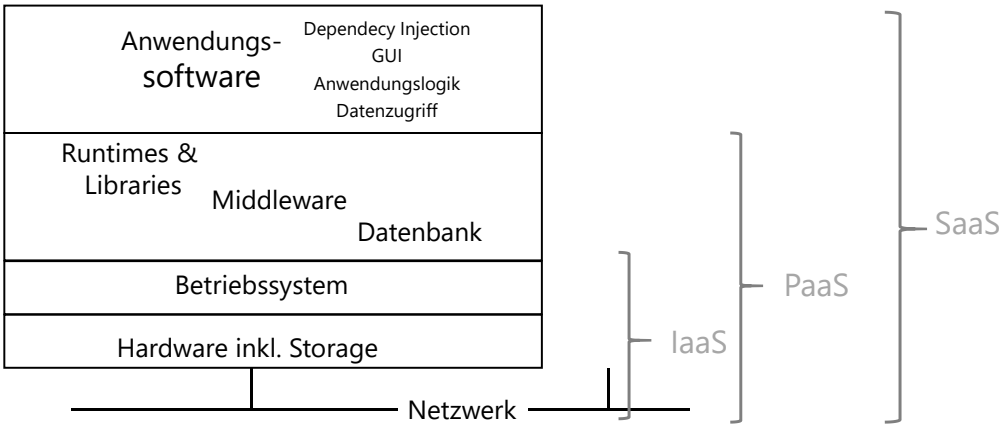

Abbildung 2-5: Schichten eines Anwendungssystems in Anlehnung an Haas[29] und Servicemodelle[30]

Speziell bezogen auf Cloud-Computing werden heute allgemein als Hauptmodelle – orientiert an den verschiedenen Schichten von Anwendungssystemen – **Infrastructure-as-a-Service** (IaaS), **Platform-as-a-Service** (PaaS) und **Software-as-a-Service** (SaaS) unterschieden. Im Grunde können jedoch in verteilten Umgebungen wie z.B. Telematikplattformen – aber eben auch für Enterprise Informationssysteme (EIS) oder gemeinsam für verschiedene EIS –die für alle Instanzen zentral wichtige Referenz-Services als Service aus Funktionalitäten oder Datenobjekten angeboten bzw. von den anderen Softwareanwendungen konsumiert werden. Dies kann erheblich zu Integrität und Effektivität der Informationsverarbeitung beitragen. Insofern werden zukünftig **Function-as-a-Service** (FaaS) und **Data-as-a-Service** (DaaS) eine wichtige Rolle spielen. Auch ohne, dass die originären Anwendungssysteme bereits Cloud-Lösungen sind können solche Services als inter-organisationale Systeme[31] betrachtet werden.

Alle aaS-Modelle, bei denen in irgendeiner Form der Anbieter etwas betreibt, haben gemein, dass dieser dann für Installation, Betrieb, Update, Wartung, Backup und Anpassung an den technologischen Fortschritt verantwortlich ist und dies nicht mehr beim Kunden liegt. Dies ist dann in der wie auch immer ausgestalteten Inanspruchnahme-Gebühr enthalten.

Im Folgenden soll mit Blick auf die dieser Ausarbeitung zugrundeliegende Aufgabenstellung nur kurz auf die vorgenannten Servicemodelle eingegangen werden.

Infrastructure-as-a-Service (IaaS)

Im Rahmen IaaS werden physikalische Ressourcen wie Netzwerke, Server oder Speicherplatz über das Internet zur Verfügung gestellt und „Infrastructure" wird als technische Infrastruktur – natürlich mit der für den Betrieb dieser Infrastrukturelemente notwendigen Software – definiert. Der Vorteil ist hier für den Kunden neben dem Wegfall von Investitionen die dynamische Nutzung dieser physikalischen Ressourcen und die beliebige Skalierbarkeit. Da die Infrastruktur

[29] Haas: Medizinische Informationssysteme und Elektronische Patientenakten. 2005, S. 33.

[30] Eine noch detailliertere Schichtung und Zuordnung findet sich unter https://kinsta.com/de/blog/arten-von-cloud-computing/.

[31] Glaser/Lo: Concepts for Building Inter-Organizational Systems in Healthcare: Lessons from Other Industries. In JHIM Vol. 20, No. 3, S. 54 ff.

von einem Dienstleister bezogen wird, entfällt vor Ort der Aufwand für Aufbau, Betrieb und Erhalt einer entsprechenden Infrastruktur, also im Extremfall muss überhaupt kein Rechenzentrum mehr betrieben werden. Trotzdem muss der Kunde sich sodann um Installation und Konfiguration und Update seiner Softwareanwendungen inklusive der notwendigen Basissoftware und Middleware kümmern. Die Nutzung der Ressourcen wird über eine vereinbarte Mietgebühr bzw. mit Blick auf den wahren Character des Cloud Computing über die tatsächliche Nutzung oder Mischverfahren abgegolten.

Platform-as-a-Service (PaaS)

Geht das Serviceangebot über physikalische Ressourcen hinaus und werden auch bestimmte Werkzeuge und/oder Basissoftware wie Datenbanken oder Middleware wie Kommunikationsserver, Integrationsmaschinen, Interpreter, Webserver usw. innerhalb der virtuellen Umgebung zur Verfügung gestellt, spricht man von Platform-as-a-Service, wobei der Begriff „Platform" nicht scharf definiert ist. Auf jeden Fall handelt es sich um ein Bundle, das mit gewissen Funktionalitäten bei Entwicklung und Einsatz von Anwendungssoftware integriert bzw. als Basis eingesetzt werden kann. Alle Software ist aber anwendungsneutral.

Software-as-a-Service (SaaS)

Nutzt der Kunde auch Anwendungssoftware und dies ebenso in skalierbarer Weise, also je nach Bedarf und Situation, spricht man von Software-as-a-Service. Dazu bedarf es auch der darunterliegenden Artefakte wie z.B. einer Plattform, auf der die Software läuft. Die Software selbst sollte das Cloud-Paradigma in geeigneter Weise unterstützen, also eine „Cloud-native" Softwarearchitektur haben, und somit eine serviceorientierte Architektur sein.

Function-as-a-Service (FaaS)

Eine besondere Form der Zurverfügungstellung von Softwarefunktionalität ist jene, mittels der spezifische Funktionalitäten bzw. Algorithmen zur Verfügung gestellt werden. Man kann dabei auch von „Fernverarbeitung" sprechen. Hier werden besonders komplexe oder besonders rechenintensive Algorithmen oder aber solche, die viele Unternehmen bzw. viele Instanzen von Anwendungslandschaften benötigen, verstanden, die über definierte Serviceschnittstellen Anfragen empfangen und „berechnete" Ergebnisse zurückgeben. Dies kann auch unter Verwendung eigener Daten des Service erfolgen.

So kann ein Service „Arzneimitteltherapiesicherheitsprüfung" entsprechende Überprüfungen übernehmen, wozu von einem lokalen medizinischen Informationssystem oder anderen Cloud-Softwarekomponenten nur die notwendigen Kontextdaten wie medizinischer Kontext des Patienten, derzeitige Medikation und neues zu verordnendes Medikament übermittelt werden und der FaaS liefert mögliche Kontraindikationen oder Wechselwirkungen zurück. Auch die Auswertung bzw. diagnostische Bewertung von Röntgenbildern, EKG-Kurven, Laborbefunden und vielen anderen kann über FaaS erfolgen. Im Grunde können viele KI-Anwendungen in dieser Weise effizient und qualitativ gesichert in die Fläche gebracht werden.

FaaS für spezialisierte komplexe Algorithmen bzw. Verarbeitungen hat gerade im Gesundheitswesen wie ersichtlich wird vielfältige Vorteile, da es eine Vielzahl von intelligenten Anwendungen gibt bzw. geben kann, die nur durch einzelne spezialisierte Anwender oder Forschergrup-

pen entwickelt werden und eine proprietäre Einbindung in proprietäre Systeme eine flächendeckende Nutzung weitgehend verhindert. Zusätzlich können für intelligente medizinische FaaS Qualitätsindikatoren definiert und Zulassungsverfahren etabliert werden, ähnlich wie dies aktuell für die Digitalen Gesundheitsanwendungen der Fall ist.

Data-as-a-Service (DaaS)

In Enterprise Informationssystemen aber auch in branchen-spezifischen Telematikplattformen wird die Nutzung von Daten notwendig, die eigentlich von vielen Anwendungssystemen in gleicher Weise benötigt werden.[32] Dies sind zum Beispiel die Stammdaten eines Systems. Die Zurverfügungstellung solcher Daten für viele Systeme ggf. auch einrichtungsübergreifend – das können dann auch Produktaxonomien und Warengruppenverzeichnisse, Terminologien, Produktkataloge, Wissensbausteine, Literatur u.v.a.m. sein – ist ein nützlicher Aspekt in verteilten offenen Systemen. Die Verzeichnisse werden als Repository oder Directory bezeichnet. Solche Daten werden heute redundant in vielen Systemen aufwändig gepflegt und fortgeschrieben – sogar redundant innerhalb der Anwendungssysteme eines heterogenen KIS. Solche Daten als DaaS verfügbar zu machen und nur durch eine zuständige Organisation oder eine zuständige Community pflegen zu lassen, hat erhebliche positive qualitative und ökonomische Effekte.

Darüber hinaus ist denkbar, dass auch Daten zu Patienten aus elektronischen Patientenakten – so z.B. Dokumente in der Patientenakte nach § 341 SGB V als Service verfügbar sind und je nach Berechtigung durch lokale oder Cloud-basierte Instanzen von Anwendungssystemen abgerufen und gepflegt werden können.

2.2.2 Bereitstellungs- und Organisationsmodelle

Ein zweiter Aspekt von Cloud-Lösungen ist die Frage, wie diese für die (potenziellen) Kunden bereitgestellt bzw. zugänglich sind. Prinzipielle Modelle sind die Public-, die Private- und die Hybrid-Cloud.

Public Cloud

In einer Public Cloud werden die Services einer Vielzahl von Kunden über öffentliche Netzwerkinfrastrukturen und das allgemeine Internet erreichbar angeboten und betrieben. Für den Kunden ist der Betrieb transparent im Sinne der Informatik – er weiß also nicht, wo in welchen tatsächlichen Infrastrukturen und ggf. mit welchen anderen Kunden geteilt die von ihm genutzten Services laufen. Speziell für SaaS bedeutet dies natürlich, dass die Software mandantenfähig sein muss, da ja trotzdem jeder Kunde mit seinen eigenen Daten arbeitet. Im Grunde gilt das natürlich auch für alle andere Daten, z.B. Daten, die der Kunde bei einer PaaS-Nutzung in der Plattform verwaltet, sodass durch geeignete technische bzw. softwaretechnische Datenschutzmechanismen gewährleistet sein muss, dass kein Kunde Zugriff auf Daten anderer Kunden hat.

Die Last-Balancierung erfolgt dann über alle Kunden hinweg und eventuell müssen die Festlegungen für Verfügbarkeits- und Performancemerkmale in speziellen Service-Level-Agreements

[32] Haas: Informatische Artefakte für eine Gesundheitstelematikplattform, in Goetz/Grode (Hg.) Thesenpapier zur Gesundheitstelematik, 2013, S. 78–84.

vereinbart werden. Die Abrechnungsmodelle sind vielfältig, orientieren sich aber zumeist an der tatsächlichen Nutzung.

Private Cloud

In einer Private Cloud werden die Services bzw. die gesamte Anwendungslandschaft exklusiv für einen Kunden eingerichtet und zur Verfügung gestellt. Die so eingerichtete gekapselte Umgebung innerhalb der eigentlichen öffentlichen Cloud gewährleistet dem Kunden bestmögliche Kontrolle und Gewährleistung des Datenschutzes, die Services sind nur über ein Intranet bzw. über ein Virtual Private Network (VPN) erreichbar und können durch weitere Maßnahmen wie Firewalls abgesichert werden. Trotz allem profitiert der Kunde von der technischen und funktionalen Skalierbarkeit und der Betreuung und technischen Fortschreibung „seiner" Cloud-Lösung, indem er diese von einem Cloud-Hoster betreiben und managen lässt.

Eine Private Cloud kann aber auch vor Ort beim Kunden in seinem eigenen Rechenzentrum auf Basis eines Intranet betrieben werden (On Premises), wobei dann gewisse Vorteile einer Private Cloud bei einem externen Dienstleister – vor allem die technische und/oder dynamische Skalierbarkeit verlorengeht, da physikalische Ressourcenbeschränkungen und daraus mit der Zeit resultierende Engpässe erst durch Nachrüstungen behoben werden können. Lediglich hinsichtlich der Software-Nutzung ist die funktionale Skalierbarkeit weiter einfach sicherzustellen, indem die gesamte mögliche (Anwendungs-/Branchen-)Software installiert wird, aber nur jene Teile freigeschaltet und nutzbar sind, die der Kunde als Service haben möchte. Ein Vorteil der Private Cloud ist die Kontrolle über den Ort der Verarbeitung und Speicherung.

Diese interne Private Cloud kann dann entweder der Kunde selbst managen oder aber diese durch einen Dienstleister in Teilen oder vollumfänglich managen lassen.

Hybrid Cloud

Wie bereits vorangehend in Kapitel 2.2.1 angesprochen, gibt es gegebenenfalls auch Services, die trotz der Nutzung einer Private Cloud für viele Kunden interessant sind, z.B. die Repositories, oder auch Nachrichten- oder Interoperabilitätsservices. Diese können dann in der Public Cloud betrieben und durch Artefakte der Private Cloud genutzt/konsumiert werden. Aber auch andere Zuschnitte sind denkbar, so z.B., dass der Webserver für die Anwendung und die Software selbst in der Public Cloud betrieben wird, aber alle Datenspeicherungen für schutzwürdige Daten (ggf. sogar vor Ort) in der Privat Cloud erfolgen ggf. alle oder ein Teil davon auch vor Ort.

Die Summe der Anwendungen der Lösung ist dann eine Hybrid-Cloud-Lösung, da Teile in der Private Cloud und andere Teile in der Public Cloud laufen. Aber auch eine Hybrid-Lösung aus Community-Cloud und Private-Cloud ist denkbar und kann sinnvoll sein.

Community Cloud

Schließen sich verschiedene Kunden wie z.B. Organisationen einer Branche hinsichtlich der Nutzung von IT-Services zusammen und nutzen gemeinsame Ressourcen – dieser aber im Grunde als PRIVATE Cloud für die Community – spricht man von einer Community-Cloud.

Die Ausprägung kann vielfältig sein. So könnten sich verschiedene Einrichtungen des Gesundheitswesens gemeinsam eine Cloud-Lösung z.B. für das medizinische Wissensmanagement

aufbauen und gemeinsam sogar die Daten und Funktionalitäten teilen und nutzen. Oder eine Community betreibt die notwendigen Repositories gemeinsam, belässt aber ihr Enterprise-System in der eigenen Private Cloud.

2.3 Marktlage im Hinblick auf Cloud-Angebote im KIS-Umfeld

Vor diesem Hintergrund stellt sich die Frage, ob die beschriebenen Cloud-Technologien schon im Bereich der KIS zum Einsatz kommen. Zu dieser Frage wurde im Rahmen der Erstellung dieses Gutachtens eine Markterkundung durchgeführt. Zur Erkundung der aktuellen Situation wurden dabei Expertengespräche geführt sowie eine Web-Recherche zu Anbietern von KIS auf dem deutschen Markt vorgenommen. Der Fokus dieser Untersuchung lag insbesondere darauf, ob und in welcher Form bereits Cloud-basierte Dienste angeboten werden. Daneben wurden anhand der Anzahl der Installationen in der BRD die Marktanteile der einzelnen Anbieter und Produkte im KIS-Markt untersucht.

Kein KIS-as-a-Service bislang in Deutschland

Das Ergebnis der Markterkundung zeigt, dass Dedalus mit seiner KIS-Sparte und insbesondere dem KIS *Orbis* Marktführer in Deutschland ist. Die KIS-Sparte hat Dedalus 2020 vom früheren Marktführer Agfa übernommen. Dahinter folgt die CompuGroup, die ihre KIS-Sparte ebenfalls erst in diesem Jahr durch die Übernahme mehrerer Systeme von Cerner deutlich ausgebaut hat. Mit Cerner, Nexus, Meierhofer und der Deutschen Telekom folgen weitere Anbieter mit vergleichbar großen Marktanteilen. Dahinter reihen sich noch mehrere Anbieter mit kleineren KIS-Sparten, wie insbesondere i-Solutions und AMC.

Mehrere der genannten Anbieter arbeiten daran, ihre Systeme zu modernisieren und auf die sich verändernden technischen Gegebenheiten und Möglichkeiten sowie die veränderten Anforderungen und Erwartungen auszurichten. Dabei spielen die plattformunabhängige Verfügbarkeit von Daten sowie die Verwendung mobiler Endgeräte eine zentrale Rolle. Dem Tragen die Anbieter Rechnung, indem sie ihre Systeme zunehmend webbasiert und Cloud-fähig ausrichten.[33]

Nutzung von Private Cloud-Umgebungen oder Cloud-Add-ons zu On-Prem-KIS

Vor diesem Hintergrund kann auch nicht ausgeschlossen werden, dass KIS von einzelnen Krankenhäusern oder Krankenhausverbünden bereits in einer Cloud-Umgebung betrieben werden. Hierbei dürfte es sich jedoch um vom Hersteller auf klassische Weise überlassene Software handeln, die auf einer vom Krankenhaus oder vom Verbund in der Regel in einer Private Cloud bereitgestellten Infrastruktur oder Plattform laufen. Anhand der Markterkundung ist allerdings **kein in Deutschland bereits verwendetes, vollständig Cloud-basiertes KIS-Angebot als Software-as-a-Service bekannt**, was auch an den heterogenen Datenschutzregeln liegen könnte.[34] Dies mag sich außerhalb Deutschlands anders verhalten.[35]

[33] Vgl. Tabelle 2-3: KIS-Anbieter mit nennenswertem Marktanteil in Deutschland, unten S. 40.

[34] Zu diesen heterogenen Regeln siehe unten Kap. 3, S. 49 ff. insbes. Kap. 3.4, S. 76 ff.

[35] Vgl. dazu bspw. *CommunityWorks* von Cerner.

Teil-Funktionalitäten oder Zusatzprogramme (Add-ons) für KIS, einschließlich RIS, werden hingegen bereits aus der Cloud als Service (SaaS) angeboten und auch verwendet.[36] Aufgrund eines hohen Speicherbedarfes wurden schon relativ früh Angebote zur externen Speicherung radiologischer Bilddaten in PACS zunächst auf dedizierte Server und mit der Zeit auch in Cloud-Umgebungen angenommen.[37] Auch gibt es inzwischen beispielsweise Software-as-a-Service-Angebote zur Unterstützung bei der radiologischen Befundung[38] oder zur medizinischen Bildanalyse und Entscheidungsunterstützung[39]. Über Schnittstellen können diese Programme die übrigen, nicht Cloud-basierten Systeme ergänzen. In der Gesamtschau handelt es sich also um einen hybriden Ansatz, bei dem die externen Systeme in der Cloud über lokale Systeme angesteuert werden, die meistens auch kryptografische Schlüssel oder im Sinne einer Pseudonymisierung die Zuordnung medizinischer Daten zu Patienten-identifizierenden Daten verwalten. Solche Teil-Funktionalitäten sind aufgrund ihrer geringeren Komplexität sowohl aus technischer als auch aus rechtlicher Sicht leichter umsetzbar. So konnte oder kann bspw. datenschutzrechtlichen Vorschriften durch eine Client- bzw. KIS-basierte Verschlüsselung oder Pseudonymisierung der Daten leichter entsprochen werden, was im Rahmen eines vollständigen KIS praktisch nicht möglich ist, da an irgendeiner Stelle im KIS der direkte Bezug eines Datensatzes zum Patienten vorhanden sein muss.

HIMSS-Studie zur „Cloud-Evolution in deutschen Krankenhäusern"

Dass an Cloud-Lösungen im Krankenhausumfeld an sich ein reges Interesse besteht, zeigt auch eine aktuelle Studie aus dem Jahr 2020 zum Cloud Computing in deutschen Krankenhäusern, welche die Healthcare Information and Management Systems Society durchgeführt hat.[40] Demnach nutzt bereits jedes zweite deutsche Krankenhaus mindestens eine Cloud-Lösung im administrativen oder klinischen Bereich. Am häufigsten sind dabei Lösungen zur Bildspeicherung (PACS) und administrative Software wie Microsoft Office 365 im Einsatz. Die Studie zeigt zudem, dass Public Cloud-Lösungen als vorteilhafter angesehen werden als On-Premise-Lösungen. Grund dafür sind hauptsächlich wirtschaftliche und funktionelle Aspekte wie Einsparungen bei Hard- und Softwareinvestitionen und die Skalierbarkeit. Hingegen werden Sicherheitsaspekte und individuelle Anpassungsmöglichkeiten an die jeweiligen Bedürfnisse als Vorteile für On-Premises-Lösungen gesehen.

Die Studie kommt zu dem Ergebnis, dass die Nachfrage nach Public-Cloud Lösungen in den – von 2020 an gerechnet – nächsten ein bis zwei Jahren moderat und dann in drei bis fünf Jahren stärker ansteigen wird. Es wird außerdem davon ausgegangen, dass die Public Cloud bis dahin die Mehrheit der deutschen Krankenhäuser erreicht haben wird.

[36] Vgl. dazu bspw. Telepaxx (https://www.telepaxx.de) oder Smart Reporting (https://www.smart-reporting.com/de).

[37] S. dazu bspw. das entsprechende Angebot von Telepaxx (https://www.telepaxx.de).

[38] S. dazu bspw. das Angebot „Smart Radiology" der Firma Smart Reporting (https://www.smart-reporting.com/de)

[39] S. dazu bspw. das Angebot „Sherlog" des Startups FUSE-AI (https://sherlog.ai/) oder „AI-RAD-Companion" von Siemens Healthineers (https://www.siemens-healthineers.com/de/).

[40] Zu dieser Studie im Auftrag der Nuance Communications Inc., welche selbst ein Interesse an Cloud-basierten Dienstleistungen für Krankenhäuser hat: Wels-Maug, Cloud-Nutzung im Krankenhaus, 16.11.2020.

Cloud Networking Survey

Eine weitere Studie der Extreme Networks, Inc., ebenfalls aus dem Jahr 2020, kommt auch zu dem Schluss, dass der Einsatz von Cloud-Computing in Krankenhäusern und Kliniken Fahrt aufgenommen hat.[41] Für die Studie wurden über 200 IT-Fachleute aus dem Gesundheitswesen in den Regionen Nordamerika, Europa, Asien, Südamerika und Mittelamerika zu Ihrer Meinung zum Aufstieg der Cloud in der Branche befragt.[42]

Laut der Studie hosten bereits 98% der Gesundheitsorganisationen mindestens eine Lösung in der Cloud. Bei diesen Lösungen handelt es sich vorwiegend um Anwendungen im Bereich E-Mail und Produktivität (62%) sowie Software für Personalmanagement und Personaleinsatzplanung (45%), gefolgt von elektronischen Akten (EMR/EHR),[43] Patientenentertainment, medizinischen Geräten und anderen Anwendungen. Stand heute nutzen laut der Studie 14% der Organisationen Cloud-Management, 41% haben Pläne, das Infrastrukturmanagement in den nächsten 1-5 Jahren einzuführen.

Studie Cloud Native 2020

Um ein umfassenderes Bild der Entwicklungen im Bereich Cloud-Computing zu erhalten, lohnt auch ein Blick auf die Bedeutung sog. Cloud-Native-Technologien innerhalb dieses Bereichs. Dabei handelt es sich – als Gegenentwurf zur Migration bestehender Lösungen in die Cloud – um die Entwicklung neuer, nativer Lösungen in der und für die Cloud. Mit diesem noch recht neuen Konzept beschäftigt sich unter anderem die Studie „Cloud Native 2020".[44] Die Studie basiert auf 374 Interviews mit obersten (IT-)Verantwortlichen von Unternehmen verschiedenster Branchen in der D-A-CH-Region.

Diese Studie kommt ebenfalls zunächst zu dem Ergebnis, dass Cloud-Computing auf dem Vormarsch und in vielen Bereichen bereits etabliert ist. So schätzt über die Hälfte der Befragten den Cloud-Reifegrad ihres Unternehmens als hoch oder sehr hoch ein. Die Relevanz von Cloud-Native-Methoden wird dabei ebenfalls hoch eingeschätzt. 39% der Befragten messen diesen Methoden bereits heute große Bedeutung bei, 67% gehen von einer großen Bedeutung in der näheren Zukunft (zwei bis drei Jahre) aus. Zudem geben 63% der Befragten an, bereits Cloud-Native-Lösungen einzusetzen, wobei aber nur etwa ein Drittel diese als bereits im Unternehmen etabliert bezeichnet.

Auch hinsichtlich der Bedenken, die die befragten Entscheider bzgl. Cloud-Computing im Allgemeinen und Cloud-Native im Besonderen äußern, deckt sich die Studie weitgehend mit den Erkenntnissen der bereits genannten Studien. So werden auch hier Sicherheitsbedenken und

[41] Siehe Schwanke-Seer/Helling: Cloud-Networking im Gesundheitswesen; 24.11.2020.

[42] Extreme Networks: Welcome to 2020! Survey says: Healthcare is Ready for Cloud Networking; 20.02.2020.

[43] Mit EMR sind „Electronic Medical Records" gemeint, mit EHR "Electronic Health Records". Beide Begriffe werden häufig synonym verwandt und beinhalten jedenfalls eine Art elektronische Patientenakte mit den wichtigsten Informationen aus der Behandlung für medizinische Leistungserbringer. Die EHR kann als Art elektronische Gesundheitsakte darüber hinaus auch weitergehende Information zu Gesundheit und Fitness aufnehmen und auch in einer für den Patienten verständlichen Form aufbereiten. Vgl. hierzu Garrett/Seidmann: EMR vs EHR – What ist he Difference?; 2011.

[44] IDG Research Services: Studie Cloud Native 2020; 2020.

insbesondere Bedenken bzgl. des Verlusts, Diebstahls, missbräuchlicher Zugriffe und der Integrität von Daten an erster Stelle genannt.

Interessanterweise wird der Datenschutz aber neben der Datenverfügbarkeit und der Belastbarkeit als einer der größten Vorteile von Cloud-Native-Anwendungen genannt.

Fazit

Wie die Markterkundung zeigt, wird bisher in Deutschland noch kein komplettes Cloud-KIS als Service genutzt. Allerdings beziehen Krankenhäuser schon heute eine größere Anzahl ergänzender Services aus der Cloud. Es ist eine starke Tendenz zu einer immer intensiveren Cloud-Nutzung bis – jedenfalls im internationalen Kontext – hin zu einem KIS-as-a-Service erkennbar. Das belegen auch die in diesem Kapitel erwähnten nationalen und internationalen Studien.

Tabelle 2-3: KIS-Anbieter mit nennenswertem Marktanteil in Deutschland

Anbieter	**KIS-Produkt(e)**	**Verbreitung in der BRD (ca.)[45]**	**Anteil/KIS-Markt DE[46]**	**Cloud-Dienste**
Dedalus Healthcare Group AG[47]	*Orbis*	800 Installationen (gesamte KIS-Sparte d. Herstellers)	37,0 %	*Orbis U* wird als Grundstein eines Cloud-fähigen KIS entwickelt.
CompuGroup Medical SE & Co. KGaA[48]	*CGM medico,* *CGM Clinical*	250 Installationen (*CGM medico*); k. A. zu CGM Clinical verfügbar	11,6 %	*CGM Memory* verspricht Rechtssicherheit bei der Speicherung von Patientendaten in der *CGM Medical Cloud* (Verschlüsselung und Entfernung des Personenbezugs) Die Cloud-Lösung ist laut Hersteller DSGVO-konform[49] und wird als Zusatzlösung zu anderen Produkten des Herstellers angeboten.
Cerner Corporation[50]	*i.s.h.Med* *Soarian Clinical*	240 Installationen (*i.s.h.Med*); Installationen im einstelligen Bereich (*Soarian Clinical*)	11,1 %	Ambitionen (Kooperation mit AWS), *Community Works* als Cloud-basierte Version des KIS-Produkts *Millennium* in USA.
Nexus AG[51]	*Nexus*	260 Installationen	12,0 %	
Meierhofer AG[52]	*M-KIS* *M-KIS Next*	250 Kunden (*M-KIS*)	11,6 %	*M-KIS Next* auf SOA-Basis modernisiert seit 2020 schrittweise M-KIS hin zu Cloud- und KI-Einsatz.
Deutsche Telekom Healthcare and Security Solutions GmbH[53]	*iMedOne*	230 Installationen	10,6 %	Die *Healthcare Cloud* bietet speziell auf das Gesundheitswesen ausgerichtete Cloud-Dienste.
i-SOLUTIONS Health GmbH[54]	*ClinicCentre*	97 Installationen	4,5 %	
AMC Advanced Medical Communication Holding GmbH[55]	*CLINIXX KIS*	36 Installationen (Stand 2015)	1,6 %	Laut Hersteller bereits Cloud-fähig (Private Cloud deutsche Telekom).

[45] Doelfs, Wohin steuert der KIS-Markt in Deutschland?, kma online, 16.06.2020.
[46] Gerundete Angaben auf Basis der im Rahmen der Recherche verfügbaren, ggf. nicht ganz vollständigen Daten; 100% ≙ 2.164 Installationen in der BRD.
[47] Quelle: https://www.dedalusgroup.de/.
[48] Quelle: https://www.cgm.com/de/index.de.jsp.
[49] Quelle: https://www.cgm.com/de/arzt_zahnarzt/cgm_zusatzloesungen_de/cgm_memory_de/cgm_memory_vorteile/vorteile.de.jsp.
[50] Quelle: https://www.cerner.com/de/de/. S.a., insbes. zu Soarian Clinical: Mau, Nervöser KIS-Markt, kma Online, 11.04.2018, und Mau, KIS-Hersteller Cerner, kma Online, 18.03.2016.
[51] Quelle: https://de-de.nexus-ag.de/home.
[52] Quelle: https://www.meierhofer.com/de_de/home.
[53] Quelle: https://www.telekom-healthcare.com/de.
[54] Quelle: https://i-solutions.de/.
[55] Quelle: https://www.amc-gmbh.com/de/.

2.4 Herausforderungen und Motivationen

2.4.1 Herausforderungen und Motivationen aus der allgemeinen Situation und Entwicklung

Krankenhäuser betreiben heute ihre KIS vor Ort im eigenen Rechenzentrum oder in einem Servicerechenzentrum. Auch Hybridverfahren sind üblich, bei denen z.B. das administrative Informationssystem in einem Rechenzentrum und das klinische Informationssystem vor Ort betrieben werden. Zu Beginn der Entwicklung der sogenannten „autonomen KIS" Mitte der 80er Jahre und somit der ersten Inhouse-Verarbeitungen waren die dazu notwendigen Infrastrukturen relativ einfach, denn diese Systeme basierten auf der mittleren Datentechnik,[56] wurden also auf zentralen Servern mit angeschlossenen Bildschirmterminals betrieben. Nach und nach kamen dann Subsysteme für die großen Leistungsstellen wie Labor, Radiologie, Strahlentherapie, Pathologie und Operationsbereich als autonom betreibbare Abteilungsinformationssysteme auf den Markt und in die Krankenhäuser. Mit Aufkommen der Client-Server-Architekturen von KIS ab etwa dem Jahr 1990 und der Implementierung entsprechender TCP/IP- Netzwerke begann der Einstieg in eine Entwicklung im Rahmen derer die technische IT-Infrastruktur immer komplexer wurde. Mit Zunahme der Heterogenität der Systeme wurde auch der Einsatz von integrierenden Kommunikationsservern notwendig.[57] Bestand die Software der ersten autonomen KIS hauptsächlich aus administrativen Modulen, vor allen Dingen für die Patientenstammdatenverwaltung, Fallverwaltung und Abrechnung sowie für die Finanzbuchhaltung, kamen danach immer mehr auch medizinische Funktionalitäten hinzu, sodass auch die Komplexität der Anwendungssoftware und der Umfang der damit einhergehenden Parametrisierung und Betreuung immer höher wurde. Hinzu kamen sodann auch der Aufbau und Betrieb von Intranets mit internen Websites für dedizierte Zwecke und zunehmend auch der Anschluss an externe Infrastrukturen wie das Internet oder die Telematikinfrastruktur. Es konnte beobachtet werden, dass der personelle Ausbau der IT-Abteilungen nicht begleitend mit Blick auf die wachsende Breite und Tiefe der informatischen Artefakte vorgenommen wurde.

Heute stehen viele Krankenhäuser vor der Herausforderung, hochkomplexe verteilte Informationssysteme und Infrastrukturen mit minimaler Personalausstattung betreiben und weiterentwickeln zu müssen. So sind IT-Abteilungen immer mehr in eine technisch-betreuende Funktion abgedrängt worden - mit dem Fokus der Aufrechterhaltung des Bestehenden - und immer weniger Treiber und Gestalter des digitalen Wandels im Krankenhaus. Daneben überfordern heute die hohen Investitionskosten in eigene Infrastruktur und Softwarelizenzen immer mehr die Krankenhäuser, die so schleichend von den Hard- und Softwareinnovationen abgekoppelt werden. Schon heute ist hier ein immenser Investitionsstau entstanden. Und auch in personeller Hinsicht ergeben sich Problemstellungen, da spezialisiertes Personal z.B. für die Netzwerkbetreuung, Datenbankbetreuung, spezielle Aspekte der Anwendungs-Systeme u.v.a.m. nicht dop-

[56] Als „mittlere Datentechnik" wurden ab 1980 die ersten lokal betreibbaren Mehrbenutzersysteme bezeichnet, auf denen lokale Büroanwendungen und erste kleinere betriebliche Anwendungen außerhalb von Rechenzentren betrieben werden konnten.

[57] Der erste Kommunikationsserver in Deutschland - genannt HEIKO - wurde an der Universität Heidelberg 1985 entwickelt und betrieben.

pelt vorgehalten werden kann, entstehen weitere Risiken durch möglichen Ausfall von Personal. Hinsichtlich beider Aspekte könnten insgesamt Cloud-typische nutzungs- oder wertschöpfungsbasierte Erstattungsmodelle mit kalkulierbaren laufenden Kosten Abhilfe schaffen.

Vor diesem Hintergrund stellt der Betrieb eines KIS als Cloudlösung eine Chance dar, das eigene IT-Personal von rein technischer Betreuung, Skalierung und Ausbau der technischen Infrastruktur aber auch der Software-Konfiguration und des Integrationsmanagements von Anwendungssystemen zu entlasten und damit Ressourcen für die Kernaufgaben einer modernen IT-Abteilung wiederzugewinnen, nämlich die strategische Informationssystemplanung, die Betreuung der Anwender, die Analyse von Prozessen und IT gestützte Prozessoptimierung und das Management des digitalen Fortschritts im Krankenhaus. Außerdem können agile und kostengünstige Skalierung und Ausbau und Anpassung an den technischen Fortschritt erfolgen.

2.4.2 Regulatorische Herausforderungen und Motivationen

Neben den unter 2.4.1 genannten Chancen des Betriebs eines KIS als Cloudlösung geht der Wechsel auf Cloud-basierte Systeme ebenso wie die Implementierung weiterer digitaler Dienste in die Krankenhausabläufe zweifelsfrei mit regulatorischen, organisatorischen und finanziellen Herausforderungen einher.[58] Es gibt für Krankenhäuser und deren Betreiber aber auch von regulatorischer Seite Gründe und Motivationen, die für die Umsetzung weitergehender Digitalisierung trotz der genannten Herausforderungen sprechen. Auch hierbei können Cloud-Angebote helfen, beispielsweise indem die Kosten für bestimmte Vorhaben leichter auf mehr Schultern verteilt werden und vor allem kleinere Häuser die nötige IT-Infrastruktur und das erforderliche IT-Personal für komplexere Software-Unterstützung nicht alleine bereitstellen müssten.

Förderung im Rahmen des Krankenhauszukunftsfonds

So möchte der Bundesgesetzgeber mit dem am 29. Oktober 2020 in Kraft getretenen Krankenhauszukunftsgesetz (KHZG) unter anderem die Digitalisierung in Krankenhäusern fördern.[59] In der Begründung des Gesetzentwurfs heißt es dazu, es könnten „[…] durch zielgerichtete Investitionen in die Digitalisierung auch eine Modernisierung der stationären Notfallkapazitäten erreicht sowie die IT-technische Vernetzung von Krankenhäusern untereinander sowie mit anderen Akteuren des Gesundheitswesens vorangetrieben werden".[60] Durch entsprechende Änderungen wurden im IT-Bereich die folgenden in § 19 Abs. 1 KHSFV aufgeführten Vorhaben nach § 14a KHG förderungsfähig:

- **Technische Anpassung Notaufnahme** (§ 19 Abs. 1 S. 1 Nr. 1 KHSFV)
  Anpassung d. technischen, insbes. informationstechnischen Ausstattung der Notaufnahme eines Krankenhauses, das die Anforderungen für eine Teilnahme an der Basis-

[58] Die finanziellen Herausforderungen gegenüber der vorläufigen Weiterführung der Legacy-Systeme ergeben sich u.a. aus den auch bei einer Cloud-Anwendung nötigen Investitionen, z.B. für die Migration. Diese dürften sich jedoch längerfristig amortisieren.

[59] Gesetze für ein Zukunftsprogramm Krankenhäuser (Krankenhauszukunftsgesetz – KHZG) vom 29.10.2020, BGBl. I S. 2208.

[60] Begründung zum Fraktionsentwurf des KHZG von CDU/CSU und SPD, Bundestags-Drucksache 19/22126, S. 28.

notfallversorgung, erweiterten Notfallversorgung, umfassenden Notfallversorgung oder für das Modul Notfallversorgung Kinder[61] erfüllt, an den jeweils aktuellen Stand der Technik

- **Einrichtung Patientenportal** (§ 19 Abs. 1 S. 1 Nr. 2 KHSFV)
  Einrichtung von Patientenportalen für digitales Aufnahme- und Entlassmanagement, die den digitalen Austausch zwischen Leistungserbringern und Leistungsempfängern sowie zwischen Leistungserbringern, Pflege- und Rehabilitationseinrichtungen und Kostenträgern vor, während und nach der Behandlung ermöglichen

- **Einrichtung digitale Dokumentation** (§ 19 Abs. 1 Nr. 3 KHSFV)
  Einrichtung einer durchgehenden, strukturierten elektronischen Dokumentation von Pflege- und Behandlungsleistungen; Einrichtung von Einrichtung von Systemen, die automatisierte, sprachbasierte Dokumentation von Pflege- und Behandlungsleistungen unterstützen

- **Einrichtung Entscheidungsunterstützungssystem** (§ 19 Abs. 1 S. 1 Nr. 4 KHSFV)
  Einrichtung teil- oder vollautomatisierter klinischer Entscheidungsunterstützungssysteme zur Unterstützung klinischer Leistungserbringer bei Behandlungsentscheidungen, mit dem Ziel, die Versorgungsqualität zu steigern

- **Einrichtung Medikationsmanagement** (§ 19 Abs. 1 S. 1 Nr. 5 KHSFV)
  Einrichtung eines durchgehenden digitalen Medikationsmanagements zur Erhöhung der Arzneimitteltherapiesicherheit, das Informationen zu allen arzneibezogenen Behandlungen während dem Behandlungsprozess zur Verfügung stellt; inkl. robotikbasierte Stellsysteme zur Ausgabe von Medikation

- **Einrichtung digitaler Kommunikationsprozess** (§ 19 Abs. 1 S. 1 Nr. 6 KHSFV)
  Einrichtung eines krankenhausinternen digitalen Prozesses zur Anforderung von Leistungen, der Leistungsanforderung und Rückmeldung zum Verlauf der Behandlung in elektronischer Form ermöglicht, mit dem Ziel, krankenhausinterne Kommunikationsprozesse zu beschleunigen

- **Maßnahmen zur Leistungsabstimmung** (§ 19 Abs. 1 S. 1 Nr. 7 KHSFV)
  Wettbewerbsrechtlich zulässige Maßnahmen zu erforderlicher Abstimmung des Leistungsangebots mehrerer Krankenhäuser zur Sicherstellung einer ausgewogenen gemeinsamen Angebotsstruktur, die flächendeckende Versorgung sicherstellt und Spezialisierung ermöglicht; dazu zählt die Bereitstellung von sicheren **Cloud-Computing-Systemen.** Hier handelt es sich um die einzige Stelle, an der Cloud-Computing als Technologie in der KHSFV ausdrücklich genannt wird. Gleichwohl ist denkbar, dass Cloud-Anwendungen auch bei der Umsetzung der übrigen förderungsfähigen IT-Vorhaben zum Einsatz kommen, in manchen Bereichen, wie dem nachfolgenden Punkt der onlinebasierten Versorgungsnachweissysteme sogar naheliegend.

[61] Nach § 136c Abs. 4 SGB V.

- **Einrichtung onlinebasiertes Versorgungsnachweissystem**
  (§ 19 Abs. 1 S. 1 Nr. 8 KHSFV)
  Einführung und Weiterentwicklung eines onlinebasierten Versorgungsnachweissystems für Betten zur Verbesserung der Zusammenarbeit zwischen Krankenhäusern und anderen Versorgungsbereichen

- **Anlagen, Systeme, Verfahren und Maßnahmen zur Unterstützung von Ärzten**
  (§ 19 Abs. 1 S. 1 Nr. 9 KHSFV)
  Beschaffung, Errichtung, Erweiterung oder Entwicklung informationstechnischer, kommunikationstechnischer und robotikbasierter Anlagen, Systeme oder Verfahren oder räumlicher Maßnahmen, die erforderlich sind, um ÄrztInnen bei der Behandlung von PatientInnen, insbesondere im Rahmen von Operationen, zu unterstützen oder um telemedizinische Netzwerkstrukturen zwischen Krankenhäusern oder zwischen Krankenhäusern und ambulanten Einrichtungen aufzubauen und den Einsatz telemedizinischer Verfahren in der stationären Versorgung von Patientinnen und Patienten zu ermöglichen

- **Anlagen, Systeme oder Verfahren zur Vermeidung von Störungen**
  (§ 19 Abs. 1 S. 1 Nr. 10 KHSFV)
  Beschaffung, Errichtung, Erweiterung oder Entwicklung informationstechnischer oder telekommunikationstechnischer Anlagen, Systeme oder Verfahren um nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, der Integrität und der Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse des Krankenhausträgers zu treffen, die für die Funktionsfähigkeit des Krankenhauses und die Sicherheit verarbeiteter Patienteninformationen maßgeblich sind; nur förderungsfähig, wenn nicht ohnehin nach § 12a Abs. 1 S. 4 Nr. 3 KHG i. V. m. § 11 Abs. 1 Nr. 4 lit. A förderungsfähig

KHZG-Förderrichtlinie

Die Anforderungen an die einzelnen förderungsfähigen Vorhaben wurden vom Bundesministerium für Gesundheit (BMG) und dem Bundesamt für soziale Sicherung (BAS) in der am 30. November 2020 veröffentlichten Förderrichtlinie[62] konkretisiert. Dabei sind für jeden Fördertatbestand des § 19 Abs. 2 KHSFV funktionale Anforderungen als Muss- und Kann-Kriterien definiert. Die Muss-Kriterien stellen dabei die zwingend zu erfüllenden Mindestanforderungen dar, die Kann-Kriterien gehen - entsprechend ihrer optionalen Natur - darüber hinaus.

Bzgl. des Cloud-Computing (insbes. Fördertatbestand nach § 19 Abs. 1 S. 1 Nr. 7 KHSFV) stellt die Förderrichtlinie zunächst klar, dass der Aufbau von IT-Strukturen, welche mittels Cloud-Computing Systemen einrichtungs- und trägerübergreifend zur Verfügung stehen, gefördert werden kann. Das soll der Erhöhung der Prozessqualität und der Reduzierung von parallelen IT-Strukturen dienen. Deshalb müssen förderungsfähige Cloud-Computing Systeme zu einer einrichtungsübergreifenden Nutzung von IT-Ressourcen führen und – eine wichtige Ergänzung - so genutzt werden können, dass die Versorgung von Patientinnen und Patienten auch bei

[62] Richtlinie zur Förderung von Vorhaben zur Digitalisierung der Prozesse und Strukturen im Verlauf eines Krankenhausaufenthaltes von Patientinnen und Patienten vom 30.11.2020 in der Version 02 (hier kurz: KHZG-Förderrichtlinie genannt).

Störungen der Telekommunikationsinfrastruktur im notwendigen Umfang sichergestellt ist.[63] Immerhin sind Cloud-Lösungen auch für die Fördertatbestände 2-6 sowie 8-10 für die einrichtungsübergreifende Kooperation zur Abstimmung des Leistungsangebots möglich. Damit steht den Krankenhäusern offen, für bestimmte gemeinsame Vorhaben auch in Cloud-Lösungen zu investieren.

In Hinblick auf den Datenschutz enthält die Förderrichtlinie wenig konkrete Anforderungen an förderungsfähige Vorhaben. Vor dem Hintergrund der gegenwärtig zersplitterten Datenschutzlage[64] dürfte es auch nur in begrenztem Umfang Sinn machen, detaillierte materielle Vorgaben in dieser Hinsicht für die förderfähigen Vorhaben zu machen. Dennoch wird in der Förderrichtlinie mehrfach darauf hingewiesen, dass die einschlägigen datenschutzrechtlichen Vorschriften und Grundsätze einzuhalten sind. Bspw. werden in den Ausführungen zu § 19 Abs. 1 S. 1 Nr. 7 KHSFV einige Risiken für die Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität verarbeiteter oder gespeicherter Daten genannt, die im Kontext des Cloud-Computing entstehen und denen unter Berücksichtigung etwaiger Zugriffsmöglichkeiten Rechnung zu tragen ist.[65]

Rechnungsabschläge ab 2025 bei mangelnder Digitalisierung

Der durch die Förderungsfähigkeit gesteckte finanzielle Anreiz zur Umsetzung von Digitalisierungsvorhaben hat allerdings auch eine Kehrseite. Denn § 5 Abs. 3h KHEntgG und § 5 Abs. 6 BPflV sehen ab dem 1. Januar 2025 einen Abschlag von bis zu 2 Prozent des Rechnungsbetrags für jeden voll- und teilstationären Fall vor, sofern ein Krankenhaus nicht sämtliche in § 19 Abs. 1 S. 1 Nr. 2 bis 6 KHSFV aufgeführten digitalen Dienste bereitstellt. Es werden also nicht nur diejenigen unterstützt, die Digitalisierung in ihren Krankenhäusern vorantreiben, sondern auch diejenigen bestraft, die dies unterlassen.

Um einen derartigen Malus in Form eines Rechnungsabschlags zu entgehen, müssen somit die oben genannten Vorhaben bis 01.01.2025 umgesetzt und die entsprechenden untenstehenden Dienste bereitgestellt werden.

- Patientenportal mit digitalem Aufnahme- und Entlassmanagement (Nr. 2)
- durchgehende strukturierte elektronische Dokumentation (Nr. 3)
- teil- oder vollautomatisiertes klinisches Entscheidungsunterstützungssystem (Nr. 4)
- durchgehendes digitales Medikationsmanagement (Nr. 5)
- krankenhausinterner digitaler Prozess zur Anforderung von Leistungen (Nr. 6)

Fazit

Der Gesetzgeber unterstreicht damit das Ziel, die Digitalisierung im Gesundheitssektor voranzutreiben und schafft durch Fördermaßnahmen Anreize dafür. Gleichzeitig werden Krankenhäuser vor erhebliche Herausforderungen gestellt, da die Umsetzung bestimmter Maßnahmen obligatorisch ist und bei mangelnder Umsetzung spürbare Strafen drohen. Das Ausmaß dieser Herausforderungen scheint im Lichte der erheblichen Anforderungen an die einzelnen Digita-

[63] KHZG-Förderrichtlinie, S. 29 f.

[64] S. dazu Kap. 3, S. 49 ff.

[65] KHZG-Förderrichtlinie, S. 29.

lisierungsvorhaben – insbesondere bzgl. des Schutzes personenbezogener Daten – umso größer. So wird die Einhaltung datenschutzrechtlicher Vorschriften im Gesetzestext nochmals explizit als Voraussetzung der Förderungsfähigkeit genannt.[66] Die diesbezügliche Rechtslage ist aufgrund der verschiedenen einschlägigen Rechtsvorschriften auf EU-, Bundes- und Landesebene überaus unübersichtlich ist. Der rechtliche Rahmen wird in Kapitel 3 eingehend betrachtet. Auf Chancen und Risiken für Krankenhäuser, die abseits der hier aufgeführten regulatorischen Anreize und Herausforderungen bestehen, soll im Folgenden genauer eingegangen werden.

2.5 Chancen und Risiken für Krankenhäuser

Die Chancen des Einsatzes von Cloudlösungen für die Krankenhäuser unterscheiden sich nicht von jenen für Unternehmen anderer Branchen. Von Armbrust et al[67] werden die nachfolgend gezeigten Hindernisse/Risiken und Chancen angegeben.

Tabelle 2-4: Quick Preview of Top 10 Obstacles to and Opportunities for Growth of Cloud Computing

	Obstacle	Opportunity
1	Availability of ServiceUse	Multiple Cloud Providers; Use Elasticity to Prevent DDOS
2	Data Lock-In	Standardize APIs; Compatible SW to enable Surge Computing
3	Data Confidentiality and Auditability	Deploy Encryption, VLANs, Firewalls; Geographical Data Storage
4	Data Transfer Bottlenecks	FedExing Disks; Data Backup/Archival; Higher BW Switches
5	Performance Unpredictability	Improved VM Support; Flash Memory; Gang Schedule VMs
6	Scalable Storage	Invent Scalable Store
7	Bugs in Large Distributed Systems	Invent Debugger that relies on Distributed VMs
8	Scaling Quickly	Invent Auto-Scaler that relies on ML; Snapshots for Conservation
9	Reputation Fate Sharing	Offer reputation-guarding services like those for email
10	Software Licensing	Pay-for-use licenses; Bulk use sale

Als Vorteile von Cloud-Lösungen - die auch für Krankenhäuser ausschöpfbar sind - werden im Allgemeinen genannt:

- Wirtschaftlichkeit des Betriebs, „Pay per Performance“
- Senkung der Grenz- und Transaktionskosten
- Kostentransparenz
- Keine Investitionskosten, keine Kapitalbindung
- Partizipation am technischen/softwaretechnischen Fortschritt bzw. Innovationen, immer auf dem Stand der aktuellen Technik
- Skalierbarkeit der Infrastruktur
- Skalierbarkeit der Softwarefunktionalitäten / Softwarekonfigurationsflexibilität / Softwareorchestrierung
- Flexible Auswahl der Anbieter für Systeme, Module und Funktionalitäten (hinsichtlich Software bei SOA-basierter Cloud-Software-Architektur)

[66] Vgl. § 19 Abs. 2 Nr. 5 KHSFV.

[67] Armbrust: Above the Clouds: A Berkeley View of Cloud Computing, S. 3.

- Nutzung der spezialisierten Expertise des Cloud-Betreibers auf allen Systemebenen (Netze, Betriebssystem, Datenbanken, sonstige Middleware, Konfiguration und Parametrierung, Datenschutz und -sicherheitsmechanismen)
- Konzentration des eigenen Personals auch betriebsbezogene Analyse, Lösungskonzeption und Lösungseinführung und -betreuung
- Schnellere Einführung neuer Systeme, Module und Funktionalitäten, da Konzentration auf die fachlogischen und internen Prozess- und Unterstützungsaspekte
- Ubiquitäre Nutzbarkeit der Systeme/Anwendungssoftware unabhängig von Raum und Zeit
- Besserer Gesamt-Service für die Endanwender (aus der Summe der externen und internen Kompetenzen)
- Garantierte höchste Verfügbarkeit
- Erleichterung der einrichtungsübergreifenden Integration und Kooperation
- Bessere Einbeziehung der Kunden durch spezielle interoperable Kundenportale bzw. Kundenfunktionalitäten als Modul des KIS
- Stammdaten- und Knowledge-Sharing in einer Community-Cloud (Beispiel Systemstammdaten-as-a-Service)

Auf der anderen Seite ergeben sich gewisse Risiken, da die Abhängigkeit von einem Dritten oder mehreren Dritten wächst. So wie bei allen verteilten Systemen determiniert das schwächste Glied in der Kette die Reißfestigkeit. Wesentlich sind auch die Risiken durch die Offenbarung von Geheimnissen gegenüber einem Dritten, die so aber auch von der Auftragsdatenverarbeitung her bekannt sind. Bei einer Public Cloud, die im Sinne der Informatik für den Nutzer vollständig transparent[68] ist (es ist nicht bekannt, wo etwas läuft, von wem Software kommt usw.), besteht im Grunde keine direkte Beziehung mehr zwischen nachgeordneten Ressourcengebern und Kunden, was ggf. die vertragliche Durchsetzung von gewissen zugesicherten Eigenschaften bzw. die In- oder Mithaftungsnahme im Schadensfalle erschwert. Ebenso ist es denkbar, dass vor allem bei Nicht-Migrierbarkeit der Unternehmensdaten (Stichwort Datenportabilität) ein Wechsel der Lösung oder von Lösungsbausteinen zu anderen Softwareprodukten oder Cloud-Anbieter fast unmöglich wird und somit eine langfristige nur aufwändig aufzulösende Abhängigkeit entsteht. Auch werden Daten im Rahmen des Loggings oder zu Backupzwecken kopiert und an weiteren Orten archiviert, deren Lokalisation sich ebenfalls dem Nutzer bzw. der nutzenden Organisation entzieht, im Extremfall kommt es zu einer nicht überschaubaren Proliferation vertraulicher Daten. Daher müssen bei einer Cloud-Nutzung hohe Anforderungen an die vertraglichen Regelungen und technisch/organisatorischen Maßnahmen gestellt werden, damit die Compliance nicht gefährdet wird.

2.6 Fragestellungen des vorliegenden Gutachtens

Im Zusammenhang mit der Migration von KIS von einer heterogenen, aus proprietären Systemen bestehenden Anwendungslandschaft hin zu einer – idealerweise agilen und adaptiven –

[68] Der Transparenzbegriff in der Informatik und für verteilte Systeme bedeutet, dass man durch etwas „hindurchschauen" kann, ohne Details kennen zu müssen, also „das Verbergen der Separation der einzelnen Komponenten eines verteilten Systems vor dem Benutzer und dem Applikationsprogrammierer, sodass das System als Ganzes wahrgenommen wird und nicht als Sammlung voneinander unabhängiger Komponenten"; Coulouris/Dollimore/Kindberg: Verteilte Systeme, S. 42 ff.

Cloud-Lösung ergeben sich aus rechtlicher und technischer Sicht vor dem Hintergrund der bestehenden Lage eine Reihe von Problemstellung. Diese sollen im Folgenden beleuchtet und Lösungsvorschlägen zugeführt werden. Wesentliche Fragestellungen sind:

Aus datenschutzrechtlicher Sicht:

- Sind Teile eines KIS oder ein ganzes KIS als Cloud-Lösung betreibbar?
- Soweit dies erlaubt ist: Welche Anforderungen müsste ein Cloud-KIS erfüllen, um datenschutzkonform betrieben werden zu können?
- Hierfür müssen zunächst folgende Fragen geklärt werden:
    - Welche datenschutzrechtlichen Vorschriften sind auf Krankenhäuser je nach Standort und Trägerschaft anwendbar?
    - Welche besonderen Anforderungen ergeben sich bzgl. Schweigepflicht?
    - Wie ist die Einschaltung von Cloud-Anbietern datenschutzrechtlich zu bewerten?
    - Welche besonderen Anforderungen ergeben sich bei der Einschaltung von Cloud-Anbietern mit Bezug zu Drittländern?

Aus technischer Sicht:

- Welche Systeme und Funktionalitäten eines KIS sind gut geeignet, als Cloud-Lösung oder Cloud-Module betrieben zu werden?
- Wie können Cloud-Systeme und Module mit Legacy-Systemen zusammenarbeiten?
- Wie kann eine Cloud Native Anwendung für ein gesamtes KIS aussehen?
- Welche Rolle können internationale Health-IT-Standards spielen?
- Wie kann eine Migrationsstrategie vom Legacy-System zum Cloud Native System aussehen?
- Welche Anforderungen sind an Cloud-KIS-Anbieter und deren Lösungsangebote zu stellen?
- Wie kann die Einbindung gegebenenfalls nicht in die Cloud migrierbarer Komponenten (Beispiel medizintechnische Geräte) bewerkstelligt werden?
- Welche Möglichkeiten bestehen, Geheimnisse nicht dem Provider zu offenbaren?

3 Rechtliche Anforderungen bzgl. Datenschutz und Schweigepflicht

Im Rahmen dieses Kapitels werden die Anforderungen an die Verarbeitung von Patientendaten in einem Cloud-KIS im Hinblick auf Datenschutz und Schweigepflicht untersucht. Es handelt sich insofern grundsätzlich nicht um direkte Anforderungen an KIS-Produkte oder deren Hersteller. Primärer Adressat der hier geprüften Normen ist das jeweils behandelnde und damit auch im Sinne des Datenschutzes verantwortliche Krankenhaus. Die Regelungen wirken sich jedoch mittelbar auch auf Hersteller aus, denn Krankenhäuser dürfen keine Systeme anschaffen und betreiben, welche es ihnen nicht ermöglichen, ihre datenschutzrechtlichen Pflichten einzuhalten (Privacy-by-Design, Art. 25 Abs. 1 DSGVO). Überdies fungieren die Anbieter eines Cloud-KIS nicht lediglich als Softwarehersteller, sondern in der Regel als Auftragsverarbeiter und unterliegen damit auch unmittelbar gesetzlichen Pflichten (Art. 28 DSGVO).

3.1 Anforderungen an Cloud-KIS nach der DSGVO

3.1.1 Anwendbarkeit der DSGVO auf Krankenhäuser

Zunächst ist festzuhalten, dass die EU-Datenschutz-Grundverordnung (DSGVO)[69] auch auf die Verarbeitung personenbezogener Daten durch oder im Auftrag von Krankenhäusern Anwendung findet. Dies ergibt sich zunächst aus Art. 2 Abs. 1 DSGVO, wonach der sachliche Anwendungsbereich der Verordnung „[…] die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie […] die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen […]" umfasst. In KIS findet dabei unzweifelhaft eine ganz oder zumindest teilweise automatisierte Verarbeitung personenbezogener Daten statt.[70]

Zudem ist keine Ausnahme vom Anwendungsbereich der Verordnung nach Art. 2 Abs. 2 DSGVO ersichtlich. Dies gilt auch für Art. 2 Abs. 2 Buchst. a DSGVO, wonach die Verordnung „keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt", findet.

Auch reine Inlandssachverhalte sind damit nicht ausgenommen. Es muss nicht in jedem Einzelfall geprüft werden, ob die betreffende konkrete Tätigkeit den freien Datenverkehr zwischen Mitgliedstaaten betrifft.[71] Es genügt, dass die Europäische Union wie für die DSGVO zu Recht

[69] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. EU L 119 v. 04.05.2016, S. 1-88, mit Berichtigungen der deutschen Sprachfassung v. 22.11.2016 (ABl. L 314, S. 72) und v. 23.05.2018 (ABl. EU L 127, S. 2).

[70] Eine automatisierte Verarbeitung liegt beim Einsatz von Datenverarbeitungsanlagen vor, in welche Daten eingegeben, dort verarbeitet und wieder ausgegeben werden. Teilautomatisiert ist die Verarbeitung, wenn manuelle Zwischenschritte erforderlich sind.

[71] So schon zur entsprechenden Formulierung in Art. 3 Abs. 2 der Datenschutz-Richtlinie 95/46/EG: EuGH, Urt. v. 06.11.2003 – C-101/01 (Lindqvist), Rdnr. 42, Slg. 2003, I-12971 = RDV 2004, 16.

die Zuständigkeit in Art. 16 Abs. 2 AEUV72 zum Ausgleich von Datenschutz und freiem Datenverkehr in der Union genutzt hat.[73]

Die eingeschränkten Kompetenzen der Union im Gesundheitsbereich (Art. 168 AEUV) sprechen nicht gegen diese Einordnung, denn die Datenschutzkompetenz umfasst grundsätzlich auch die Verarbeitung personenbezogener Daten im Gesundheitswesen.[74] Zwar muss auch bei der Nutzung solcher anderer Kompetenzen der Union, gerade auch der Querschnittskompetenz zum Datenschutz, die Verantwortung der Mitgliedstaaten für die Festlegung ihrer Gesundheitspolitik, die Organisation des Gesundheitswesens und die medizinische Versorgung gewahrt werden (Art. 168 Abs. 7 S. 1 AEUV). Diese Querschnittsklausel zur Wahrung der Verantwortung der Mitgliedstaaten steht zumindest einer teilweisen Harmonisierung des Datenschutzes im Gesundheitswesen jedoch nicht entgegen. Angesichts der vielen Öffnungsklauseln der DSGVO gerade für die Verarbeitung von Gesundheitsdaten kann man davon ausgehen, dass die entsprechende Verantwortung der Mitgliedstaaten jedenfalls gewahrt bleibt und die DSGVO grundsätzlich auch auf eine solche Verarbeitung Anwendung findet.

Nach den Übrigen Ausnahmen des Art. 2 Abs. 2 DSGVO findet die Verordnung zudem keine Anwendung auf die Verarbeitung personenbezogener Daten

- durch die Mitgliedstaaten bei Tätigkeiten im Bereich der gemeinsamen Außen- und Sicherheitspolitik nach Titel V Kapitel 2 EUV,
- durch natürliche Personen bei Tätigkeiten im ausschließlich persönlichen oder familiären Bereich und
- durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

Da auch keine dieser weiteren Ausnahmen auf die Verarbeitung personenbezogener Daten durch oder im Auftrag von Krankenhäusern Anwendung findet, bleibt es bei einer Anwendbarkeit der DSGVO in diesem Bereich.

3.1.2 Cloud-Computing durch Auftragsverarbeiter nach Art. 28 DSGVO

Im Rahmen der Auftragsverarbeitung lässt die DSGVO die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen zu. Dies macht den vereinfachten, Einsatz externer Dienstleister als Auftragnehmer bzw. Outsourcing-Nehmer, die im Rahmen ihrer Dienstleistung weisungsgebunden personenbezogene Daten verarbeiten, überhaupt erst möglich, ohne dass hierbei die im Übrigen hohen datenschutzrechtlichen Hürden für eine Datenweitergabe an eigenverantwortliche Dritte eingehalten werden müssen.

---

[72] Vertrag über die Arbeitsweise der Europäischen Union, Fassung aufgrund des am 1.12.2009 in Kraft getretenen Vertrages von Lissabon (Konsolidierte Fassung bekanntgemacht im ABl. EG Nr. C 115 vom 9.5.2008, S. 47) zuletzt geändert durch die Akte über die Bedingungen des Beitritts der Republik Kroatien und die Anpassungen des Vertrags über die Europäische Union, des Vertrags über die Arbeitsweise der Europäischen Union und des Vertrags zur Gründung der Europäischen Atomgemeinschaft (ABl. EU L 112/21 vom 24.4.2012) m.W.v. 1.7.2013.

[73] Schneider, Einrichtungsübergreifende elektronische Patientenakten, S. 409 ff. (allgemein zur Datenschutzkompetenz der Union), S. 469 f. (zum Entwurf der DSGVO), jeweils m.w.N.

[74] Allgemein zum Verhältnis der Kompetenzen im Bereich Datenschutz und Gesundheitsschutz und den Ausführungen in diesem Absatz: Schneider, Einrichtungsübergreifende elektronische Patientenakten, S. 415 ff. m.w.N.

Im Folgenden werden vor diesem Hintergrund die Möglichkeiten einer DSGVO-konformen Einschaltung von Cloud-Anbietern durch Krankenhäuseruntersucht. Geprüft wird dabei nicht die generelle Zulässigkeit der Verarbeitung von Gesundheitsdaten im Krankenhaus, die hier vorausgesetzt wird.[75] Es sollen vielmehr die zusätzlichen Voraussetzungen, die aufgrund des Outsourcings von Patientendaten in die Cloud erfüllt werden müssen, betrachtet werden.

Einordnung der Einschaltung eines Cloud-Anbieters als Auftragsverarbeitung

Werden im Rahmen des Cloud-Computing personenbezogene Daten verarbeitet, so liegt in den meisten Fällen eine Auftragsverarbeitung nach Art. 28 DSGVO vor.

Verantwortlicher im Sinne der DSGVO bleibt hierbei der Auftraggeber, also der Nutzer eines Cloud-Dienstes. Der Cloud-Anbieter wird hingegen nicht selbst Verantwortlicher, sondern agiert als weisungsgebundener Auftragnehmer, der in diesem Kontext üblicherweise als Auftragsverarbeiter bezeichnet wird. Es ist die Pflicht des Verantwortlichen, den Auftragsverarbeiter sorgsam auszuwählen und nur mit solchen Auftragsverarbeitern zusammenzuarbeiten, „die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der Betroffenen gewährleistet" (Art. 28 Abs. 1 DSGVO).

Je nach Ausgestaltung des Cloud-Angebots besteht die Dienstleistung des Anbieters in der Zurverfügungstellung verschiedener Dienste wie Rechenleistung, Speicherplatz, Entwicklungsumgebung, Softwareanwendungen usw. Werden bei der Nutzung dieser Dienste personenbezogenen Daten verarbeitet, so erfolgt diese Verarbeitung durch den Auftragsverarbeiter im Auftrag des Verantwortlichen. Er verarbeitet also personenbezogene Daten für den Verantwortlichen, ohne ein eigenes, originäres Interesse an diesen Daten zu verfolgen. Der Verantwortliche legt die Zwecke und Mittel der Verarbeitung fest.

Die Weitergabe personenbezogener Daten an einen Auftragsverarbeiter innerhalb des Europäischen Wirtschaftsraums (EWR)[76] ist nach wohl herrschender Meinung gegenüber einer sonstigen Datenweitergabe privilegiert. Das ergibt sich aus Art. 4 Nr. 10 DSGVO, wonach der Auftragsverarbeiter kein Dritter i. S. d.im Sinne dieser Verordnung ist. Vielmehr wird die Verarbeitung durch den Auftragsverarbeiter, bei Beachtung gewissermaßen im Innenverhältnis zwischen Verantwortlichem und Auftragsverarbeiter dem Verantwortlichen zugerechnet.[77] Art. 28 DSGVO stellt insofern einen Erlaubnistatbestand für die Datenweitergabe an den Auftragsverarbeiter dar, sodass eine solche Übermittlung als Verarbeitungshandlung keiner gesonderten Rechtsgrundlage nach Art. 6 DSGVO bedarf.

Abgrenzung von der gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO

In selteneren Fällen kann auch eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO gegeben sein. Nach dem Wortlaut der DSGVO setzt dies voraus, dass mehrere Verantwortliche

[75] Dies ergibt sich im Rahmen eines Behandlungsvertrags aus Art. 9 Abs. 2 Buchst. h DSGVO sowie über die Öffnungsklausel des Art. 9 Abs. 4 DSGVO aus den jeweiligen LKHG.

[76] Der EWR umfasst die EU-Mitgliedstaaten sowie Island, Liechtenstein und Norwegen.

[77] Vgl. Kurzpapier Nr. 13 der Datenschutzkonferenz (DSK) vom 17.12.2018.

die Zwecke der und die Mittel zur Verarbeitung personenbezogener Daten gemeinsam festlegen.

Das könnte dann der Fall sein, wenn ein Cloud-Anbieter Daten auch für eigene Zwecke verarbeitet.[78] Aber auch der gemeinsame Betrieb einer Cloud zur Leistungsabstimmung durch mehrere Krankenhäuser, der nach § 19 Abs. 1 Nr. 7 KHSFV ein über den Krankenhauszukunftsfonds förderungsfähiges Vorhaben darstellt, kann ein Fall der gemeinsamen Verantwortlichkeit sein.

Die Anforderungen an gemeinsam Verantwortliche sind in Art. 26 DSGVO geregelt und umfassen insbesondere den Abschluss einer Vereinbarung, in der festgelegt wird, wer welche Verpflichtungen nach der DSGVO erfüllt. Die wesentlichen Inhalte dieser Vereinbarung sind den betroffenen Personen transparent zu machen.

Soweit in diesem Rahmen eine Datenweitergabe zwischen den gemeinsam Verantwortlichen erfolgt, bedarf auch diese sowie die Weiterverarbeitung personenbezogener Daten nach der Weitergabe einer gesonderten datenschutzrechtlichen Erlaubnis, die nicht durch die gemeinsame Verantwortlichkeit ersetzt wird.[79] Eine Verarbeitung in gemeinsamer Verantwortung kann allerdings nach der jüngeren Rechtsprechung des EuGH auch dann vorliegen, wenn nicht alle Beteiligten Zugriff auf die personenbezogenen Daten haben, sofern ein hinreichender Einfluss auf Zweck und/oder Mittel der Verarbeitung besteht.[80]

Die gemeinsame Verantwortlichkeit ist im Bereich des Cloud-Computing als Sonderkonstellation gegenüber dem Regelfall der Auftragsverarbeitung anzusehen. Sie wird im Folgenden deshalb nicht weiter untersucht.

Anforderungen an die Auftragsverarbeitung nach Art. 28 DSGVO

Die Verarbeitung personenbezogener Daten im Auftrag muss zunächst den gleichen Anforderungen genügen wie die Verarbeitung durch den Verantwortlichen selbst. Zudem hat die Auftragsverarbeitung gemäß Art. 28 Abs. 3 S. 1 DSGVO auf Grundlage einer Vereinbarung zu erfolgen, sofern sie nicht auf Grundlage eines anderen Rechtsinstruments nach dem Unionsrecht

[78] Offen gelassen wird hier die Frage, ob eine solche eigene (Mit-)Verantwortung des Cloud-Anbieters nur anstelle oder auch neben einer Auftragsverarbeitung rechtlich zulässig ist. Ohne explizite Zustimmung des Auftraggebers wird eine Verarbeitung auch zu bestimmten eigenen Zwecken des Auftragsnehmers jedenfalls vor dem Hintergrund einer Auftragsverarbeitung nicht zulässig sein.

[79] EuGH, Urteil v. 05.06.2018, C-210/16 (Facebook Fanpages), Rdnr. 39. Bestätigt durch: EuGH, Urteil v. 10.07.2018, C-25/17 (Zeugen Jehovas), Leitsatz 3; EuGH, Urteil v. 29.07.2019, C-40/17 (Fashion ID), Rdnr. 89.

[80] EuGH, Urteil v. 05.06.2018, C-210/16 (Facebook Fanpages), Randnummer 38. Bestätigt durch: EuGH, Urteil v. 10.07.2018, C-25/17 (Zeugen Jehovas), Leitsatz 3; EuGH, Urteil v. 29.07.2019, C-40/17 (Fashion ID), Rdnr. 69, in der zuletzt genannten Fundstelle prägnant formuliert: „Im Übrigen setzt die gemeinsame Verantwortlichkeit mehrerer Akteure für dieselbe Verarbeitung nach dieser Bestimmung nicht voraus, dass jeder von ihnen Zugang zu den betreffenden personenbezogenen Daten hat." Mit der genannten Bestimmung ist in diesem Urteil noch die Definition des Verantwortlichen in Art. 2 Buchst. d der Datenschutz-Richtlinie 95/46/EG gemeint. Doch die Datenschutz-Grundverordnung (DSGVO) enthält in Art. 4 Nr. 7 eine praktisch gleichlautende Definition, so dass diese Serie von Urteil auch auf Sachverhalte nach Geltung der DSGVO Anwendung finden kann.

oder dem Recht der Mitgliedstaaten erfolgt. Letzteres ist im Krankenhausbereich in Deutschland nicht der Fall ist, weshalb hier für eine Auftragsverarbeitung immer ein Vertrag erforderlich ist.81 Dieser Vertrag enthält mindestens Regelungen zu

- Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung,
- Art der personenbezogenen Daten,
- Kategorien betroffener Personen und die
- Pflichten und Rechte des Verantwortlichen.

Weiter hat der Vertrag nach Art. 28 Abs. 3 S. 2 DSGVO insbesondere die folgenden Verpflichtungen des Auftragsverarbeiters vorzusehen:

a) Verarbeitung personenbezogener Daten nur auf dokumentierte Weisung des Verantwortlichen
b) Verpflichtung zur Vertraulichkeit oder gesetzliche Verschwiegenheitspflicht der zur Verarbeitung personenbezogener Daten befugten Personen
c) Implementierung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO
d) Einsatz von Unterauftragnehmern nur unter den Voraussetzungen des Art. 28 Abs. 2 und Abs. 4 DSGVO
e) Unterstützung des Verantwortlichen bei der Beantwortung von Betroffenenanfragen durch technische und organisatorische Maßnahmen
f) Unterstützung des Verantwortlichen bei der Einhaltung seiner Pflichten bzgl. der Sicherheit personenbezogener Daten (Art. 32 DSGVO), dem Umgang mit Datenschutzverletzungen (Art. 33, 34 DSGVO) sowie der Datenschutz-Folgenabschätzung und vorherigen Konsultation (Art. 35, 36 DSGVO)
g) nach Wahl des Verantwortlichen Rückgabe oder Löschung aller personenbezogenen Daten sowie deren Kopien nach Abschluss der Verarbeitungsleistungen, sofern keine Pflicht zur Speicherung besteht; und
h) Nachweis der Einhaltung der genannten Pflichten und Information des Verantwortlichen, falls eine erteilte Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt

3.1.3 Cloud-Computing in Drittländern nach Art. 44 ff. DSGVO

Sollen personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermittelt werden, so bedarf diese Übermittlung einer eigenständigen Grundlage nach Kapitel V der DSGVO. Dadurch soll sichergestellt werden, dass die Stelle im Drittland oder die internationale Organisation, welche die Daten empfängt bzw. importiert, ein angemessenes Datenschutzniveau für natürliche Personen bietet (Art. 44 DSGVO).

81 Die Regelungen der deutschen Bundesländer in ihren Landeskrankenhausgesetzen (LKHG) zur Auftragsverarbeitung (siehe unten Kap. 3.4, S. 78 ff.) stellen keine derartigen gesetzlichen Grundlagen dar, denn sie ordnen keine Auftragsverarbeitung an, sondern ermöglichen diese lediglich, und dies auch nur unter bestimmten Bedingungen, zu denen i.d.R. ausdrücklich auch der Abschluss eines Vertrages gehört. Selbst ohne solche explizite Anordnung ist die DSGVO und damit das grundsätzliche Vertragserfordernis nach Art. 28 Abs. 3 DSGVO auch im Rahmen der weiten Öffnungsklausel für die Verarbeitung von Gesundheitsdaten (Art. 9 Abs. 4 DSGVO) und deren Nutzung durch die LKHG weiterhin subsidiär anwendbar.

Angemessenes Datenschutzniveau im Drittland (Art. 45 DSGVO)

Die erste mögliche Rechtsgrundlage für eine Drittlandübermittlung sind die Angemessenheitsbeschlüsse der EU-Kommission nach Art. 45 DSGVO. Diese besagen, dass ein Drittland, ein Gebiet oder Sektor in diesem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau bietet. Solche **Angemessenheitsbeschlüsse** existieren derzeit für Andorra, Argentinien, die Färöer-Inseln, Guernsey, Israel, die Isle of Man, Japan, Jersey, Neuseeland, die Schweiz, Uruguay sowie eingeschränkt auch für Kanada; entsprechende Gespräche mit Südkorea finden gegenwärtig statt.[82]

Auch für Datenübermittlungen in die USA bestand ein Angemessenheitsbeschluss auf Basis des sogenannten **Privacy Shield**-Abkommens zwischen der EU und den USA.[83] Dieser wurde allerdings vom EuGH in seinem sogenannten Schrems II-Urteil vom 16. Juli 2020 aufgehoben.[84] Für die Nutzung von Cloud-Diensten ist dieses Urteil von großer Bedeutung, da viele große Cloud-Anbieter aus den USA stammen.[85] Somit verliert Art. 45 DSGVO als Rechtsgrundlage für die Drittlandübermittlung erheblich an praktischer Bedeutung, da er derzeit keine datenschutzkonforme Übermittlung personenbezogener Daten in die USA mehr gewährleisten kann.

Geeignete Garantien für den Datenschutz beim Empfänger (Art. 46 DSGVO)

Die DSGVO bietet aber noch weitere Rechtsgrundlagen, die für eine Drittlandübermittlung herangezogen werden können. So darf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation gemäß Art. 46 auch auf vom Verantwortlichen oder dem Auftragsverarbeiter vorgesehene geeignete Garantien gestützt werden. Diese Garantien können in Form der folgenden „Transfertools" ausgestaltet sein.

Grundsätzlich geeignete Garantien nach Art. 46 DSGVO (Transfertools)

Die größte praktische Relevanz im Bereich der geeigneten Garantien kommt den Standarddatenschutzklauseln nach Art. 46 Abs. 2 Buchst. c DSGVO zu. Dabei handelt es sich um von der EU-Kommission erlassene Standardvertragsklauseln (**Standard Contractual Clauses, SCC**), die mit Verantwortlichen oder Auftragsverarbeitern im Drittland vereinbart werden können und welche die Vertragsparteien dann entsprechend bzgl. datenschutzrechtlicher Anforderungen binden.[86] Da es sich um von der Kommission vorgefertigte Klauseln handelt, müssen diese un-

[82] Quelle: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[83] Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, ABl. EU Nr. L 207 vom 1. August 2016, S. 1-112. Die auf Basis der EG-Datenschutzrichtlinie 95/46/EG erlassenen Angemessenheitsbeschlüsse wie der zum Privacy Shield gelten nach Art. 45 Abs. 9 DSGVO grundsätzlich auch unter der DSGVO fort.

[84] EuGH, Urteil vom 16. Juli 2020 - C-311/18 („Schrems II").

[85] Dies gilt insbesondere für die drei sogenannten „Hyperscaler": Amazon Web Services, Microsoft mit Azure und Google mit seiner Cloud Platform; Karlstetter, Was sind Hyperscaler?, CloudComputing-Insider, 31.08.2018.

[86] In Kraft sind derzeit für die Auftragsverarbeitung aber lediglich SCC in Bezug auf die sog. „Controller-to-Processor"-Konstellation (C2P) nach der Kommissions-Entscheidung 2010/87/EU (ABl. EU Nr. L 39 vom 12. Februar 2010, S. 6-18). Damit könnte ein verantwortliches Krankenhaus als „Controller" einen Cloud-Anbieter in den USA als „Processor" (Auftragsverarbeiter) einschalten, nicht aber ein europäischer KIS-Anbieter als „Processor" erster Stufe einen

verändert in den Vertrag übernommen werden. Sie müssen zudem so in den Vertragstext übernommen werden, dass deutlich wird, dass sie vor anderen Klauseln Vorrang haben. Konkretisierungen sind lediglich bezüglich der Art der Daten, der Form der Verarbeitung, den entsprechenden Zwecken sowie den technischen und organisatorischen Schutzmaßnahmen in den Anlagen zu einem Vertrag über die Auftragsverarbeitung nach dem Muster der Standardvertragsklauseln vorgesehen.

Außerdem kann die Drittlandübermittlung personenbezogener Daten gemäß Art. 46 Abs. 2 Buchst. e DSGVO auf Verhaltensregeln (**Codes of Conduct**) nach Art. 40 Abs. 3 DSGVO gestützt werden. Diese müssen allerdings mit durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters versehen sein und von der zuständigen Aufsichtsbehörde genehmigt sowie von der EU-Kommission mit allgemeiner Gültigkeit versehen sein. Im Krankenhausbereich gibt es momentan aber keine solchen Verhaltensregeln, so dass diese Rechtsgrundlage für den Drittlandtransfer vorliegend ausscheidet.

Entsprechendes gilt gemäß Art. 46 Abs. 2 Buchst. f DSGVO für die in Art. 42 DSGVO genauer beschriebenen **Zertifizierungsmechanismen**. Auch diese eröffnen Möglichkeiten für mehr Rechtssicherheit bei der Verarbeitung innerhalb der EU, aber grundsätzlich auch für einen Drittlandtransfer. Von den Aufsichtsbehörden genehmigte Zertifizierungsverfahren liegen derzeit aber noch nicht vor.[87]

Letztlich können gem. Art. 46 Abs. 3 Buchst. a DSGVO auch zwischen den Vertragsparteien individuell vereinbarte Vertragsklauseln geeignete Garantien darstellen, sofern diese von der zuständigen Aufsichtsbehörde genehmigt wurden. Die Aufsichtsbehörde wendet vor Genehmigung dieser sogenannten **Ad-hoc-Klauseln** das Kohärenzverfahren nach Art. 63 DSGVO an. Dieses Verfahren beruht auf der Zusammenarbeit der Aufsichtsbehörden untereinander und mit der Kommission und soll der einheitlichen Anwendung der DSGVO in der gesamten Union dienen. Es führt jedoch auch dazu, dass sich die Genehmigung solcher Klauseln in die Länge ziehen kann. Dies mag auch ein Grund dafür sein, dass solche Ad-hoc-Klauseln bislang eine untergeordnete Rolle für den Drittlandtransfern spielten. Hier ist jedenfalls kein Standard verfügbar, auf den die Krankenhäuser beim Cloud-Computing einfach zurückgreifen könnten.

Eine weitere Möglichkeit ist die Verwendung verbindlicher interner Datenschutzvorschriften (**Binding Corporate Rules, BCR**) nach Art. 47 DSGVO. Diese internen Vorschriften gelten nur für den Drittlandtransfer personenbezogener Daten innerhalb einer Unternehmensgruppe oder Gruppe von Unternehmen. Sie müssen für alle betreffenden Unternehmen und deren Mitarbeiter bindend sein und den betroffenen Personen ausdrücklich durchsetzbare Rechte übertragen. Für Krankenhäuser haben auch solche Regelungen keine oder kaum eine Bedeutung.

US-Cloud-Anbieter als „Processor" zweiter Stufe (Unterauftragnehmer), da dies keine „C2P"-, sondern eine „P2P"-Konstellation darstellen würde. Dieser Herausforderung könnte man z.B. durch einen direkten Vertragsschluss zwischen Krankenhaus und Cloud-Betreiber vermittelt durch den KIS-Anbieter begegnen (sog. Vertretungsmodell). Auch hat die Kommission am 12. November 2020 einen Entwurf für P2P-SCC vorgelegt: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries. Die Herausforderungen der ggf. nötigen ergänzenden Schutzmaßnahmen (s.u. S. 57 ff.) können allerdings weder durch das Vertretungsmodell noch die P2P-SCC, wenn sie denn in Kraft treten, umschifft werden. Vgl. dazu auch Hellmich/Hoffmann, Wie lässt sich der internationale Datentransfer retten?, LTO, 07.12.2020.

[87] Gühr/Karper/Maseberg, Der lange Weg zur Akkreditierung nach Art. 42 DSGVO, DuD 2020, 649 ff.

Zwar könnten sich auch Krankenhausgruppen solche internen Regeln geben und sie genehmigen lassen. Professionelle Cloud-Anbieter in Drittstaaten gehören aber in aller Regel nicht zur Gruppe eines Krankenhausunternehmens.

Liegen weder Angemessenheitsbeschlüsse nach Art. 45 DSGVO noch geeignete Garantien nach Art. 46 DSGVO oder verbindliche interne Datenschutzvorschriften nach Art. 47 DSGVO vor, kommt für eine datenschutzkonforme Drittlandübermittlung nur noch einer der **Ausnahmetatbestände des Art. 49 DSGVO** in Betracht. Da es sich bei den aufgeführten Anwendungsfällen ausdrücklich um Ausnahmeregelungen handelt, sind diese restriktiv auszulegen.

Im Krankenhaus-Kontext wäre wohl am ehesten eine ausdrückliche **Einwilligung** nach Art. 49 Abs. 1 Buchst. a DSGVO als Grundlage für die Drittlandübermittlung denkbar. Dabei ist allerdings zu bedenken, dass die Einwilligung stets freiwillig erfolgen muss (Art. 4 Nr. 11 DSGVO) und insofern auch strikten Kopplungsrestriktionen unterliegt (Art. 7 Abs. 4 DSGVO). Den Patienten müsste es somit freistehen, eine Verarbeitung ihrer personenbezogenen Daten, die eine Übermittlung in ein Drittland beinhaltet, abzulehnen. Zumindest in Krankenhäusern, die nach dem Landeskrankenhausplan öffentlich-rechtlich für die Versorgung der Bevölkerung zur Verfügung stehen, hätten die Patienten aber auch ohne Einwilligung in die Datenverarbeitung einen Anspruch auf Behandlung. Das würde zumindest für solche Krankenhäuser bedeuten, dass sie neben ihrem primären Cloud-KIS noch ein weiteres lokales KIS oder ein EU-KIS für Patienten, die nicht einwilligen und deren Behandlung gleichwohl nicht abgelehnt werden darf, vorhalten müssten. Insofern kann die Einwilligung nach Art. 49 Abs. 1 Buchst. a DSGVO nicht als in der Fläche praktikable Lösung für eine Drittlandübermittlung bei der Verwendung eines Cloud-KIS angesehen werden. Die vieldiskutierte Frage, ob eine Einwilligung überhaupt für regelmäßige oder doch nur für sporadische Datenübermittlungen in Drittländer zulässig ist, kann in diesem Zusammenhang also dahinstehen.[88]

Pflicht zur Bewertung der Effektivität der geeigneten Garantien im Drittland

Die vorstehend genannten Garantien, einschließlich der internen Datenschutzvorschriften, geltend grundsätzlich als zur Sicherstellung eines angemessenen Datenschutzniveaus geeignet. Die tatsächliche Wirksamkeit des Schutzes, den solche Garantien bieten können, hängt aber von den **Gegebenheiten im jeweiligen Drittland** ab.

Deshalb muss trotz Verwendung eines der genannten Transfertools immer auch eine Bewertung stattfinden, ob der jeweilige Vertragspartner im Drittland die zugesicherten Garantien überhaupt einhalten und somit tatsächlich ein angemessenes Schutzniveau gewährleisten kann. Bei dieser Bewertung ist insbesondere der Umfang der **Befugnisse öffentlicher Stellen** des Drittlands zu berücksichtigen. Ist ein Datenimporteur im Drittland nach den dortigen Gesetzen verpflichtet, personenbezogene Daten gegenüber Behörden offenzulegen, und nimmt dies Ausmaße an, die nach dem EU-Recht mit einer demokratischen Gesellschaft nicht verein-

[88] Vgl. dazu EDSA, Leitlinien 2/2018, S. 5, dort ablehnend, soweit nicht lediglich Einzelfälle betroffen sind, was bei einem kompletten Cloud-KIS nicht der Fall wäre. Ob wirklich keine wiederholten Übermittlungen (vgl. Art. 49 Abs. 1 Unterabs. 2 DSGVO) auf eine Einwilligung nach Art. 49 Abs. 1 Unterabs. 1 Buchst. a DSGVO, die für einen (ggf. abstrakt) bestimmten Fall erklärt wird, gestützt werden können, ist aber wie gesagt umstritten. Der Abgleich der beiden Unterabsätze spricht eher dafür, in dem „bestimmten Fall" nach Unterabs. 1 etwas anderes zu sehen als im Ausschluss wiederholter Übermittlungen nach Unterabs. 2.

bar sind, kann auch eine von diesem Datenimporteur zugesicherte Konformität mit den Regelungen der DSGVO keinen angemessenen Schutz bieten.[89] Da es sich bei den genannten Garantien lediglich um vertragliche Vereinbarungen zwischen den an einer Drittladübermittlung beteiligten Parteien handelt, sind diese für Behörden im Drittland selbstverständlich nicht bindend.

Pflicht zu ergänzenden Schutzmaßnahmen bei mangelhafter Effektivität

Führt die geforderte Bewertung zu dem Ergebnis, dass das verwendete Transfertool keinen effektiven Schutz bieten kann, zum Beispiel, weil nationale Behörden unangemessene Zugriffsbefugnisse auf personenbezogenen Daten haben, so müssen zusätzliche Maßnahmen zur Sicherstellung eines angemessenen Schutzniveaus ergriffen werden. Nach Auffassung des EuGH gilt dies derzeit für die USA.[90] Der EuGH macht jedoch keine weiteren Ausführungen zu den in Betracht kommenden Maßnahmen.[91]

Allerdings führt der **Europäische Datenschutzausschuss (EDSA)** in seiner aktuellen Empfehlung[92] einige ergänzende Maßnahmen auf, die in Kombination mit einem der Transfertools die Sicherstellung eines angemessenen Schutzniveaus unterstützen können. Der EDSA unterteilt dabei in technische, vertragliche und organisatorische Maßnahmen, weist aber darauf hin, dass letztlich nur technische Maßnahmen einen Zugriff durch Behörden im Drittstaat effektiv verhindern können. Es wird deshalb eine Kombination mehrerer, aufeinander aufbauender Maßnahmen empfohlen, um ein dem EU-Standard entsprechendes Datenschutzniveau zu erreichen.

Der EDSA nennt fünf Use Cases, für die aus seiner Sicht **effektive technische Maßnahmen** vorgesehen werden können:

Use Case 1: Datenspeicherung für Backup-Zwecke und andere Zwecke, die keinen Zugriff auf Daten im Klartext erfordern.
In diesem Fall kann durch starke (Ende-zu-Ende-)Verschlüsselung der personenbezogenen Daten vor der Übermittlung sichergestellt werden, dass ein Zugriff durch Behörden des Drittstaats verhindert wird. Die Schlüssel verbleiben beim Datenexporteur.

Use Case 2: Übermittlung pseudonymisierter Daten zu Analyse- oder Forschungszwecken
Die Pseudonymisierung personenbezogener Daten kann als effektive Maßnahme angesehen werden, sofern die zur Depseudonymisierung erforderlichen Zusatzinformationen ausschließlich beim Datenexporteur verbleiben.

[89] EuGH, Urteil vom 16. Juli 2020 - C-311/18 („Schrems II"), Rdnr. 135 (Grundregel), 186 f. (zu den USA).

[90] Vgl. EuGH, Urteil vom 16. Juli 2020 - C-311/18 („Schrems II").

[91] Der EuGH führt lediglich aus, dass der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien und ggf. ergänzende Maßnahmen treffen soll, um einen Ausgleich für den im Drittland bestehenden Mangel an Datenschutz zu bewirken: EuGH, Urteil vom 16. Juli 2020 - C-311/18 („Schrems II"), Rdnr. 91 ff. (geeignete Garantien wie Standardvertragsklauseln), 133 ff. (geeignete ergänzende Maßnahmen, wenn kein ausreichendes Schutzniveau trotz grds. geeigneter Garantien besteht).

[92] Vgl. EDSA, Recommendations 01/2020.

Use Case 3: Transportverschlüsselung bei Transit durch Drittländer
Will ein Datenexporteur personenbezogene Daten an einen Bestimmungsort mit angemessenem Datenschutzniveau übermitteln, wobei die Daten ein Drittland ohne angemessenes Datenschutzniveau passieren, so kann eine entsprechend starke Transportverschlüsselung eine effektive technische Maßnahme darstellen.[93]

Use Case 4: Datenübermittlung an besonders geschützte Empfänger
Werden personenbezogene Daten an einen Empfänger im Drittstaat übermittelt, der aufgrund der nationalen Gesetzgebung einen besonderen Schutz vor Zugriffen auf bei ihm befindliche Daten genießt, so kann eine Transportverschlüsselung als effektive Maßnahme zum Schutz der an diesen Empfänger übermittelten personenbezogenen Daten angesehen werden.

Use Case 5: Aufgeteilte oder Mehrpartei-Verarbeitung
Die aufgeteilte Verarbeitung personenbezogener Daten durch mehrere Parteien in der Form, dass jede Partei nur einen Teil erhält, der allein keinen Aufschluss auf bestimmte oder bestimmbare Personen gibt (Secure Multi Party Computation), kann als effektive technische Maßnahme angesehen werden.

Neben Szenarien, in denen entsprechend effektive technische Maßnahmen getroffen werden können, nennt der EDSA auch zwei Szenarien, in denen nach dem Stand der Technik **keine ausreichend effektiven technischen Maßnahmen** gefunden werden konnten. Beide Use Cases gelten für den Fall, dass öffentliche Stellen des Drittstaates Zugriffsbefugnisse auf personenbezogene Daten haben, die über das hinausgehen, was aus EU-Sicht in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist.[94]

Use Case 6: Übermittlung an Cloud-Anbieter oder sonstige Auftragsverarbeiter, die Zugriff auf Daten im Klartext benötigen
Benötigt ein Cloud-Anbieter oder sonstiger Auftragsverarbeiter im unsicheren Drittland zur Ausführung der ihm übertragenen Verarbeitungshandlungen Zugriff auf personenbezogene Daten im Klartext, so können laut dem EDSA nach dem heutigen Stand der Technik keine effektiven technischen Maßnahmen zum Schutz dieser Daten vorgesehen werden. Der EDSA schließt jedoch nicht aus, dass sich das im Zuge der technischen Weiterentwicklung ändern könnte.

Use Case 7: Fernzugriff auf personenbezogene Daten für gemeinsame Geschäftszwecke
Stellt ein Datenexporteur einem Datenimporteur im Drittland personenbezogene Daten für gemeinsame Geschäftszwecke, beispielsweise innerhalb einer Unternehmensgruppe, zur Verfügung, so können laut dem EDSA keine effektiven technischen Maßnahmen zum Schutz dieser Daten getroffen werden.

Neben den genannten technischen Maßnahmen nennt der EDSA auch einige **vertragliche Maßnahmen**, die dazu beitragen können, ein angemessenes Datenschutzniveau im Drittland sicherzustellen. Dabei wird allerdings nochmal betont, dass solche Maßnahmen die Behörden

[93] Wobei der EDSA (Recommendations 01/2020, S. 24) darauf hinweist, dass ergänzend eine Ende-zu-Ende-Verschlüsselung der personenbezogenen Inhalte angezeigt sein kann, wenn die Transportverschlüsselung aufgrund von Schwächen der eingesetzten Infrastruktur oder Software allein keinen ausreichenden Schutz bietet.

[94] EDSA, Recommendations 01/2020, S. 26-27, Nr. 87-90.

eines Drittlands selbstverständlich nicht zu binden vermögen und daher für sich genommen, auch in Kombination mit einem der üblichen Transfertools, nicht für ein angemessenes Datenschutzniveau bei Empfänger ausreichen, wenn in dessen Staat aus EU-Sicht ausufernde Zugriffsbefugnisse für öffentliche Stellen bestehen. Dennoch könnten vertragliche Abreden, wie die Verpflichtung zur Verwendung bestimmter technischer Maßnahme oder die Vereinbarung von Informations- und Transparenzpflichten, die im jeweiligen Transfertool bereits enthaltenen Schutzvorkehrungen unterstützen und verstärken.[95]

Zuletzt nennt der EDSA **organisatorische Maßnahmen** wie interne Richtlinien, Organisationsmethoden oder Standards, die Verantwortliche und Auftragsverarbeiter einerseits sich selbst, andererseits aber auch Datenimporteuren im Drittstaat auferlegen können. Diese könnten dazu beitragen, einen einheitlichen Schutz personenbezogener Daten während des gesamten Verarbeitungszyklus sicherzustellen. Zwar können auch diese organisatorischen Maßnahmen allein nicht sicherstellen, dass ein Datentransfer den Anforderungen des EU-Rechts genügt. Sie seien aber gegebenenfalls erforderlich, um technische und vertragliche Maßnahmen so zu ergänzen, dass ein angemessenes, im Wesentlichen dem in der EU gleichwertiges Datenschutzniveau gewährleistet werden kann.[96]

Nach dem EDSA kommt somit eine Verarbeitung von Klartextdaten in Drittländern, deren Datenschutzniveau aufgrund von Zugriffsbefugnissen dortiger öffentlicher Stellen als unangemessen gilt, nicht in Betracht.[97] Ob das in dieser Allgemeinheit dem Verhältnismäßigkeitsgrundsatz im Sinne eines Risiko-basierten Ansatzes auch bezüglich der rechtlichen Risiken in Drittländern gerecht wird, kann man hinterfragen.[98] In Bezug auf Patientendaten als besonders schützenswerte Kategorie von Daten (Art. 9 DSGVO), die zudem nach deutschem Recht noch einem Beschlagnahmeverbot (§ 97 StPO) unterliegt, erscheint dieses „Verdikt" des EDSA jedoch nachvollziehbar.

Die Verwendung von **Cloud-Diensten**, die Server in den **USA** nutzen, dürfte somit für den Betrieb eines Cloud-KIS **ausscheiden**, da eine Übermittlung personenbezogener Patientendaten in die USA auf Basis der aktuellen Rechtslage kaum DSGVO-konform möglich ist.

3.1.4 Cloud-Computing durch Anbieter im EWR mit Bezug zu unsicheren Drittländern

Es wird deshalb diskutiert, ob stattdessen EU-Tochtergesellschaften oder -Niederlassungen entsprechender US-Anbieter, die eigene Server in der EU oder dem EWR betreiben, eingesetzt werden können. In der Regel kann dadurch eine Übermittlung in einen Drittstaat wie die USA vermieden werden.

Während dem grundsätzlich zugestimmt werden kann, muss an dieser Stelle aber auf den **Konflikt zwischen der DSGVO und dem U.S. CLOUD Act** hingewiesen werden. Das zuletzt genannte Gesetz erlaubt es US-Behörden, Daten von Unternehmen anzufordern, die US-Recht

[95] EDSA, Recommendations 01/2020, S. 28, Nr. 93.

[96] EDSA, Recommendations 01/2020, S. 35, Nr. 122.

[97] Vgl. EDSA, Recommendations 01/2020, S. 26-27, Nr. 88.

[98] So z.B. der Bitkom in seiner Stellungnahme vom 21. Dezember 2020 zum Entwurf der Empfehlungen des EDSA: https://www.bitkom.org/sites/default/files/2020-12/20201221_bitkom-position-edpb-recommendations.pdf.

unterliegen.[99] Dabei wird ausdrücklich klargestellt, dass es nicht von Bedeutung ist, wo sich diese Daten befinden. Demnach wären bei Anwendung des CLOUD Act auch Daten auf den EU-Servern von Unternehmen mit US-Bezug nicht sicher vor dem Zugriff durch US-Behörden.

Diese Zugriffsmöglichkeit kollidiert mit **Art. 48 DSGVO**, wonach Offenlegungsverlangen auf Basis eines Urteils eines Gerichts oder der Entscheidung einer Verwaltungsbehörde im Drittland nur nachgekommen werden darf, wenn zwischen dem ersuchenden Drittland und der Union eine entsprechende internationale Übereinkunft besteht wie zum Beispiel ein Rechtshilfeabkommen. Solche Abkommen bestehen zwar zwischen den USA und Mitgliedstaaten der EU wie auch Deutschland. Sie schreiben allerdings vor, dass öffentliche Stellen im jeweiligen Mitgliedstaat, in dem die Daten belegen sind, der Herausgabe an die USA zustimmen müssen. Somit würde eine Offenlegung personenbezogener Daten allein auf Verlangen einer öffentlichen Stelle in den USA ohne Zustimmung durch eine entsprechende Stelle im betroffenen EU-Mitgliedstaat einen Verstoß gegen Europäisches Datenschutzrecht darstellen.

Grundsätzlich steht den betroffenen Providern auch nach dem CLOUD Act **Rechtsschutz** gegen entsprechende Offenlegungsverlangen unter Bezugnahme auf das Recht des Speicherortes der Daten zur Verfügung. Dies ist jedoch nur dann der Fall, wenn eine Offenlegung mit hoher Wahrscheinlichkeit das Recht einer „qualifizierten Regierung" verletzen würde. Die entsprechende Qualifizierung einer Regierung erfordert dabei den Abschluss eines bilateralen Vertrags mit den USA (sogenannte „executive agreements"). Eine solche Vereinbarung existiert derzeit nur zwischen den USA und dem Vereinigten Königreich. Unternehmen in der EU mit US-Bezug müssen sich bei der Anfrage einer US-Behörde somit entscheiden, ob sie gegen US- oder EU-Recht verstoßen.[100] Selbst wenn ein Provider aufgrund eines „executive agreements" Rechtsbehelfe gegen eine Herausgabeanordnung aus den USA unter Berufung auf das Recht des Speicherortes der Daten einlegen dürfte und einen solchen auch einlegt, hätte das zuständige US-Gericht im Rahmen der dann durchzuführenden Prüfung („comity analysis") einen Spielraum, die Ermittlungsinteressen der USA höher zu gewichten als die Einhaltung des aus seiner Sicht ausländischen Rechts.[101]

In diesem Zusammenhang wird teilweise die Meinung vertreten, dass es möglich sein muss, diesen Zielkonflikt zwischen CLOUD Act und DSGVO durch eine **Interessenabwägung** zu lösen. Demnach schließe „[e]in einseitiger und absoluter Vorrang des europäischen Datenschutzrechts, der in einem solchen Fall jegliche Abwägung von vornherein ausschließen und per se zu einer Verletzung des ausländischen Rechts führen würde […] international agierende CSP [Cloud Service Provider, Anmerkung der Verfasser] de facto vom europäischen Markt aus".[102] Da der CLOUD Act lediglich auf die Beweiserlangung bei schweren Verbrechen anwendbar sei,

[99] Der vollständige Titel dieses Gesetzes lautet "Clarifying Lawful Overseas Use of Data Act". Der Gesetzestext dieses „Artikelgesetzes", das mehrere Abschnitte des Titels 18 des U.S. Codes (Bundesrechts) zum Strafverfahren geändert hat, kann hier abgerufen werden: https://www.congress.gov/bill/115th-congress/house-bill/4943.

[100] Vgl. dazu Piltz, Schrems II: US CLOUD Act kein Problem?.

[101] Section 2703 lit. h of title 18, U.S. Code; siehe soeben S. 60, Fn. 99, oder https://www.law.cornell.edu/uscode/text/18/2703.

[102] Rost/Brink/Birk, Cloud Computing und Datenschutz, RDV 2020, S. 240, 243.

sollte es „[…] unter Einhaltung der DS-GVO gelingen, eine Vereinbarkeit zwischen beiden Interessenlagen, der US-amerikanischen und der europäischen, herzustellen".[103] Der CLOUD Act dürfe deshalb nicht als unüberwindliches Hemmnis verstanden werden und sei aufgrund der neuen Qualität, welche die Verbrechen im digitalen Zeitalter erlangt haben, auch notwendig.[104]

Dass der Konflikt zwischen DSGVO und U.S. CLOUD Act mit der Schrems II-Entscheidung des EuGH an Bedeutung gewonnen hat, zeigt allerdings auch ein Blick ins Nachbarland **Frankreich**. Dort hat die nationale Datenschutzaufsichtsbehörde CNIL die Speicherung von Gesundheitsdaten des französischen **„Health Data Hub"** auf in der EU belegenen Servern eines Unternehmens, das über seine Konzernmutter auch US-Recht unterliegt (Microsoft Ireland Operations Limited), für rechtswidrig erklärt und untersagt.[105]

Dem folgte das oberste französische Verwaltungsgericht (**Conseil d'État**) im vorläufigen Rechtsschutz jedoch nicht und hat eine Beschwerde gegen das Hosting des dortigen Health Data Hub mit Microsoft Irland als Serviceprovider abgelehnt.[106] Das Gericht begründete seine Entscheidung damit, dass im Rahmen des Health Data Hub eine Übermittlung von Gesundheitsdaten in Länder außerhalb der EU vertraglich ausgeschlossen wurde und eine derartige Übermittlung aufgrund eines französischen Ministerialerlasses vom 9. Oktober 2020 zudem verboten sei. Außerdem beziehe sich die Schrems II-Entscheidung des EuGH lediglich auf die Übermittlung personenbezogener Daten in die USA, nicht aber auf die Verarbeitung personenbezogener Daten in der EU durch Tochtergesellschaften von US-Unternehmen. Die streitgegenständliche Datenverarbeitung stelle auch keinen aktuellen Verstoß gegen die DSGVO, sondern allenfalls das Risiko eines solchen dar und könne schon deshalb nicht umgehend unterbunden werden. Als zusätzliche Sicherheitsmaßnahme würden die Daten vor dem Hosting pseudonymisiert und mittels von Microsoft zur Verfügung gestellter Tools verschlüsselt. Ein weiteres Argument für die Aufrechterhaltung der Datenverarbeitung durch **Microsoft Irland** für den Health Data Hub sei das wichtige öffentliche Interesse, das aufgrund der COVID-19-Pandemie an der Datenverarbeitung zu Zwecken der Forschung und Bekämpfung des Virus bestehe, zumal eine vergleichbare Alternative zu den Services von Microsoft derzeit nicht zur Verfügung stünde. Das Gericht machte allerdings auch deutlich, dass ein Zugriff bzw. ein Offenlegungsersuchen von US-Behörden gegenüber Microsoft Irland nicht völlig ausgeschlossen werden könne und somit ein Restrisiko für die personenbezogenen Daten bestünde. Es forderte den Health Data Hub und Microsoft Irland deshalb auf, eine zwischen den Unternehmen bereits getroffene Datenschutz-Zusatzvereinbarung zu überarbeiten und darin klarzustellen, dass Microsoft personenbezogene Daten nur an Behörden weitergeben darf, wenn das Recht der Europäischen Union oder eines Mitgliedstaats (und somit ausdrücklich nicht das Recht der

[103] Rost/Brink/Birk, Cloud Computing und Datenschutz, RDV 2020, S. 240, 244.

[104] Vgl. Rost/Brink/Birk, Cloud Computing und Datenschutz, RDV 2020, S. 240, 244. Das wirft nach hier vertretener Auffassung allerdings die Frage auf, ob eine solche Abwägung nicht eher eine politische Aufgabe der EU und/oder ihrer Mitgliedstaaten wäre, welche sich überlegen könnten, der DSGVO entgegenkommende Vereinbarungen mit den USA auszuhandeln, die ggf. die Zustimmung spezieller Stellen der Strafverfolgungsbehörden am Datenspeicherort erfordern, wenn diese auch nicht im Einzelfall wie bei klassischen Rechtshilfeersuchen den teils zeitraubenden diplomatischen Weg nehmen müssten.

[105] Vgl. https://www.cnil.fr/en/council-state-asks-health-data-hub-additional-guarantees-limit-risk-transfer-united-states.

[106] Conseil d'État, Entscheidung vom 13. Oktober 2020 – Aktenzeichen 444937, https://www.conseil-etat.fr/Media/actualites/documents/2020/10-octobre/ordonnance-n-444937.

USA) dies vorschreibt. Das Gericht ordnete an, ihm die überarbeitete Vereinbarung vorzulegen.[107]

Diese Entscheidung des Conseil d'État im einstweiligen Rechtsschutz ist anhand der vorstehend zusammengefassten Argumente gut nachvollziehbar. Allerdings wird beim Health Data Hub mit der **Pseudonymisierung** vor Übertragung in die Cloud auch eine technische Schutzmaßnahme angewendet, die nach dem Europäischen Datenschutzausschuss grundsätzlich sogar eine Übermittlung in unsichere Drittstaaten rechtfertigen könnte. Zudem enthalten die Standardverträge zur Auftragsverarbeitung der großen US-Cloud-Anbieter für den europäischen Markt gerade nicht die **Beschränkung von Datenherausgaben** – ohne oder gegen die Weisung des Auftraggebers – auf Verpflichtungen nach dem Recht der EU oder eines Mitgliedstaates, wie es das Gericht gemäß Art. 28 Abs. 3 S. 2 Buchst. a Halbsatz 2 DSGVO gefordert hat. Diese Standardbedingungen sprechen in der Regel nur allgemein von rechtlichen Verpflichtungen, denen der Cloud-Anbieter unterliegt. Denn die Hyperscaler sind sich der möglichen Kollision der Rechtsordnungen von USA sowie EU durchaus bewusst und wollen hier möglichst keine klare Stellung beziehen. Vor diesem Hintergrund lässt sich dem im Eilrechtsschutz getroffenen Beschluss des Conseil d'Etat eine generelle Folgerung dahingehend, dass die Verarbeitung von Patientendaten im Klartext bei Providern, die dem CLOUD Act unterliegen, zulässig ist, nicht entnehmen.

Insbesondere, wenn es – wie im Falle eines KIS in der Cloud – um Gesundheitsdaten geht, muss nach **deutschem Recht** neben der datenschutzrechtlichen Zulässigkeit auch die strafrechtliche Relevanz einer Offenlegung nach dem U.S. CLOUD Act betrachtet werden. Dies betrifft einerseits die Verletzung von Privatgeheimnissen nach § 203 StGB und andererseits das Beschlagnahmeverbot nach § 97 StPO. Eine Offenlegung von Gesundheitsdaten gegenüber einer US-Behörde auf Verlangen dieser Behörde könnte somit nicht nur einen Datenschutzverstoß, sondern auch eine **Straftat** darstellen.[108] Die Einschaltung von Cloud-Providern, die dem CLOUD Act unterliegen, zur Verarbeitung von Patientendaten im Klartext ist folglich mit erheblichen rechtlichen Risiken behaftet und sollte vermieden werden.[109]

3.1.5 Technische und organisatorische Maßnahmen der Datensicherheit

Die Sicherheit der Verarbeitung ist für alle personenbezogenen Daten in Art. 32 DSGVO geregelt. Dieser normative Ansatz gilt allgemein, unabhängig davon, ob es sich um Patientendaten in einem KIS handelt und ob die Verarbeitung in der Cloud oder vor Ort erfolgt. Gleichwohl

[107] Hierfür wurde eine Frist von 15 Tagen gesetzt, welche bereits abgelaufen ist. Eine weitere Entscheidung zu dieser Angelegenheit ist bislang jedoch nicht bekannt.

[108] Siehe dazu unten Kap. 3.3, S. 66 ff. Ausländisches Recht, wie der CLOUD Act bzw. Titel 18 U.S. Code, stellt keine gesetzliche Offenbarungsbefugnis i.S.v. § 203 StGB dar, weshalb z.B. auch in § 43e Bundesrechtsanwaltsordnung (BRAO) zum Schutz vor dem Zugriff ausländischer Behörden gefordert wird, dass im Sitzland der ausländischen Diensteanbieter ein dem Inland vergleichbares Geheimnisschutzniveau besteht; vgl. Cornelius, NJW 2017, 3751, 3754. Auch folgende Kommentatoren nennen ausschließlich deutsche Rechtsvorschriften als Befugnisnormen: Cierniak/Niehaus, in: MüKo StGB, § 203 Rdnr. 91 f.; Weidemann, in: BeckOK StGB, § 203 Rdnr. 52-54 (Stand: 01.11.2020); Eisele, in: Schönke/Schröder, StGB, § 203 Rdnr. 82-85.

[109] Wenn sich die in der EU belegenen Provider allerdings vertraglich auf eine ausschließliche Geltung des Rechts der EU und ihrer Mitgliedstaaten einlassen, dann kann die Risikoabwägung ggf. anders, nämlich zu Gunsten einer rechtlichen Nutzbarkeit dieser Provider ausfallen, wenn die faktische Abhängigkeit der Anbieter von ihrem EU-Geschäft die vom US-Geschäft erheblich überwiegt; vgl. unten Kap. 6.3.2, S. 289 f.

können sich für Cloud-KIS aus diesem gemeinsamen normativen Ansatzpunkt besondere Anforderungen hinsichtlich technischer und organisatorischer Maßnahmen ergeben, die dem Risiko der entsprechenden Verarbeitung adäquat sind.

Denn nach Art. 32 Abs. 1 Halbsatz 1 DSGVO treffen der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen, um ein **dem Risiko angemessenes Schutzniveau** zu gewährleisten.

Nach Art. 32 Abs. 1 Halbsatz 2 DSGVO können hierzu folgende Maßnahmen gehören:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten,

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Gemäß Art. 32 Abs. 2 DSGVO sind bei der Beurteilung des angemessenen Schutzniveaus also insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind. Nach der nicht abschließenden Aufzählung des Art. 32 Abs. 2 DSGVO bestehen diese Risiken in der Vernichtung, dem Verlust, der Veränderung sowie der unbefugten Offenlegung von bzw. dem unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden, gleich ob dies unbeabsichtigt oder unrechtmäßig erfolgt.

Die DSGVO enthält somit eine Regelung, die auch bei Nutzung der **Öffnungsklauseln** in der DSGVO für **Gesundheitsdaten** durch die Mitgliedstaaten zumindest subsidiär anwendbar bleibt. Zusätzliche Bedingungen für die Verarbeitung von Gesundheitsdaten dürfen die Mitgliedstaaten nach Art. 9 Abs. 4 DSGVO allerdings beibehalten oder einführen. Diese zusätzlichen Bedingungen dürften sich auch auf Maßnahmen der Datensicherheit und nicht nur solche der grundlegenden Rechtmäßigkeit beziehen. Sie haben somit Vorrang vor Art. 32 DSGVO, schließen aber einen Rückgriff auf diese Vorschrift, soweit die zusätzlichen Regelungen schweigen, nicht aus.[110]

Bei der Konkretisierung risikoadäquater Maßnahmen wird vor diesem Hintergrund für Cloud-KIS zu berücksichtigen sein, dass **Patientendaten** eine sensible Kategorie personenbezogener Daten darstellen, die nach Art. 9 DSGVO **besonders geschützt** sind. Der Schutzbedarf dieser

[110] Im Übrigen konkretisieren einige Landesdatenschutzgesetze wie das in Baden-Württemberg auch den Katalog der Maßnahmen, an welche auch bei der Verarbeitung „normaler" personenbezogener Daten zu denken ist. Da durch diese „(Regel-)Beispielstechnik" keine zwingende rechtliche Vorgabe verbunden ist, mag dies mit dem insoweit vorrangigen Europarecht noch vereinbar sein, auch wenn es insoweit gewisse Zweifel gibt.

Daten und damit – als einer der beiden grundlegenden Faktoren des Risikos – das Schadenspotential bei Verletzung ihres Schutzes sind im Allgemeinen hoch oder sehr hoch. Vor allem im Hinblick auf den anderen grundlegenden Faktor des Risikos, der Wahrscheinlichkeit des Schadenseintritts, werden für Cloud-KIS neben der allgemeinen Frage des sicheren Betriebs von KIS die spezifischen Gefährdungen der Cloud zu berücksichtigen sein, insbesondere mit ihrer Abhängigkeit von einer Netzanbindung (als Gefährdung der Verfügbarkeit), aber auch mit ihrer Öffnung für einen Zugriff über das lokale Netz hinaus (als Gefährdung der Vertraulichkeit).

3.2 Datenschutzrechtliche Anforderungen an Cloud-KIS nach Bundesrecht

3.2.1 Bundesdatenschutzgesetz (BDSG)

Das neue, an die DSGVO angepasste Bundesdatenschutzgesetz (BDSG) enthält – im Gegensatz zum früheren, bis 24.05.2018 geltenden § 11 BDSG a.F. – keine Vorschriften zur Auftragsverarbeitung mehr. Soweit keine besonderen Vorschriften hierzu aus anderen Gesetzen anwendbar sind (vgl. § 1 Abs. 2 BDSG), sondern auf nationaler Ebene allein das BDSG Anwendung findet, verbleibt es damit lediglich bei der Geltung von Art. 28 DSGVO und den Ausführungen nach dem vorigen Abschnitt.[111]

3.2.2 Die Regelungen der Sozialgesetzbücher (SGB)

Der Schutz von Sozialdaten nach dem SGB X

Die allgemeinen Regeln zum Sozialdatenschutz im 2. Kapitel des SGB X gelten lediglich für Stellen nach § 35 SGB I und dies sind vor allem die Leistungsträger in der Sozialversicherung, zu denen auch die Krankenkassen in der GKV gehören. Wenn diese Cloud-Anbieter beauftragen wollen, müssen sie für diese Verarbeitung von Sozialdaten im Auftrag auch § 80 SGB X beachten. Dieser enthält ergänzend zu Art. 28 DSGVO einige Anforderungen, die kurz wie folgt zusammengefasst werden können:

- Abs. 1: Rechtzeitige vorherige Anzeige bei der Rechts- oder Fachaufsichtsbehörde
- Abs. 2: Verarbeitung nur in
    - Deutschland,
    - einem anderen Mitgliedstaat der EU,
    - einem nach § 35 Abs. 7 SGB I gleichgestellten Staat (Vertragsstaat des EWR) oder
    - einem Drittstaat oder einer internationalen Organisation, soweit ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt[112].
- Abs. 3: Auftrag an nicht-öffentliche Stellen ist grundsätzlich nur zulässig, wenn
    - beim Verantwortlichen sonst Störungen im Betriebsablauf auftreten können oder
    - die übertragenen Arbeiten beim Auftragsverarbeiter erheblich kostengünstiger besorgt werden können.
- Abs. 4: Klarstellende Regelungen zur Datenschutzaufsicht

[111] Siehe soeben Abschnitt 3.1, S. 49 ff.

[112] Ansonsten grundsätzlich geeignete Garantien nach Art. 46 DSGVO reichen insoweit nicht aus.

- Abs. 5: Ausnahme von Abs. 3 für die bloße Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen; im Umkehrschluss werden diese Tätigkeiten damit aber grundsätzlich als Auftragsverarbeitung eingestuft.

Auf Krankenhäuser ist diese recht restriktive Vorschrift jedoch nicht anwendbar, auch wenn diese Leistungen für die GKV erbringen.

Grundsätzlich finden SGB I und SGB X auf Krankenhäuser als Leistungserbringer keine Anwendung, da diese nicht von § 35 SGB I umfasst sind und somit auch keine Sozialdaten nach der Definition des § 67 Abs. 2 SGB X verarbeiten.[113] Allerdings bestehen Ausnahmen zu diesem Grundsatz, sofern andere Vorschriften die entsprechende Anwendung des § 35 SGB I auf Leistungserbringer ausdrücklich vorsehen.[114] Eine Anwendbarkeit von Regelungen des SGB X auf Leistungserbringer ohne ausdrücklichen Verweis, wie sie das Bundessozialgericht (BSG) in einer Entscheidung vom 10.12.2008[115] angenommen hat, ist nach der hier vertretenen Meinung hingegen ausgeschlossen.[116] Vor diesem Hintergrund hat das genannte Urteil in der Literatur auch ganz überwiegend Kritik erfahren.[117]

Es ergeben sich somit keine zusätzlichen rechtlichen Anforderungen an die Verwendung von Cloud-basierten KIS durch Krankenhäuser aus den SGB I und SGB X.

Der Schutz von Leistungsdaten nach dem SGB V

Denn für Leistungserbringer gelten lediglich die für sie gemünzten Vorschriften des SGB V. Die entsprechenden Vorschriften enthalten für diese lediglich im Titel zur Übermittlung von Leistungsdaten einzelne Vorgaben zur Auftragsverarbeitung, so in

- § 295a SGB V für die Abrechnung von Selektivverträgen,
- § 300 Abs. 2 SGB V für die Einschaltung von Apothekenrechenzentren,
- § 301a Abs. 2 SGB V für die Einschaltung von Rechenzentren durch Hebammen und
- § 302 Abs. 2 S. 2 ff. SGB V für die Einschaltung von Rechenzentren durch sonstige Leistungserbringer.

Die Übermittlung von Leistungsdaten zur Abrechnung der Krankenhäuser mit der GKV ist in § 301 SGB V geregelt, wo jedoch eine entsprechende Regelung zur Einschaltung bzw. Zwischenschaltung von Auftragnehmern fehlt.

Hieraus könnte man den Umkehrschluss ziehen, dass Krankenhäuser zur Abrechnung mit der GKV keine Auftragnehmer einschalten dürfen. Entsprechend urteilte auch das BSG in der bereits genannten Entscheidung vom 10. Dezember 2008.[118] Demnach sei die Weitergabe von Patientendaten durch Leistungserbringer im Geltungsbereich des SGB V nur dann und in dem Umfang erlaubt, wie es die Vorschriften des SGB V über die Datenverarbeitung gestatten. Die

[113] Siehe Schneider, VSSR 2009, 381, 386-394.

[114] Siehe dazu bspw. § 295a Abs. 1 S. 1 Halbsatz 2 SGB V.

[115] BSG, Urteil vom 10. Dezember 2008 – B 6 KA 37/07 R.

[116] Vgl. dazu auch Dierks, Lösungsvorschläge für ein neues Gesundheitsforschungsdatenschutzrecht in Bund und Ländern, S. 73.

[117] Vgl. dazu bspw. Schneider, VSSR 2009, 381, 387 m.w.N.

[118] BSG, Urteil vom 10. Dezember 2008 – B 6 KA 37/07 R.

allgemeinen Datenschutzregelungen fänden insoweit keine Anwendung. Somit dürften Krankenhäuser die Patientendaten gesetzlich Versicherter nicht zur Leistungsabrechnung an private Dienstleistungsunternehmen übermitteln. Entsprechend ohne gesetzliche Ermächtigung erstellte Abrechnungen dürfe eine kassenärztliche Vereinigung deshalb zurückweisen.

Gerade auch angesichts des nach diesem Urteil erfolgten gesetzgeberischen Nachjustierens von Vorschriften zur Einschaltung von Auftragnehmern durch bestimmte Leistungserbringer und Außerachtlassung von anderen Leistungserbringern ist ein solcher Schluss nicht ganz fernliegend,[119] da das SGB V in seinem Anwendungsbereich jedenfalls Vorrang vor den „flexibleren" Regelungen des allgemeinen Datenschutzrechts hat.[120] Dies gilt nach hier vertretener Auffassung jedoch nur für die Zwischenschaltung von Auftragsverarbeitern bei der Übermittlung von Leistungsdaten zur Abrechnung mit der GKV.[121] Im Übrigen bleibt das allgemeine Datenschutzrecht auch auf die genannten Leistungserbringer anwendbar, sowohl was die subsidiäre Geltung für Abrechnungsvorgänge als auch die alleinige Geltung für die rein medizinische Datenverarbeitung angeht.[122]

Ein KIS kann weit mehr Funktionen haben als die Abrechnung mit der GKV. Außerdem würde die Auslagerung eines KIS in eine Cloud nicht gezielt und allein zur Übermittlung von Leistungsdaten an die GKV erfolgen, sondern bereits, um die Speicherung dieser Daten effizienter zu gestalten. Daher soll vorerst davon ausgegangen werden, dass die einschlägigen Vorschriften des SGB V dem entsprechenden Outsourcing eines KIS nicht kategorisch im Wege stehen, auch soweit im KIS Leistungsdaten zur Abrechnung mit der GKV gespeichert werden. Unter dieser Prämisse birgt auch das SGB V keine nennenswerten rechtlichen Anforderungen an die Verwendung Cloud-basierter KIS durch Krankenhäuser.[123]

3.3 Verhältnis von Datenschutzrecht und Schweigepflicht

3.3.1 Schweigepflicht der Heilberufe und Outsourcing an mitwirkende Personen

Grundlagen der Schweigepflicht der Heilberufe

Die Schweigepflicht der Heilberufe ergibt sich aus dem ärztlichen Berufsrecht (vgl. § 9 MBO-Ä),[124] dem Behandlungsvertrag (§§ 630a – 630h BGB), sowie aus dem Strafrecht. Sie wird insbesondere durch § 203 StGB zur „Verletzung von Privatgeheimnissen" strafrechtlich vorgegeben und bei vorsätzlichen Verstößen sanktioniert.[125]

---

[119] Anderer Ansicht ist bspw. Kircher, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, S. 192, 205 ff.

[120] Schneider, VSSR 2009, 381, 387 ff.; Schneider, in: Krauskopf, SGB V, § 295 Rdnr. 22.

[121] So schon Schneider, VSSR 2009, 381, 388 ff.; Schneider, in: Krauskopf, SGB V, § 294 Rdnr. 14.

[122] Siehe soeben Fn. 121.

[123] Zum gleichwohl bestehenden gesetzgeberischen Anpassungs- und Klarstellungsbedarf s. unten Kap. 6.1.2, S. 282, und Schneider, VSSR 2009, 381, 400 f., sowie Schneider, in: Krauskopf, SGB V, § 295a Rdnr. 10.

[124] (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte

[125] § 203 StGB legt insoweit den Mindeststandard fest, vgl. Eisele, in: Schönke/Schröder, StGB, § 203 Rdnr. 47. Das Vorsatzerfordernis ergibt sich aus § 15 StGB, wobei ein Offenbaren durch Datenweitergabe an einen Auftragsverarbeiter meist offensichtlich und damit vorsätzlich stattfinden dürfte. Zum Verhältnis der Schweigepflicht zum (Sozial-)Datenschutz s. auch Schneider, VSSR 2009, 381, 384 f.

Gemäß § 203 Abs. 1 Nr. 1 StGB wird mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert, anvertraut worden oder sonst bekannt geworden ist.

Nach § 203 Abs. 3 S. 2 Halbsatz 1 StGB dürfen die in Absatz 1 genannten Personen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Person erforderlich ist. Das Gleiche gilt gemäß § 203 Abs. 3 S. 2 Halbsatz 2 StGB auch für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in Absatz 1 Genannten mitwirken.

Mit einer Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird gemäß § 203 Abs. 4 S. 1 StGB bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person bekannt geworden ist. Nach § 203 Abs. 4 S. 2 StGB wird ebenso bestraft, wer (1.) als in Absatz 1 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in Absatz 1 genannte Person sind, (2.) als in Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in Absatz 1 genannte Person sind, oder (3.) nach dem Tod der nach Satz 1 oder nach dem Absatz 1 verpflichteten Personen ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

Gemäß § 203 Abs. 5 StGB sind die Absätze 1 bis 4 auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

§ 203 Abs. 6 StGB bestimmt, dass die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe ist, wenn der Täter gegen Entgelt oder in der Absicht sich oder einem anderen zu bereichern oder einen anderen zu schädigen handelt.

Neuregelung des § 203 StGB im Jahr 2017 und Auslagerung von Tätigkeiten

§ 203 Abs. 3, Abs. 4 StGB der jetzigen Fassung des Strafgesetzbuches wurden erst am 30. Oktober 2017 in das StGB eingefügt.[126] Vor der Reform des § 203 StGB war eine Heranziehung von externen Dienstleistern zu Hilfstätigkeit für die von § 203 StGB umfassten Berufsgruppen nicht oder jedenfalls nicht ohne erhebliches rechtliches Risiko möglich, sofern diese Dienstleister dadurch von geschützten Geheimnissen Kenntnis erlangen konnten und keine einschlägige

[126] Artikel 1 Nr. 2 Buchst. c des Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 30. Oktober 2017, BGBl. I S. 3618.

Befugnisnorm oder ausdrückliche Einwilligung des Berechtigten vorhanden war.[127] Denn externe Dienstleister wurden nach herrschender Meinung nicht als Gehilfen der Berufsgeheimnisträger angesehen. Es war in einer solchen Konstellation auch ausgeschlossen oder zumindest äußerst fraglich, ob mittels einer Vertragsgestaltung, die den Dritten zur Verschwiegenheit verpflichten und die Kontrolle durch den Berufsgeheimnisträger ermöglichen sollte, eine Strafbarkeit nach § 203 StGB umgangen werden konnte.[128]

Aufgrund dieser Probleme sah die Bundesregierung Handlungsbedarf zur Schaffung berufsrechtlicher Befugnisnormen und zur Einschränkung der Strafbarkeit außerhalb seiner Kompetenz zur Schaffung solcher Befugnisnormen.[129] Sie führte aus, dass das Zugänglichmachen von geschützten Geheimnissen gegenüber Personen, die zwar nicht in die Sphäre des Berufsgeheimnisträgers eingegliedert sind, aber dennoch an dessen beruflicher oder dienstlicher Tätigkeit mitwirken, ein Offenbaren darstelle. Der Berufsgeheimnisträger würde jedoch befugt und damit nicht rechtswidrig handeln, soweit ein Offenbaren für die Inanspruchnahme dieser sonstigen mitwirkenden Person erforderlich sei. Die mit der Einbindung dritter Personen verbundene Verringerung des Geheimnisschutzes solle dadurch kompensiert werden, dass die mitwirkenden Personen in die Strafbarkeit nach § 203 StGB einbezogen werden können. Den Berufsgeheimnisträger treffe hierbei die – unabhängig von berufsrechtlichen oder sonstigen rechtlichen Vorgaben – geltende Pflicht dafür Sorge zu tragen, dass die einbezogenen Personen zur Geheimhaltung verpflichtet werden. Die Verletzung der Pflicht solle strafbewehrt sein, wenn die einbezogene Person unbefugt ein Geheimnis offenbart habe.[130]

Der Regierungsentwurf wurde letztlich weitgehend unverändert verabschiedet und trat im November 2017 in Kraft. Im neue § 203 Abs. 3 StGB findet sich nun eine Regelung zur Einschaltung von intern mitwirkenden Personen (berufsmäßig tätige Gehilfen oder zu Vorbereitung auf den Beruf tätige Personen) in Satz 1 sowie zu externen sonstigen mitwirkenden Personen in Satz 2. Die Befugnis nach § 203 Abs. 3 Satz 1 StGB wirkt tatbestandsausschließend, sodass schon keine strafbare Offenbarung gegeben ist. § 203 Abs. 3 Satz 2 StGB wirkt hingegen nicht tatbestandsausschließend, sondern stellt einen Rechtfertigungsgrund dar.[131]

Allerdings verlangt § 203 Abs. 4 S. 2 Nr. 1 StGB von den Berufsgeheimnisträgern, dass sie jegliche mitwirkenden Personen, die sie einschalten, gleich ob interne Gehilfen oder externe Dienstleister, zur Geheimhaltung entsprechend der für sie geltenden Regelungen verpflichten. Unterlassen sie dies, machen sie sich strafbar, wenn die mitwirkende Person ein ihr zugänglich

[127] Zur Rechtslage insoweit vor dieser Reform: Schneider, VSSR 2009, 381, 385 m.w.N.

[128] Allenfalls eine förmliche Verpflichtung nach dem Verpflichtungsgesetz hätte Dienstleister öffentlicher Kliniken zu für den öffentlichen Dienst besonders Verpflichteten gemacht (§ 11 Abs. 1 Nr. 4 StGB) und möglicherweise, wenn auch nicht sicher, eine Strafbarkeit des Offenbarens von Patientengeheimnissen ausgeschlossen. Vgl. hierzu und zu Sondervorschriften in Baden-Württemberg, die auf die Schweigepflicht Bezug nehmen: Schneider, Sekundärnutzung klinischer Daten, S. 269 f.

[129] Gesetzentwurf der Bundesregierung zur Reform der Schweigepflicht (soeben Fn. 126), Bundestags-Drucksache 18/11936 vom 12. April 2017, S. 1.

[130] Zum Ganzen: Regierungsentwurf zum Schweigepflicht-Reformgesetz, Bundestags-Drucksache 18/11936, S. 2.

[131] Fischer StGB § 203 Rdnr. 45 f.

gemachtes Geheimnis unbefugt offenbart.[132] Gleiches gilt nach § 203 Abs. 4 S. 2 Nr. 2 StGB, wenn eine mitwirkende Person eine weitere mitwirkende Person einschaltet.

Der Gesetzgeber hat auch klargestellt, dass für das Vorliegen einer Offenbarung nach § 203 StGB bereits die Möglichkeit der Kenntnisnahme durch einen externen Dienstleister ausreicht.[133] Es bedarf keiner tatsächlichen Kenntnisnahme des externen Dienstleisters.[134]

Externe Dienstleister im IT-Bereich und Cloud-Anbieter

Der neue § 203 Abs. 3 S. 2 Halbsatz 1 StGB betrifft externe Dienstleister, denen fremde Geheimnisse im Rahmen ihrer Mitwirkung an beruflichen oder dienstlichen Tätigkeiten des Berufsgeheimnisträgers bekannt werden, wie beispielsweise Mitarbeiter von Service-, Reparatur- und Wartungsunternehmen, etwa EDV-Wartung. In der Gesetzesbegründung des § 203 Abs. 3 StGB sind die folgenden, nicht abschließende Regelbeispiele mitwirkender Tätigkeiten aufgeführt:[135]

- Schreibarbeiten,
- Rechnungswesen,
- Annahme von Telefonanrufen,
- Aktenarchivierung und -vernichtung,
- Einrichtung, Betrieb, Wartung – einschließlich Fernwartung – und Anpassung informationstechnischer Anlagen, Anwendungen und Systeme aller Art, beispielsweise auch von entsprechend ausgestatteten medizinischen Geräten,
- Bereitstellung von informationstechnischen Anlagen und Systemen zur externen Speicherung von Daten,
- Mitwirkung an der Erfüllung von Buchführungs- und steuerrechtlichen Pflichten des Berufsgeheimnisträgers.

Auch wird in der Begründung Folgendes festgehalten:[136] „Für sämtliche in § 203 Absatz 1 StGB genannten Personen kann zudem die Speicherung von Daten auf externen informationstechnischen Anlagen (wie z. B. in einer „Cloud") wirtschaftlich sinnvoll sein. Diese wirtschaftlichen Interessen von Berufsgeheimnisträgern sind grundsätzlich berechtigt, Voraussetzung ist allerdings, dass sie in Einklang gebracht werden können mit den berechtigten Interessen der Inhaber der Geheimnisse an deren rechtlichen Schutz."

[132] Fischer StGB § 203 Rdnr. 55 ff.

[133] Regierungsentwurf zum Schweigepflicht-Reformgesetz, Bundestags-Drucksache 18/11936, S. 28. Vor Inkrafttreten dieses Gesetzes wurde z.T. in der Literatur angenommen, dass es einer tatsächlichen Kenntnisnahme durch den Dritten bedürfe, wenn für diesen nur kurzeitig (Fern-)Zugriff auf ein IT-System bestand, z.B. für Wartungszwecke, vgl. Bundestags-Drucksache 18/11936, S. 18. Auch nach alter Rechtslage war jedoch unstreitig, dass es keiner tatsächlichen Kenntnisnahme bedurfte, wenn die Datenhaltung auf Dritte ausgelagert wurde. Und nach neuer Rechtslage gilt dies ausweislich des insoweit offenen Gesetzeswortlautes und der eindeutigen Gesetzesbegründung selbst für den bloß temporären Zugriff auf ein an anderer Stelle vorgehaltenes datenhaltendes System.

[134] So nun auch einhellig die Literatur in Anschluss an die Gesetzesbegründung. Siehe nur: Cornelius NJW 2017, 3571, 3572; Weidemann in BeckOK StGB § 203 Rdnr. 37.

[135] Regierungsentwurf zum Schweigepflicht-Reformgesetz, Bundestags-Drucksache 18/11936, S. 22.

[136] Regierungsentwurf zum Schweigepflicht-Reformgesetz, Bundestags-Drucksache 18/11936, S. 18.

Somit lassen sich auch Dienstleister im Cloud Computing-Bereich unter den Begriff der sonstigen mitwirkenden Personen nach § 203 Abs. 3 Satz 2 StGB fassen.[137]

Erforderlichkeit des Offenbarens und Schutzmaßnahmen wie eine Verschlüsselung

Eine Offenbarung an externe Dienstleister ist nach § 203 Abs. 3 S. 2 StGB zulässig, wenn sie zur Inanspruchnahme von deren Tätigkeiten erforderlich ist. Voraussetzung hierfür ist, dass die Offenbarung auch nur in dem Umfang erfolgt, der für die Mitwirkung und Unterstützung der jeweils primär geheimnisverpflichtenden Tätigkeit tatsächlich erforderlich ist.[138] Es kommt aber gerade nicht darauf an, ob die Beauftragung des Externen für die Ausübung der Tätigkeit des Berufsgeheimnisträgers erforderlich ist.[139]

Es stellt sich folglich die Frage, wann ein Offenbaren erforderlich ist und wann gegebenenfalls eine client-basierte Verschlüsselung oder andere Schutzmaßnahmen gegenüber sonstigen mitwirkenden Personen wie beispielsweise eine Pseudonymisierung verlangt werden können. Hierbei steht die Praktikabilität und Wirtschaftlichkeit der Systeme, wie bereits in der eben zitierten Gesetzesbegründung ausgeführt,[140] in einem Spannungsfeld mit dem Schutz von Patientendaten durch § 203 StGB. Dies ist insbesondere bei Public-Cloud-Systemen diskussionswürdig, kann aber auch für Private-Cloud- oder Community-Cloud-Systemen unter Umständen von Bedeutung sein.[141]

Der Begriff der Erforderlichkeit wird teilweise als sehr vage kritisiert. Der einzelne Schweigeverpflichtete könne die für die Beurteilung der Erforderlichkeit vielfältigen technischen Fragestellungen kaum selbst beurteilen und müsse daher von vorneherein verhindern, dass der Externe auf die für die Tätigkeit nicht erforderlichen Daten zugreifen könne. Der Begriff sei daher ungeeignet die bestehende Rechtunsicherheit zu beseitigen.[142] Zum Teil wird sogar ein Verstoß gegen den Bestimmtheitsgrundsatz des Art. 103 Abs. 2 GG angenommen.[143]

Dem wird mit der Ansicht, dass mit dieser Voraussetzung signifikante Einschränkungen des Outsourcings oder die Schaffung weiterer Rechtsunsicherheiten kaum verbunden sein dürften, entgegengetreten.[144] So wird im Münchener Kommentar zum StGB dazu ausgeführt:[145]

„Wenn etwa die Mitwirkung im Verwalten eines Kundendatenbestandes des Geheimhaltungsverpflichten oder in der Anpassung der Kundenverträge an veränderte Gegebenheiten besteht, so

[137] Fischer StGB § 203 Rn. 45 f.

[138] Regierungsentwurf zum Schweigepflicht-Reformgesetz, Bundestags-Drucksache 18/11936, S. 22 f.; Fischer StGB § 203 Rdnr. 48.

[139] Eisele in Schönke/Schröder StGB § 203 Rdnr. 51; Cornelius NJW 2017, 3571 (3572). Beispiel des Arztes, der seine Abrechnungen zulässig extern bearbeiten lassen kann, obwohl er dies ohne weiteres selbst vornehmen könnte.

[140] Regierungsentwurf zum Schweigepflicht-Reformgesetz, Bundestags-Drucksache 18/11936, S. 18.

[141] Bei einer Community Cloud, die z.B. von mehreren Krankenhäusern betrieben wird, wäre das eine Krankenhaus eine sonstige mitwirkende Person des anderen Krankenhauses; dabei ist zu beachten, dass die Schweigepflicht auch zwischen verschiedenen originär nach § 203 Abs. 1 StGB Schweigeverpflichteten gilt. Und auch eine Private Cloud könnte von einem professionellen Dienstleister für ein Krankenhaus betrieben werden.

[142] So: Eisele in Schönke/Schröder StGB § 203 Rdnr. 52.

[143] Weidemann in BeckOK StGB § 203 Rdnr. 37, mit Verweis auf Fechtner/Haßdenteufel CR 2017, 355, 360.

[144] Cierniak/Niehaus in Münchner Kommentar StGB § 203 Rdnr. 138.

[145] Cierniak/Niehaus in Münchner Kommentar StGB § 203 Rdnr. 138.

wird – entsprechend der gesetzgeberischen Zielrichtung – die Übermittlung des gesamten Kundendatenbestandes nach Abs. 3 Satz 2 erlaubt sein. Gleiches gilt für die vom Gesetzgeber ausdrücklich angesprochene externe Speicherung von Daten, etwa im Rahmen von Cloud-Systemen."

Weiter wird hier ausgeführt, dass das Merkmal der Erforderlichkeit in der Praxis lediglich ein „symbolisches Entgegenkommen" gegenüber den Kritikern der Neuregelung sei und eine Inanspruchnahme Externer nicht wirksam begrenzen könne, da eine Differenzierung nach erforderlichen und nicht-erforderlichen Teilen von Datenbeständen bei der Übermittlung erkennbar sinnwidrig sei.[146]

Keine der beiden Ansichten vermag vollends zu überzeugen. Der Begriff der Erforderlichkeit ist mehr als nur reine Symbolik. Er ist Bestandteil des Gesetzeswortlautes und wirkt einschränkend, soweit bestimmte Daten zur Ausführung der ausgelagerten Tätigkeit eben nicht erforderlich sind und gegebenenfalls auch dann, wenn technische Möglichkeiten wie Verschlüsselung oder Pseudonymisierung die Erforderlichkeit doch entfallen lassen können. Gerade die Einschätzung der zuletzt technischen Möglichkeiten wird die Bewertung der Erforderlichkeit tatsächlich nicht immer einfach machen. Allerdings besteht keine derart große Rechtsunsicherheit, wie sie manch andere Kommentierungen annehmen. In der Praxis wir sich ein Berufsgeheimnisträger zwar immer auch einen eigenen Eindruck bilden müssen, kann dabei jedoch im Hinblick auf die technischen Möglichkeiten auf die Aussagen der Hersteller und bestenfalls auch der Aussteller von Datenschutz- und IT-Sicherheits-Zertifikaten zurückgreifen. Zur Disziplinierung der Hersteller kann hier das Lauterkeitsrecht und die Abmahnbarkeit von Verstößen gegen die Schweigeflicht bzw. der Anstiftung oder Beihilfe hierzu eine wichtige Rolle spielen. Über eine Anstiftung oder Beihilfe zur Schweigepflichtverletzung durch nicht erforderliches Offenbaren durch Berufsgeheimnisträger könnten Verantwortliche bei den Herstellern wie auch den Zertifikatausstellern nicht zuletzt auch strafrechtlich sanktioniert werden, wenn sie vorsätzlich technische Möglichkeiten „unterschlagen", um ihre einfachere Lösung zu vermarkten.

Die Erforderlichkeit der Offenbarung lässt sich letztlich wie folgt beschreiben: Solange die Tätigkeit durch technische oder organisatorische Maßnahmen auch ohne eine Kenntnisnahme des Geheimnisses durch den externen Dienstleister bewirkt werden kann, ist eine Offenbarung grundsätzlich nicht erforderlich. Ist nach dem Stand der Technik eine Kenntnisnahme durch solche Maßnahmen nicht vermeidbar, so ist eine Offenbarung grundsätzlich erforderlich.[147] Der Vorsitzende Richter am BGH a. D. Fischer legt in seinem Kommentar den Begriff der Erforderlichkeit in nachvollziehbarer Weise in seinem Kommentar dementsprechend wie folgt aus:[148] § 203 Abs. 3 S. 2 StGB enthält „keine Befugnis zu einer allgemeinen Öffnung des Schutzbereichs gegenüber Externen, so dass insoweit auch weiterhin organisatorische Vorkehrungen und interne Sicherungen vorzuhalten sind, um die Offenbarung auf das zwingend Erforderliche zu beschränken. Wird dieser Bereich überschritten, entfällt insoweit die Rechtfertigung. Die Erforderlichkeit bestimmt sich nach den konkreten Umständen der externen Tätigkeit, ist aber unabhängig von subjektiven oder vertraglichen Festlegungen zu beurteilen."

[146] Cierniak/Niehaus in Münchner Kommentar StGB § 203 Rdnr. 138.

[147] So auch: Cornelius NJW 2017, 3571, 3572.

[148] Fischer StGB § 203 Rdnr. 48.

Auch in der Gesetzesbegründung wird darauf hingewiesen, dass „die einem Berufsgeheimnisträger anvertrauten oder ihm in beruflicher Eigenschaft sonst bekannt gewordenen Geheimnisse in seiner Sphäre verbleiben [sollen] und [...] diese nur im erforderlichen Ausmaß verlassen" dürfen; bei „einer das erforderliche Ausmaß übersteigenden Offenbarung" macht sich demnach der Berufsgeheimnisträger selbst strafbar.[149] Die Betonung des erforderlichen Ausmaßes legt sehr nahe, dass dem Gesetzgeber keineswegs eine Alles-oder-Nichts-Lösung bezüglich der Datenbestände der Berufsgeheimnisträger vorschwebte, sondern er die Offenbarungsbefugnis vom der Art der ausgelagerten Tätigkeit und den jeweils zu prüfenden Erfordernissen abhängig machen wollte.

Grundsätzlich gilt somit, dass alle nach Stand der Technik möglichen technischen und organisatorischen Maßnahmen zur Vermeidung einer Offenbarung ergriffen werden müssen und bei einer Offenbarung Ausmaß und Umfang durch Sicherheitsvorkehrungen auf das zwingend Erforderliche beschränkt werden müssen.

Diese Maßnahmen könnten unter anderem eine Anonymisierung, eine Pseudonymisierung oder eine Verschlüsselung der Daten mit alleinigem Schlüssel des Geheimnisträgers sein.[150] Soweit eine Verschlüsselung, Anonymisierung oder Pseudonymisierung der Daten für die Tätigkeit des Dienstleisters nach Stand der Technik nicht möglich ist, ist die Offenbarung nach § 203 Abs. 3 Satz 2 StGB erforderlich.

So nimmt auch Cornelius zunächst an, dass „Anonymisierung, Pseudonymisierung oder Verschlüsselung von Daten (solange der Geheimnisträger allein den jeweiligen Schlüssel hat) beim IT-Outsourcing nach wie vor die Mittel der Wahl" seinen.[151] Um dann jedoch auszuführen, dass nach heutigem Stand der Technik eine Verschlüsselung ausscheide, wenn der Externe im Fall der Auslagerung des Rechnungswesens an externe IT-Dienstleister notwendigerweise mit dem fremden Geheimnis in Kontakt kommt oder die Daten in einer Cloud im Rahmen einer „Software-as-a-Service" nicht nur gespeichert, sondern auch verarbeitet werden.[152]

Dem ist jedoch nur teilweise zuzustimmen. Eine Verschlüsselung der Dateninhalte (nicht lediglich des Transports) bei „Software-as-a-Service" ist nach dem Stand der Technik nicht unmöglich, sondern nur eingeschränkt möglich. So kann eine externe Speicherung auch mit einer client-basierten Verschlüsselung erfolgen und bestimmte weitergehende Verarbeitungsvorgänge, wie beispielsweise das gezielte Suchen über einen verschlüsselten Datenbestand, sind ebenfalls möglich. Insoweit wird man auch hier dann von „Software-as-a-Service" und nicht nur von „Infrastructure-as-a-Service" oder Platform-as-a-Service" sprechen können. Bei der Verarbeitung von verschlüsselten Daten ist aber in jedem Fall mit gewissen Performance-Einbußen zu rechnen. Eine darüberhinausgehende Form der Verarbeitung, insbesondere mit statistischen Analysen oder Methoden der KI, ist jedoch mangels praktikabler homomorpher Verschlüsselung derzeit in einer verschlüsselten Form noch nicht möglich.

[149] Regierungsentwurf zum Schweigepflicht-Reformgesetz, Bundestags-Drucksache 18/11936, S. 28.

[150] Cornelius NJW 2017, 3571, 3572.

[151] Cornelius NJW 2017, 3571, 3572.

[152] Cornelius NJW 2017, 3571, 3572.

Weitergehende „Software-as-a-Service"-Leistungen können zudem mit einer Pseudonymisierung vereinbar sein, denn hier werden in der Cloud dann nur die pseudonymisierten Daten verarbeitet. Dies setzt aber voraus, dass im Krankenhaus ein Client zuvor die Pseudonymisierung und nach Rückmeldung von Ergebnissen die De-Pseudonymisierung vornimmt. Die Komplettverlagerung eines KIS in die Cloud unter Verzicht auf jegliche über bloße Anzeigetools hinausgehende lokale Software wäre damit aber nicht möglich.

Vor diesem Hintergrund könnte man wohl vertreten, dass der Betrieb eines kompletten KIS eine Tätigkeit ist, deren Auslagerung gemäß § 203 Abs. 3 Satz 2 StGB mangels möglicher technischer Alternativen der Erforderlichkeit unterfällt und für welche das Offenbaren von unmittelbar personenbezogenen Patientendaten somit ebenfalls erforderlich wäre. Für das Outsourcing von Teilmodulen von KIS verbleibt es aber in der Regel beim Erfordernis von Schutzmaßnahmen, die eine Offenbarung in der Regel ausschließen werden.

Selbst bei technischer Möglichkeit der Maßnahme muss sich die Erforderlichkeit aber auch daran messen lassen, inwiefern sie die Inanspruchnahme externer mitwirkender Personen in tatsächlicher Weise erschwert oder faktisch unmöglich macht. Technisch mögliche, aber wirtschaftlich nicht tragbare oder jedenfalls dysfunktionale Maßnahmen wird man allein vor dem Hintergrund der Schweigepflicht wohl nicht verlangen können. So könnten beispielsweise verschlüsselungsbedingte Performance-Einbußen zu sehr langen Wartezeiten für Rückmeldungen aus einem Cloud-Systemführen. Dies wäre insbesondere bei Modulen mit akutmedizinischer Bedeutung[153] bedenklich, da im Notfall eine schnelle Rückmeldung von entscheidender Bedeutung sein kann.

Deswegen könnte als Maßstab statt eines technisch-absoluten Unmöglichkeitsbegriff ein relativer „Unmöglichkeitsbegriff" angewendet werden, der sowohl technische als auch wirtschaftliche Aspekte berücksichtigt und eher als Zumutbarkeitsschwelle zur groben Unverhältnismäßigkeit bezeichnet werden kann.[154] Denn gerade die Wirtschaftlichkeit des Outsourcings bestimmter Tätigkeiten an mitwirkende Personen war maßgebliche Begründung für die Reform des § 203 StGB.[155] Vor diesem Hintergrund könnte man unter Umständen eine temporäre Verarbeitung von personenbezogenen Daten der Patienten, auch mit Gesundheitsbezug, ohne zusätzliche Sicherheitsmaßnahmen vornehmen können, wenn dies zur Erbringung der Dienste in einer wirtschaftlichen Weise notwendig ist. Je flüchtiger die Speicherung und je rückstandsfreier der Zustand nach der Verarbeitung ist, desto eher wird man hiervon ausgehen können. Bei Teil-Funktionalitäten oder Zusatzprogrammen (Add-Ons) zeigen bereits auf dem Markt befindliche Angebote hingegen, dass Maßnahmen zur Pseudonymisierung oder Verschlüsselung technisch und wirtschaftlich ohne nennenswerte Funktionseinbußen durchführbar sein können.

[153] Anders könnte dies z.B. bei reinen Archivsystemen zu bewerten sein.

[154] Dieser Maßstab ist auch nach der hier vertretenen Auffassung allerdings strenger als die übliche Verhältnismäßigkeitsprüfung bei technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, selbst wenn dort das besondere Risiko für Patientendaten berücksichtigt wird. Der hiesige Maßstab orientiert sich eher an den zivilrechtlichen Kriterien für einen grob unverhältnismäßigen Aufwand entsprechend § 275 Abs. 2 BGB, wenn auch nicht an dem für eine (sei es auch nur faktische) Unmöglichkeit nach § 275 Abs. 1 BGB, vgl. Grüneberg, in Palandt (Begr.), BGB, § 275 Rdnr. 4 ff. (zu den Arten der Unmöglichkeit), Rdnr. 22 (zur faktischen Unmöglichkeit, Rdnr. 26 ff. (zum groben Missverhältnis).

[155] Vgl. Regierungsentwurf zum Reformgesetz, Bundestags-Drucksache 18/11936, S. 17.

Eine solche nur temporäre Speicherung von Patientendaten kann bei Eingreifen von weiteren Vorschriften aber grundsätzlich unzulässig sein. So ist im vertragsärztlichen Bereich ein solches Outsourcing, jedenfalls zur Abrechnung mit den Krankenkassen, nach § 295 SGB V wohl nicht erlaubt. Dies dürfte sich im Umkehrschluss aus § 295a Abs. 2 SGB V ergeben, wo der Gesetzgeber bewusst für die selektivvertragliche Abrechnung von Vertragsärzten ein solches Outsourcing gestattet.[156]

Darüber hinaus sind in jedem Fall technische und organisatorische Zugangsbeschränkungen zu treffen. Dies gilt insbesondere, wenn eine Verschlüsselung, Pseudonymisierung oder Anonymisierung von Daten technisch nicht möglich ist. Die Standard-Sicherheitsmaßnahmen der Public-Cloud-Systeme können den besonderen Schutzbedarf von Patientendaten aber unter Umständen nicht vollständig abbilden, sodass erweiterte Zugangsbeschränkungen als Sicherheitsmaßnahmen zu besorgen sein könnten. Eine solche erweiterte technische Zugangsbeschränkung könnte beispielsweise eine 2-Faktor-Authentifizierung sein.[157]

3.3.2 Datenschutz und Schweigepflicht als eigenständige Schranken für die Weitergabe von Patientendaten

Die deutsche Zwei-Schranken-Theorie im Hinblick auf Datenschutz und Schweigepflicht[158] bleibt auch nach Inkrafttreten der DSGVO erhalten.[159] Das heißt, dass die jeweiligen Voraussetzungen des Datenschutzes und der Schweigepflicht unabhängig voneinander zu prüfen sind und für eine Übermittlung bzw. ein Offenbaren von Patientendaten vorliegen müssen. Die Erfüllung der Voraussetzungen des einen Normkomplexes führt nicht zwingend zur Einhaltung der Anforderungen des anderen Komplexes. Eine datenschutzrechtliche Erlaubnis zur Datenweitergabe bedingt damit nicht automatisch eine Offenbarungsbefugnis im Sinne der Schweigepflicht.

Dies lässt sich zunächst aus Art. 9 Abs. 3 DSGVO entnehmen:[160] Nach dieser Vorschrift können die besonderen Datenkategorien wie Gesundheitsdaten zu medizinischen Zwecken u.a. durch Fachpersonal erhoben werden, das „dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach Unionsrecht oder dem Recht eines Mitgliedstaates oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt".

[156] Schneider, VSSR 2009, 381, 387 f. Verfassungsrechtlich bestehen Bedenken, ob aufgrund dieser Regelungslücke eine sachlich nicht gerechtfertigte und somit verfassungswidrige Ungleichbehandlung der Vertragsärzte in der Regelversorgung gegeben ist. Weitere Ausführungen hierzu müssen, da sie nicht Gegenstand des Gutachtens sind, unterbleiben. Zum Sozialdatenschutz siehe auch unten Kap. 3.2.2, S. 64 ff.

[157] DSK, Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern, Anlage, Nr. 14, 14.11.2014.

[158] Ausführlich: Schneider, Sekundärnutzung klinischer Daten, S. 76 ff. m.w.N.

[159] Cornelius NJW 2017, 3751, 3753 m.w.N.; im Ergebnis auch: Dierks, Lösungsvorschläge für ein neues Gesundheitsforschungsdatenschutzrecht in Bund und Ländern, S. 76.

[160] Vgl. Schneider, Einrichtungsübergreifende elektronische Patientenakten, S. 485, noch zu Art. 89 Abs. 1 Buchst. a Halbsatz 2 DSGVO-Kommissionsentwurf, der aber weitgehend in Art. 9 Abs. 3 DSGVO übernommen wurde, mit der Abwandlung, dass nach dem neuen Wortlaut auch die Union entsprechende Geheimhaltungspflichten erlassen könnte, freilich aber nur, soweit sie dazu die primärrechtliche Gesetzgebungskompetenz hat.

Daneben findet sich in Art. 90 DSGVO eine weitere Vorschrift, in der der Unionsgesetzgeber die Mitgliedsstaaten ermächtigt, den Aufsichtsbehörden weitere Befugnisse einzuräumen, um Verantwortliche oder Auftragsverarbeiter zu kontrollieren, die einem von den zuständigen nationalen Stellen auferlegten Berufsgeheimnis oder einer gleichwertigen Geheimhaltungspflicht unterliegen. Der Unionsgesetzgeber erkennt damit auch die ärztliche Schweigepflicht als nationales Berufsgeheimnis (§ 9 MBO-Ä, § 203 StGB) grundsätzlich an.

Auch der nationale Gesetzgeber hat, als er im Rahmen des Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (DSAnpUG-EU)[161] das BDSG neu gefasst hat, die parallele Geltung von Datenschutz und Schweigepflicht fortgeschrieben. So wurde in § 1 Abs. 2 S. 2 BDSG n.F. der Passus, dass die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten (§ 203 Abs. 1 Nr. 1 StGB) oder von Berufsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen (§ 9 MBO-Ä), vom BDSG unberührt bleibt, unverändert aus § 1 Abs. 3 S. 2 BDSG a.F. übernommen.

Schließlich ist festzustellen, dass die Schweigepflicht in Deutschland in gesetzlicher Form in § 203 StGB und damit strafrechtlich geregelt ist, wofür dem Unionsgesetzgeber nach den Art. 2 ff. AEUV im Allgemeinen keine oder nur sehr eingeschränkte Kompetenz zusteht, sodass die DSGVO insoweit die ärztliche Schweigepflicht ohnehin kaum modifizieren oder im Wege des Anwendungsvorrangs verdrängen könnte.[162]

Zudem dürften die Mitgliedstaaten nach Art. 9 Abs. 4 DSGVO für die Verarbeitung von Gesundheitsdaten ohnehin zusätzliche Bedingungen – wie solche zur Schweigepflicht – aufstellen.

Damit sind bei der Sekundärnutzung medizinischer Behandlungsdaten nach wie vor die beiden Schranken – Datenschutz und Schweigepflicht – zu beachten.

3.3.3 Zusammenfallen von datenschutzrechtlicher Erlaubnis und Offenbarungsbefugnis in Sonderfällen

Wenn sich eine datenschutzrechtliche Erlaubnis jedoch speziell auch das Arzt-Patienten-Verhältnis einbezieht, dann stellt diese Rechtsgrundlage auch eine Befugnis zum Offenbaren im Sinne der Schweigepflicht dar.[163]

Auseinanderfallen bei allgemeinen Normen nach DSGVO und BDSG

Allgemeine datenschutzrechtliche Normen wie Art. 28 DSGVO zur Auftragsverarbeitung oder auch die Normen des BDSG können daher keine Offenbarungsbefugnisse im Sinne der Schweigepflicht darstellen. Eine abweichende Bewertung dann möglich, wenn das Outsourcing der personenbezogenen Patientendaten zwar den datenschutzrechtlichen Anforderungen entspricht, aber nicht gemäß § 203 Abs. 3 S. 2 StGB erforderlich ist.[164]

[161] BGBl. I S. 1626

[162] Vgl. Schneider, Einrichtungsübergreifende elektronische Patientenakten, S. 482, Fn. 2415 m.w.N.

[163] Schneider, VSSR 2009, 381, 382 f. m.w.N.; Schneider, Sekundärnutzung klinischer Daten, S. 76.

[164] Cornelius NJW 2017, 3751, 3752 f.

Zusammenfallen bei Datenschutzregeln in den Landeskrankenhausgesetzen

Anders sieht dies bei den Datenschutzregeln der Landeskrankenhausgesetze aus, die bereichsspezifisch für Patientendaten gemacht wurden und die teils auch Regelungen zur Auftragsverarbeitung enthalten; diese Regelungen sind gleichzeitig Offenbarungsbefugnisse im Sinne des § 203 StGB.[165] Im Anwendungsbereich dieser Regelungen kommt es damit nur darauf an, ob ihre jeweiligen Voraussetzungen erfüllt sind (einschließlich des subsidiär anwendbaren Art. 18 DSGVO), nicht aber darauf, ob ein Offenbaren nach § 203 Abs. 3 S. 2 StGB erforderlich ist. Die Nutzung von Verschlüsslung und/oder Pseudonymisierung ist zwar auch nach Datenschutzrecht als technische Schutzmaßnahme zu prüfen (vgl. Art. 28 Abs. 3 S. 2 Buchst. c i.V.m. Art. 32 Abs. 1 Halbsatz 2 Buchst. a DSGVO), jedoch nicht so streng wie im Strafrecht. Die gilt selbst dann, wenn man im zuletzt genannten Gebiet nur den Maßstab der groben Unverhältnismäßigkeit anlegt, also schon dann keine Pflicht zu diesen Maßnahmen annimmt, wenn es die ausgelagerte Tätigkeit unter Berücksichtigung von Performance- und Wirtschaftlichkeitsaspekten praktisch unmöglich machen würde.[166]

Datenschutzrechtliche Einwilligung und Schweigepflichtentbindung

Auch eine datenschutzrechtliche Einwilligung kann, soweit sie sich auf Gesundheitsdaten und den Behandlungskontext bezieht, gleichzeitig als Schweigepflichtentbindung im Sinne des § 203 StGB gewertet werden. Allerdings ist ein entsprechendes Vorgehen jedenfalls für Kernmodule eines KIS kaum praktikabel, da für Patienten, welche die Einwilligung verweigern, was sie dürfen, dann Alternativsysteme vor Ort auf dem Krankenhauscampus vorgehalten werden müssten.[167]

3.4 Datenschutzrechtliche Anforderungen an Cloud-KIS in den Bundesländern

Auf den Patientendatenschutz in Krankenhäusern sind der Kompetenzordnung des Grundgesetzes folgend vor allem die jeweiligen Landeskrankenhausgesetze (LKHG) anwendbar, die vielfach auch Vorgaben zur Datenverarbeitung im Allgemeinen und der Auftragsverarbeitung im Besonderen enthalten. Dabei verweisen diese LKHG aber teils ausdrücklich wieder auf andere Vorschriften. Und auch im Übrigen, soweit die LKHG keine besonderen Regelungen enthalten, finden allgemeinere Regelungen wie das jeweilige Landesdatenschutzgesetz (LDSG), das Bundesdatenschutzgesetz (BDSG) oder die Datenschutz-Grundverordnung (DSGVO) Anwendung.

Grob zusammengefasst lässt sich folgende Struktur erkennen:

[165] Zu den Details siehe unten Kap. 3.3, S. 66 ff. Zum Grundsatz nach geltendem Recht: Dierks, Lösungsvorschläge für ein neues Gesundheitsforschungsdatenschutzrecht in Bund und Ländern, S. 76. Zur im Grundsatz vergleichbaren früheren Rechtslage: Schneider, Sekundärnutzung klinischer Daten, S. 266 ff.

[166] Siehe dazu oben Kap. 3.3.1, S. 73.

[167] Ähnlich auch Weidemann in BeckOK StGB § 203 Rdnr. 125.

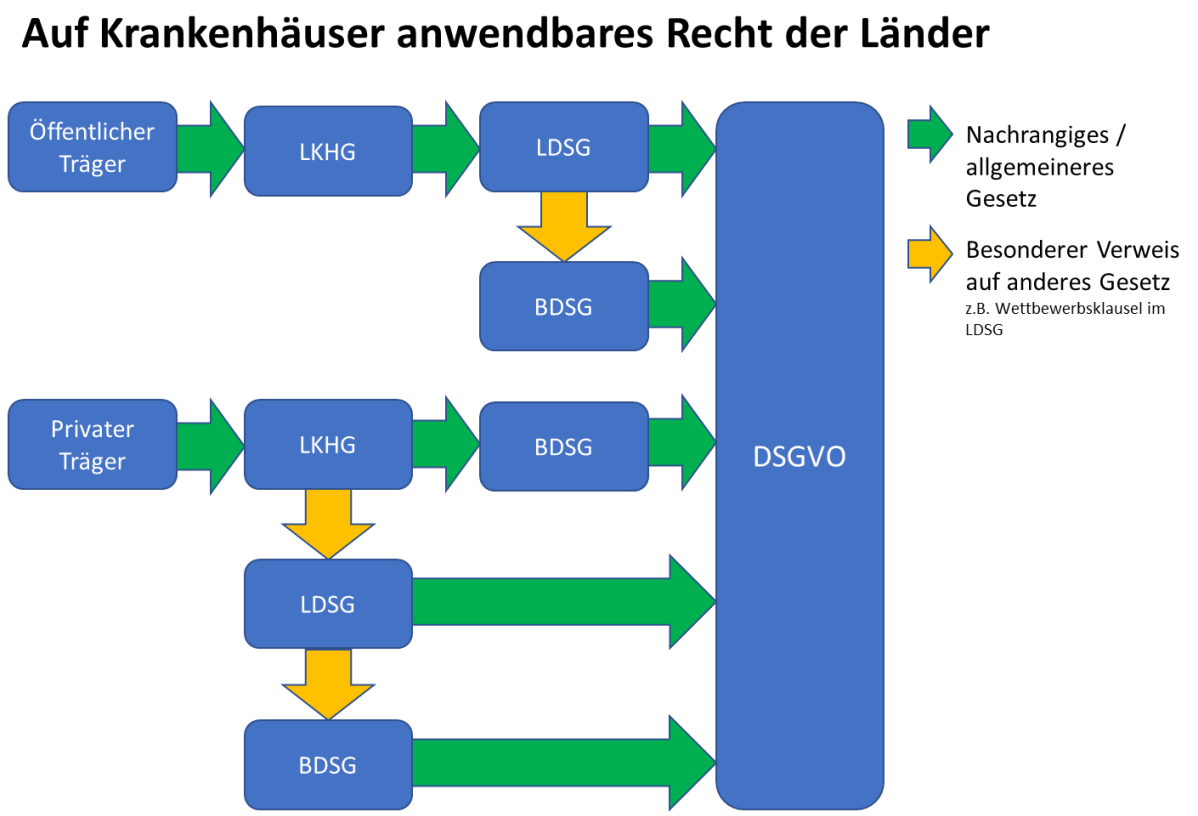

Abb. 3-1*: Prüfungsreihenfolge zum auf Klinken anwendbaren Datenschutzrecht*

Diese Struktur und Prüfungsreihenfolge veranschaulicht auch das Vorgehen im ersten Block zum jeweiligen Bundesland, nämlich dem zum auf Krankenhäusern anwendbaren Datenschutzrecht. Basierend hierauf wird dann in einem zweiten Block untersucht, welche Regelungen zur Auftragsverarbeitung für (welche) Krankenhäuser im jeweiligen Bundesland gelten, bevor in einem dritten Block auf datenschutzrechtliche Vorgaben zu technischen und organisatorischen Maßnahmen nach Landesrecht eingegangen wird.

3.4.1 Baden-Württemberg

Auf Krankenhäuser anwendbare Datenschutzvorschriften[168]

Das LKHG BW ist gemäß dessen § 2 Abs. 1 S. 1 auf alle Krankenhäuser anwendbar, die nach dem Krankenhausfinanzierungsgesetz des Bundes (KHG)[169] öffentlich gefördert werden. Für Universitätsklinken gelten Besonderheiten,[170] jedoch findet nach § 2 Abs. 2 LKHG BW unter anderem der Datenschutz-Abschnitt dieses Gesetzes auch auf sie Anwendung. Die Datenschutzregeln im 7. Abschnitt des LKHG BW sind nach § 43 Abs. 1 LKHG BW auf Krankenhäuser

[168] Zum auf Kliniken in Baden-Württemberg anwendbaren Datenschutzrecht mit Stand Mai 2014 vgl. Schneider, Sekundärnutzung klinischer Daten, S. 123 ff.

[169] Krankenhausfinanzierungsgesetz in der Fassung der Bekanntmachung vom 10. April 1991 (BGBl. I S. 886), das zuletzt durch Artikel 1 des Gesetzes vom 23. Oktober 2020 (BGBl. I S. 2208) geändert worden ist.

[170] Vorrangig gilt für diese das Universitätsklinika-Gesetz (UKG) BW in der Fassung vom 15. September 2005, zuletzt geändert durch Artikel 26 der Verordnung vom 23. Februar 2017 (GBl. S. 99, 102). Das UKG enthält aber keine Datenschutzregeln.

i.S.v. § 107 Abs. 1 SGB V sowie entsprechend auf Vorsorge- und Rehabilitationseinrichtungen nach § 107 Abs. 2 SGB V anzuwenden.[171]

In § 107 SGB V sind Krankenhäuser sowie Vorsorge- und Rehabilitationseinrichtungen („Reha-Krankenhäuser") entsprechend ihrer umgangssprachlichen Wortbedeutung weit definiert. Damit fallen zunächst alle Arten von Krankenhäusern, unabhängig von ihrer Trägerschaft (sei sie öffentlich, kirchlich oder privat), von Zulassungsstatus und öffentlicher Förderung, in den Geltungsbereich der genannten Datenschutzregelungen. Klarstellend ausgenommen werden aber Krankenhäuser sowie Vorsorge- oder Rehabilitationseinrichtungen, deren Träger der Bund ist (§ 43 Abs. 1 S. 3 LKHG BW).

In den Bereichen, in denen das LKHG keine besonderen Vorschriften zum Datenschutz enthält, bleibt es bei den „subsidiären" (nachrangigen) Regeln, auf welche § 43 Abs. 5 LKHG BW abstrakt und dynamisch mit folgenden Worten verweist: „Soweit sich aus diesem Gesetz nichts anderes ergibt, sind auf Patientendaten die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden." Welche Vorschriften dies jeweils sind, wird im Folgenden geklärt.

Öffnungsklausel der DSGVO

Die DSGVO enthält viele Öffnungsklauseln, in deren Rahmen die EU-Mitgliedstaaten eigene Regelungen erlassen können (fakultative Öffnungsklauseln) und teils auch müssen (obligatorische Öffnungsklauseln). Letzteres ist beispielsweise dahingehend der Fall, dass die Mitgliedstaaten die zuständigen Datenschutzaufsichtsbehörden zu bestimmen haben (Art. 51, 54 DSGVO). Auch fakultative Öffnungsklauseln finden sich an einigen Stellen. Gerade für die Verarbeitung von Gesundheitsdaten, zu denen auch die Patientendaten von Krankenhäusern gehören, enthält Art. 9 Abs. 4 DSGVO eine denkbar weite Öffnungsklausel. Für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten können die Mitgliedstaaten demnach „zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten". In den übrigen Absätzen des Art. 9 DSGVO werden zwar primär Rechtsgrundlagen für die Verarbeitung besonderer Kategorien personenbezogener Daten, wie eben von Gesundheitsdaten, festgelegt. Die Festlegung zusätzlicher mitgliedstaatlicher Rechtsgrundlagen für die Verarbeitung oder die Einschränkung unionsrechtlicher Grundlagen aus der DSGVO ist für sich genommen schon eine großzügige Öffnung. Zudem wird man aufgrund der weiten Formulierung des Art. 9 Abs. 4 DSGVO davon ausgehen können, dass die Mitgliedstaaten hier weitere Rahmenbedingungen, wie z. B. besondere technische und organisatorische Schutzmaßnahmen festlegen können, auch für die Auftragsverarbeitung, welche typisch für den Betrieb von KIS in der Cloud ist.

[171] Der allgemeine Anwendungsbereich ist nach § 2 Abs. 1 LKHG BW zwar enger: Erfasst sind grds. nur Krankenhäuser, die nach dem KHG öffentlich gefördert werden. Nach § 2 Abs. 4 LKHG BW bleiben allerdings „Vorschriften dieses Gesetzes, die sich ausdrücklich auf andere Krankenhäuser oder auf Vorsorge- oder Rehabilitationseinrichtungen beziehen" unberührt. Die Vorschriften zum Datenschutz in den §§ 43 ff. LKHG BW gelten damit auch für Krankenhäuser, die im Übrigen nicht in den Anwendungsbereich des Gesetzes fallen. Für Universitätsklinika wird die Geltung der Datenschutzvorschriften des 7. Abschnitts in § 2 Abs. 2 LKHG BW explizit klargestellt, weil das Gesetz ansonsten nur partiell auf diese Anwendung findet.

Innerhalb des durch die Öffnungsklauseln der DSGVO gesetzten Rahmen genießen die nationalen Regelungen Vorrang vor denen der DSGVO, weil letztere sich selbst insoweit zurücknimmt. Das heißt nicht, dass die DSGVO überhaupt nicht mehr zur Anwendung kommen würde, da diese Klauseln meist nur eine begrenzte Reichweite haben und auch die weite Öffnung bei Gesundheitsdaten nach Art. 9 Abs. 4 DSGVO in Deutschland nicht zu einer abschließenden, die DSGVO komplett ausschließenden Regelung genutzt wurde.[172] Außerhalb des Anwendungsbereiches der Öffnungsklauseln verbleibt es beim Anwendungsvorrang der DSGVO und auch soweit eine Öffnungsklausel greift, diese aber nicht (vollständig) genutzt wird, verbleibt es nachrangig bei der unmittelbaren Geltung der DSGVO.

Innerhalb der Anwendung der weiten Öffnungsklausel für Gesundheitsdaten sind aber vorrangig Rechtsvorschriften der Mitgliedstaaten auf ihre Anwendbarkeit zu prüfen. Wer diese Vorschriften innerhalb der Mitgliedstaaten erlassen (oder aufrechterhalten) darf, richtet sich nach der innerstaatlichen Kompetenzverteilung. Für den Patientendatenschutz in Krankenhäusern sind dies nach herrschender Meinung in Deutschland, jedenfalls außerhalb der besonderen Leistungsbeziehungen (Abrechnung, spezielle Qualitätssicherungsverfahren) zur GKV, die Bundesländer. Diese haben in ihren LKHG zumeist entsprechende Regelungen mit dem kraft Kompetenzordnung und Spezialität höchsten Vorrang geschaffen. Im Übrigen ist im Anwendungsbereich der Öffnungsklauseln, wiederum v.a. der nach Art. 9 Abs. 4 DSGVO für Gesundheitsdaten, die subsidiäre Anwendung der jeweiligen LDSG oder des BDSG zu prüfen. In diesen allgemeinen Datenschutzgesetzen wird zwar nur zum Teil auf Gesundheitsdaten Bezug genommen, aber sie werden in den LKHG teil für subsidiär auch auf Patientendaten anwendbar erklärt. Neben der subsidiären Anwendung dieser nationalen Regelungen (sei es auf Bundes- oder Landesebene) kommt auch die direkte Anwendung der DSGVO außerhalb der Öffnungsklauseln oder innerhalb dieser Klauseln deren subsidiäre Anwendung auf unterster Rangebene in Betracht. Bei der Frage insbesondere nach der nachrangigen Anwendung von LDSG BW oder BDSG kann auch die Frage relevant werden, ob es sich um öffentliche oder private Krankenhäuser handelt.

Krankenhäuser öffentlicher Träger

Auf öffentliche Krankenhäuser in Baden-Württemberg findet wie auf alle Krankenhäuser zunächst mit Vorrang das LKHG BW Anwendung.

Gilt subsidiär das LDSG oder das BDSG?

Nachrangig gilt für diese als öffentliche Stellen des Landes Baden-Württemberg zunächst das LDSG BW (§ 2 Abs. 3 S. 1 LDSG BW und § 43 Abs. 5 LKHG BW).

Dabei bleibt es für als Eigenbetriebe der öffentlichen Hand geführte Kliniken, welche also unmittelbar einer Behörde oder sonstigen Stelle des Landes, einer Gemeinde, einem Gemeindeverband oder einer sonstigen unter der Aufsicht des Landes stehenden juristischen Person des

[172] Dies gilt trotz der recht weitreichenden Nutzung dieser Öffnungsklausel in Deutschland. Offen gelassen werden soll an dieser Stelle, ob diese Klausel überhaupt eine abschließende Regelung durch mitgliedstaatliches Recht zulassen würde oder ob dies selbst für diese Art der Öffnung zu weit wäre.

öffentlichen Rechts (öffentliche Stellen) zugeordnet sind und über keine juristische Selbständigkeit (eigene Rechtspersönlichkeit)[173] verfügen. Dabei ist die öffentliche Stelle zugleich Verantwortlicher nach Art. 4 Nr. 7 DSGVO (§ 2 Abs. 1 LDSG BW).

Gemäß § 2 Abs. 2 LDSG BW ist dieses Gesetz auch auf juristische Personen des privaten Rechts und sonstige Vereinigungen des privaten Rechts anwendbar, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine juristische Person des öffentlichen Rechts nach § 2 Abs. 1 LDSG BW mit absoluter Mehrheit beteiligt ist.

Hält die öffentliche Hand nicht die absolute Mehrheit oder wird keine Aufgabe der öffentlichen Verwaltung wahrgenommen, handelt es sich ohnehin nicht um eine öffentliche Stelle i. S. d. § 2 Abs. 1 S. 1 LDSG BW, so dass dieses Gesetz nicht zur Anwendung kommt. Es handelt sich dann um eine nicht-öffentliche Stelle gemäß § 2 Abs. 4 S. 1 BDSG. Auf diese ist über den Verweis in § 43 Abs. 5 LKHG BW – soweit die DSGVO nicht (aufgrund der Nutzung von Öffnungsklauseln) unmittelbar anwendbar ist (§ 1 Abs. 5 BDSG) – das BDSG nach § 1 Abs. 1 S. 2 BDSG anwendbar. Das BDSG gilt damit in solchen Krankenhäusern dann subsidiär, wenn die DSGVO aufgrund der Nutzung von Öffnungsklauseln nicht unmittelbar anwendbar ist.

Soweit öffentliche Stellen und damit auch öffentliche Kliniken als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, verweist § 2 Abs. 6 S. 1 LDSG BW auf die für nicht-öffentliche Stellen geltenden Vorschriften, also im Anwendungsbereich von Öffnungsklauseln jene des BDSG und im Übrigen die der DSGVO. Lediglich für Zweckverbände, welche im Krankenhausbereich aber praktisch keine Rolle spielen, gilt dieser Verweis nach § 2 Abs. 6 S. 2 LDSG BW nicht.

Bei einer privaten Rechtsform gilt der Verweis in § 2 Abs. 6 LDSG BW jedoch nur, wenn die öffentliche Hand die Mehrheit hält und man annimmt, dass Krankenhäuser gemäß § 2 Abs. 5 LDSG BW Aufgaben der öffentlichen Verwaltung wahrnehmen. Wollte man die Wahrnehmung von Aufgaben der öffentlichen Verwaltung durch Krankenhäuser verneinen, käme man für Kliniken in privater Rechtsform, aber im (Teil-)Eigentum öffentlicher Träger – unabhängig von den Mehrheitsverhältnissen – über den Verweis in § 43 Abs. 5 LKHG unmittelbar zur Anwendung der Vorschriften des BDSG, da in diesem Fall das LDSG BW nicht anwendbar ist, weil die Klinik dann keine öffentliche Stelle i. S .d. § 2 Abs. 1 und 2 LDSG wäre und eine nicht-öffentliche Stelle nach § 2 Abs. 4 BDSG vorläge.

Die Krankenhausversorgung kann jedoch im Sinn der Daseinsvorsorge auch als Aufgabe der öffentlichen Verwaltung wahrgenommen werden. Dies ist der Fall, wenn ein Krankenhaus in öffentlicher Trägerschaft steht oder ein privater Krankenhausträger mit Aufgaben der öffentlichen Verwaltung „beliehen" würde. Für Letzteres genügt die Aufnahme in den Landeskrankenhausplan jedoch nicht. In aller Regel findet auch keine solche Beleihung im Krankenhausbereich statt, da es sich bei der Krankenhausversorgung in öffentlicher Hand üblicherweise um Leistungsverwaltung, nicht aber um hoheitliche Eingriffsverwaltung handelt, und nur bei letzterer

[173] Eine eigne Rechtspersönlichkeit läge z.B. bei einer Anstalt, Körperschaft oder Stiftung öffentlichen Rechts oder einer der Gesellschaftsformen (z.B. GmbH oder AG) des privaten Rechts vor. Eigen- bzw. Regiebetriebe sind dagegen rechtlich unselbständige organisatorische Einheiten einer übergeordneten juristischen Person der öffentlichen Verwaltung, welche direkten Durchgriff auf den Betrieb und seine Leitung hat.

eine Beleihung in Betracht kommt.[174] Eine Trägerschaft des Staates findet sich jedoch häufig und führt – bei entsprechenden Mehrheitsverhältnissen – zur Einordnung als öffentliche Stelle nach § 2 Abs. 1, 2 LDSG.

Trotz der Einordnung der Krankenhausversorgung als Daseinsvorsorge und damit grundsätzlich zulässiges Tätigkeitsfeld der öffentlichen (Leistungs-)Verwaltung wird man nicht bestreiten können, dass diese Tätigkeit in (teils sogar zunehmendem) Wettbewerb mit anderen Krankenhausträgern wie insbesondere erwerbswirtschaftlichen Unternehmen erfolgt. Ob und gegebenenfalls inwieweit sich dieser Wettbewerb um die Behandlung von Patienten und damit im Rahmen des primären Nutzungszwecks der Daten sich bei der Sekundärnutzung von Patientendaten zu anderen Zwecken wie Qualitätssicherung oder Forschung fortsetzt und auch für diese Verarbeitungszwecke zur subsidiären Anwendung des BDSG führt, bedarf vorliegend keiner Entscheidung. Denn ein KIS dient primär der (administrativen und medizinischen) Abbildung und Steuerung der Behandlung der Patienten und muss zuallererst vor diesem Hintergrund gerechtfertigt werden.

Damit nehmen jedenfalls Krankenhäuser öffentlicher Träger in privater Rechtsform als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teil, weshalb für diese nach § 2 Abs. 6 LDSG BW die für nicht-öffentliche Stellen geltenden Vorschriften des BDSG (subsidiär) Anwendung finden.

Zu prüfen bleibt, ob von einer entsprechenden Teilnahme als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb auch ausgegangen werden kann, wenn das Krankenhaus mit einer eigenen, aber öffentlich-rechtlich ausgestalteten Rechtspersönlichkeit ausgestattet ist, insbesondere also, wenn es als eigenständige Anstalt oder Stiftung des öffentlichen Rechts verfasst ist. Insoweit ist zweifelhaft, ob man noch von einem Unternehmen sprechen kann. Als Wettbewerbsunternehmen gelten aber sowohl die öffentlich-rechtlichen als auch die privatrechtlichen Unternehmen mit Ausnahme der Zweckverbände.[175] Dies lässt sich auch mit einem Umkehrschluss zur Ausnahme der Zweckverbände begründen: Wären öffentlich-rechtliche Rechtsformen von vornherein nicht als Unternehmen anzusehen, bräuchten (öffentlich-rechtliche) Zweckverbände nicht – wie in § 2 Abs. 6 S. 2 LDSG BW geschehen – gesondert aus der Regelung ausgenommen zu werden.

Ergebnis: Für alle öffentlich geführten Kliniken gilt damit vorrangig das LKHG BW. Für als Eigenbetriebe geführte Kliniken der öffentlichen Hand gilt nachrangig das LDSG BW sowie außerhalb der Öffnungsklauseln die DSGVO direkt. Für Kliniken öffentlicher Träger mit eigener Rechtspersönlichkeit gilt nachrangig das BDSG und außerhalb der Öffnungsklauseln die DSGVO direkt.

Krankenhäuser privater Träger

Die Ausführungen zur Anwendung des LKHG BW auf öffentliche Kliniken sind auf Kliniken privater Träger übertragbar. Der allgemeine Anwendungsbereich des LKHG BW ist zwar nach § 2

[174] Abweichungen von dieser Regel können für die ausnahmsweise zulässige Zwangsbehandlung im Rahmen der Unterbringung psychisch Kranker oder des Maßregelvollzuges gelten, welche aber üblicherweise auf spezielle Kliniken konzentriert ist, die hier ausgeklammert werden.

[175] Bergmann/Möhrle/Herb, LDSG BW, § 2 Abschnitt 6.

Abs. 1 S. 1 LKHG BW auf Kliniken beschränkt, die nach dem KHG gefördert werden, worunter nicht alle Kliniken privater Träger fallen. Darauf kommt es jedoch vorliegend jedoch nicht an, weil der spezifische Anwendungsbereich des Datenschutz-Abschnitts des LKHG BW gemäß § 43 Abs. 1 LKHG BW auf Krankenhäuser im Sinne des § 107 Abs. 1 SGB V bezogen ist. Darunter fallen auch Kliniken privater Träger.[176]

Gilt subsidiär das LDSG oder das BDSG?

Nachrangig zum LKHG sind die jeweils geltenden Vorschriften anwendbar (§ 43 Abs. 5 LKHG BW). Bei Klinken privater Träger handelt es sich um nicht-öffentliche Stellen nach § 2 Abs. 4 S. 1 BDSG. Auf sie sind daher subsidiär die DSGVO – soweit sie unmittelbar anwendbar ist (§ 1 Abs. 5 BDSG) – und im Übrigen die sonst einschlägigen Vorschriften des BDSG anwendbar. Das LDSG ist auch nicht nachrangig anwendbar, weil eine Klinik privater Träger keine öffentliche Stelle i. S. d. § 2 Abs. 1 und 2 LDSG BW ist.

Ergebnis: Für den Schutz von Patientendaten in Kliniken privater Träger gelten in Baden-Württemberg folgende Rechtsvorschriften in absteigender Rangfolge: 1. das LKHG BW, 2. das BDSG und 3. die DSGVO.[177]

Öffnungsklausel für kirchliche Träger?

Die Vorschriften des Datenschutz-Abschnitts gelten grundsätzlich unabhängig von ihrer Rechtsform auch für Krankenhäuser, die von Religionsgemeinschaften oder diesen zuzuordnenden Einrichtungen betrieben werden. Dies gilt allerdings nur, soweit die Religionsgemeinschaften bis zum 01.01.2008 im Einzelnen keine gleichwertigen Regelungen zum Schutz personenbezogener Daten getroffen haben (§ 43 Abs. 2 S. 1 LKHG BW).[178]

Jedoch bliebe auch im zuletzt genannten Fall die Anwendung von § 49 LKHG BW unberührt (§ 43 Abs. 2 S. 2 LKHG BW), wonach es kein unbefugtes Offenbaren i.S.v. besonderen gesetzlichen Geheimhaltungspflichten darstellt, wenn Patientendaten unter den Voraussetzungen der §§ 45 bis 48 LKHG BW weitergegeben werden. Dies ist insbesondere vor dem Hintergrund der nach § 203 Abs. 1 Nr. 1 StGB statuierten und sanktionierten ärztlichen Schweigepflicht zu sehen. Diese stellt auch für Religionsgemeinschaften zwingendes staatliches Recht dar. Die Schweigepflicht kann als eigenständige Schranke im Gegensatz zum Datenschutzrecht (i.e.S.) nur durch staatliches, nicht aber durch kirchliches Recht befugt durchbrochen werden. Jedenfalls hat der baden-württembergischen Gesetzgeber eine entsprechende Wertung getroffen. Von Verfassungs wegen – weil die kirchliche Selbstbestimmung nicht die für alle Schweigeverpflichteten geltende allgemeine bundesrechtliche Schranke des § 203 StGB suspendieren kann – gilt dies aber wohl auch über Baden-Württemberg hinaus.[179] Deshalb sind auch für Krankenhäuser in kirchlicher Trägerschaft insoweit die §§ 45 bis 48 LKHG maßgeblich. Diese Schweigepflicht-fokussierte entsprechende Anwendung des staatlichen Datenschutzrechts entbindet

[176] Vgl. dazu oben bei öffentlichen Kliniken die Ausführungen zu § 107 SGB V, S. 78.

[177] Europarechtskonforme Nutzung der in der DSGVO bestehenden Öffnungsklauseln jeweils vorausgesetzt.

[178] Dies stellt eine der weiter unten (Kap. 3.5.1, S. 164 f.) etwas eingehender bewerteten Öffnungsklauseln im staatlichen Recht zu Gunsten abweichender kirchlicher Regelungen dar.

[179] Insbesondere zu letzterem Punkt: Beyerle, Rechtsfragen medizinischer Qualitätskontrolle, S. 132 f.

die Krankenhäuser der Kirchen allerdings nicht davon, ihr gegebenenfalls ebenfalls einschlägiges kirchliches Datenschutzrecht parallel anzuwenden. Damit erhöhen sich insgesamt die Hürden für eine Übermittlung bzw. ein Offenbaren patientenbezogener Daten, da die jeweils strengste Regelung eingehalten werden muss.

Zusammenfassung

Für alle Kliniken in Baden-Württemberg, mit Ausnahme solcher, die dem Bund zugeordnet sind, gilt vorrangig das LKHG BW. Für öffentliche Kliniken als Eigenbetriebe gilt nachrangig das LDSG BW. Für öffentliche Kliniken mit eigener Rechtspersönlichkeit und Kliniken in privater Trägerschaft gilt – soweit sie unmittelbar anwendbar ist – die DSGVO, ansonsten – im Rahmen von Öffnungsklauseln – das BDSG. Innerhalb des LKHG BW besteht zudem eine Öffnungsklausel für kirchliche Krankenhäuser, für welche von den öffentlich-rechtlichen Religionsgemeinschaften in den Grenzen der DSGVO eigene Datenschutzregeln erlassen werden dürften.

Vorschriften zur Auftragsverarbeitung[180]

Geltende Regelung in § 48 LKHG BW: andere Krankenhäuser oder Rechenzentren

Für alle Krankenhäuser in Baden-Württemberg, mit Ausnahme solcher des Bundes,[181] regelt § 48 LKHG BW die Verarbeitung von Patientendaten im Auftrag eines der genannten Krankenhäuser. Nach § 48 Abs. 1 LKHG BW sind Patientendaten grundsätzlich im Krankenhaus selbst oder durch ein anderes Krankenhaus zu verarbeiten.

Durch ein Rechenzentrum im Auftrag eines Krankenhauses dürfen Patientendaten gemäß § 48 Abs. 2 LKHG BW nur automatisiert verarbeitet werden, wenn

1) die für Auftraggeber und Auftragnehmer zuständige Datenschutzaufsichtsbehörde hiervon benachrichtigt wird,
2) der Auftragnehmer seinen Mitarbeitern, soweit ihnen aus zwingenden Gründen eine Zugriffsberechtigung auf Patientendaten eingeräumt wird, eine § 203 StGB entsprechende Schweigepflicht auferlegt und
3) die nach dem Bundesdatenschutzgesetz oder dem Landesdatenschutzgesetz für die Verarbeitung von personenbezogenen Daten im Auftrag erforderlichen technischen und organisatorischen Maßnahmen schriftlich festgelegt werden.

Verhältnis von Rechenzentrum und Auftragsverarbeiter

Fraglich ist, inwieweit sich der Begriff des „Rechenzentrums" von dem Begriff des „Auftragsverarbeiters" unterscheidet. Bei der Einführung des § 48 Abs. 2 LKHG BW am 12.12.1991 verwendete der Gesetzgeber noch den Begriff „eine andere Stelle".[182] Die Einführung wurde damit begründet, dass § 48 Abs. 2 LKHG BW eine Ausnahme vom Grundsatz des § 48 Abs. 1 LKHG BW sei. Diese Ausnahme sei für die Verarbeitung in automatisierten Verfahren durch Rechenzentren von Bedeutung, derer sich die Krankenhäuser schon seit langem bedienen würden. Sie

[180] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 267 ff.

[181] Wie das Bundeswehrkrankenhaus Ulm.

[182] Landeskrankenhausgesetz Baden-Württemberg (LKHG) vom 15. Dezember 1986 in der Gültigkeit vom 01.01.1992 bis 31.08.1993, geändert durch das Gesetz vom 12.12.1991.

umfasse Stellen bzw. Rechenzentren, die Patientendaten in wirtschaftlicher und einer den Belangen des Datenschutzes gerecht werdenden Weise im Auftrag des Krankenhauses verarbeiten.[183] Erst durch eine Änderung des Gesetzes im Jahr 2000 wurde der Begriff des „Rechenzentrums" in das LKHG BW eingeführt.[184] Der Gesetzgeber begründete dies damit, dass durch den alten und weiteren Begriff der „anderen Stelle" grundsätzlich alle Arten von Auftragsverarbeitern umfasst werden konnten, was zur Folge hatte, dass Krankenhäuser beispielsweise die Korrespondenz der Ärzte über externe Schreibbüros abwickeln ließen, ohne die Einwilligung der Patienten einzuholen. Schutzvorschriften wie § 203 StGB und der strafprozessuale Beschlagnahmeschutz wären hierdurch nach Ansicht des Landesgesetzgebers in einer unzulässigen Weise unterlaufen worden. Diese Vorschrift habe bei ihrer Einführung ausschließlich die Datenverarbeitung in automatisierten Verfahren durch Rechenzentren im Auge gehabt, was durch den bisherigen Anwendungsbereich nicht präzise zum Ausdruck gekommen sei.[185]

Verhältnis von Rechenzentrum und Cloud-Anbieter

Grundsätzlich beruhen alle Cloud-Dienste auf Leistungen von Rechenzentren, da eine entsprechende IT-Infrastruktur notwendig ist, um sie überhaupt anbieten zu können. Fraglich ist, ob die auf dieser Infrastruktur des Rechenzentrums aufbauenden Plattformen und Software als vom Rechenzentrum angeboten gelten und somit auch unter den Begriff des Rechenzentrums des § 48 Abs. 2 LKHG BW fallen. Ist der Betreiber des Rechenzentrums zugleich auch Anbieter der Plattformen und Software, so gelten diese als vom Rechenzentrum angeboten und unterfallen dem Begriff. Werden von einem Betreiber mehrere Rechenzentren gleichzeitig betrieben – was bei Cloud-Diensten typischerweise der Fall ist – erscheint dies ebenfalls unproblematisch. Solange dieser Anbieter alle diese Rechenzentren betreibt oder anmietet, um diese dann als skalierbares Paket aus Rechen- und Speicherleistung an Krankenhäuser zu vertreiben, wird man wohl auch diesen Anbieter als Rechenzentrum bezeichnen können, da § 48 Abs. 2 LKHG BW sich wohl nicht nur auf ein dediziertes Rechenzentrum bezieht. Auch in der Gesetzesbegründung wird in der Mehrzahl von Rechenzentren gesprochen, was zwar nicht zwingend, aber doch eher gegen das Erfordernis eines dedizierten Rechenzentrums pro Krankenhaus spricht.

Wenn lediglich ein bestimmtes Rechenzentrum beauftragt wird und die Patientendaten nur in diesem Rechenzentrum verarbeitet werden, hat dies zwar Vorteile im Hinblick auf eine transparente Lokalisierung dieser Verarbeitung und damit auch die Kontrolle und Durchsetzung der Einhaltung rechtlicher Anforderungen. Auch bei der Beauftragung von Cloud-Dienstleistern können jedoch Lokalisierungsvorgaben gemacht werden, die eine Kontrolle und Durchsetzung unter einer oder mehreren bestimmten Jurisdiktionen sicherstellen können. Die Lokalisierung ist hier wegen der Virtualisierung der Verarbeitung bzw. deren Verteilung auf eine Mehrzahl von verteilten und oft auch entfernten physischen Ressourcen nicht so eng begrenzt und transparent, aber doch auch kontrollierbar. Vor diesem Hintergrund besteht auch nach Sinn und Zweck der Regelung kein zwingender Grund, die Beauftragung von Cloud-Anbietern generell auszuschließen.

[183] Landtag von Baden-Württemberg, Drucksache 10/5620 vom 23. Juli 1991, S. 21.

[184] Landeskrankenhausgesetz Baden-Württemberg (LKHG) vom 15. Dezember 1986 in der Gültigkeit vom 10.06.2000 bis 28.02.2005, geändert durch das Gesetz vom 23.05.2000.

[185] Landtag von Baden-Württemberg, Drucksache 12/4899 vom 22. Februar 2000, S. 49.

Anders könnte es jedoch sein, wenn der Betreiber des Rechenzentrums nicht zugleich der Anbieter der Plattform oder der Software ist. Kauft der Anbieter der Software oder der Plattform von einem Betreiber eines Rechenzentrums dessen Rechen- und Speicherleistung zu, um diese dann an Krankenhäuser weiterzuverkaufen, besteht aus Sicht des Krankenhauses jedoch kein wesentlicher Unterschied, ob der Anbieter auch Betreiber des Rechenzentrums ist oder lediglich die Rechen- und Speicherleistung des Rechenzentrums eines anderen Betreibers mit umfasst. Der Anbieter bietet wie in den obigen Beispielen die automatisierten Verfahren wie jedes andere Rechenzentrum an. Lediglich im Innenverhältnis von Anbieter der Software und dem Betreiber des Rechenzentrums besteht ein Unterschied. Der Anbieter unterfällt somit in einer solchen Konstellation wohl dem Begriff des Rechenzentrums.

Mietet das Krankenhaus hingegen eigenständig die Infrastruktur eines Rechenzentrums und beschafft von einem anderen Anbieter ein KIS, um es selbst im Rechenzentrum zu betreiben, könnte der KIS-Anbieter u.U. nicht als Rechenzentrum im Sinne des § 48 Abs. 2 LKHG BW zu sehen sein. Soweit dieser Anbieter auch keine Möglichkeit des Zugriffs auf patientenbezogene Daten hätte, würde dies allerdings kein Problem darstellen, da dann auch kein Outsourcing bzw. keine erlaubnispflichtige Auftragsverarbeitung vorläge. Nur hinsichtlich einer möglichen Fernwartung könnten sich Probleme ergeben, wenn der Anbieter im Zuge dieser Zugriff auf die personenbezogenen Daten erhalten könnte. Eine Regelung zur Fernwartung, also zum Fernzugriff auf eine (On Premises-)Installation zu Wartungszwecken, existiert im LKHG BW leider nicht, sodass die Frage geklärt werden müsste, inwieweit diese Fernwartung eine Auftragsverarbeitung darstellt (wofür bei der Möglichkeit des Zugriffs auf patientenbezogene Daten vieles spricht) und auf § 48 Abs. 2 LKHG BW gestützt werden kann. Dies sind aber alles Fragen, die nicht den Einsatz von KIS-as-a-Service betreffen, da hier die Wartung durch den Anbieter auf dessen eigenen Systemen mit übernommen wird.[186]

Technische und organisatorischen Sicherheitsmaßnahmen

§ 48 Abs. 2 Nr. 3 Halbsatz 2 LKHG BW stellt im Übrigen klar, dass die Vorschrift des § 3a Landesverwaltungsverfahrensgesetz (LVwVfG) BW über die elektronische Kommunikation mit Behörden keine Anwendung findet. Insoweit gelten also für Krankenhäuser die allgemeinen Maßgaben von Datenschutz und Datensicherheit, nach denen die elektronische Kommunikation aber ähnlich wie in § 3a LVwVfG BW zwischen den Kommunikationspartnern auch gesondert eröffnet oder vereinbart werden muss. Bei Kommunikation über offene Netze sind ebenso eine Authentifizierung der Kommunikationspartner (wenn auch nicht zwingend durch qualifizierte elektronische Signaturen wie in § 3a Abs. 2 LVwVfG BW vorgesehen) und eine starke Verschlüsselung vorgeschrieben. Dies ergibt sich schon aus dem Verweis in § 48 Abs. 2 Nr. 3 Halbsatz 1 LKHG BW auf die nach dem BDSG oder dem LDSG erforderlichen technischen und organisatorischen Maßnahmen der Datensicherheit. In den alten Fassungen dieser Gesetze war dies in den § 9 LDSG BW a.F. und § 9 BDSG a.F. geregelt. Eine eigene Regelung der erforderlichen technischen und organisatorischen Maßnahmen für die Verarbeitung von personenbezogenen

[186] Im technischen Sinne findet hier auch häufig eine Fernwartung insofern statt, als dass die Mitarbeiter des Cloud-Anbieters jedenfalls für die Wartung bzw. Pflege der Software i.d.R. nicht direkt vor den Servern im Rechenzentrum sitzen, sondern sich von ihrer normalen Büroumgebung aus der Ferne bzw. „remote" auf die realen oder virtuellen Server aufschalten. Dabei handelt es sich aber nicht um eine Fernwartung im hier verwandten spezifisch datenschutzrechtlichen Sinne.

Daten im Auftrag ist in der jeweiligen Neufassung nicht mehr enthalten. Allerdings lassen sich Regelungen zu technischen und organisatorischen Sicherheitsmaßnahmen in § 22 BDSG und § 3 LDSG BW finden. Die Regelung in § 22 BDSG bezieht sich auf die Verarbeitung besonderer Kategorien personenbezogener Daten allgemein und nicht speziell auf die Verarbeitung im Auftrag. Sie ist gleichwohl anwendbar, da vorliegend bei der Verarbeitung im Auftrag auch eine Verarbeitung von Gesundheitsdaten vorgenommen wird, welche eine der genannten besonderen Kategorien darstellen. Die Regelung in § 3 LDSG BW gilt allgemein für die Verarbeitung jeglicher personenbezogenen Daten und konkretisiert insoweit Art. 32 DSGVO exemplarisch.

Benachrichtigung der Datenschutzaufsichtsbehörden

Die gemäß § 48 Abs. 2 Nr. 1 LKHG BW zu benachrichtigenden Datenschutzaufsichtsbehörden ergeben sich für die dem LKHG BW unterworfenen Krankenhäuser aus der Übersicht zum anwendbaren Datenschutzrecht sowie zur zuständigen Datenschutzaufsicht. Für die eingeschalteten Rechenzentren ist deren zuständige Aufsichtsbehörde im Einzelfall zu prüfen. Bei Rechenzentren der öffentlichen Hand wird sich in der Regel die gleiche Aufsichtsbehörde wie bei öffentlichen Krankenhäusern, bei privaten Rechenzentren regelmäßig die gleiche wie bei Privatkliniken am jeweiligen Sitz ergeben.[187] Weil primär das Krankenhaus als Auftraggeber für die Einhaltung von § 48 LKHG BW verantwortlich ist, sollte sich dieses auch von der Benachrichtigung der für den Auftragnehmer, also das Rechenzentrum zuständigen Datenschutzaufsichtsbehörde überzeugen. Das gilt selbst dann, wenn diese Benachrichtigung vom Auftragnehmer ausgeht. Das Krankenhaus sollte in diesem Fall den Auftragnehmer hierauf vertraglich verpflichten und sich möglichst auch eine Kopie der Benachrichtigung vorlegen lassen. Die eigene Datenschutzaufsichtsbehörde muss das Krankenhaus natürlich selbst benachrichtigen.

Verpflichtung entsprechend § 203 StGB

Aus § 48 Abs. 2 Nr. 2 LKHG BW ergibt sich zunächst, dass der Auftragnehmer seinen Mitarbeitern nur aus zwingenden Gründen, also soweit unbedingt erforderlich, Zugriffsrechte auf Patientendaten einräumen darf. Zudem muss der Auftragnehmer seinen Mitarbeitern dann eine § 203 StGB entsprechende Schweigepflicht auferlegen. Ursprünglich bestanden insoweit offene Fragen, als dass eine solche, jedenfalls bei privaten Krankenhäusern rein rechtsgeschäftliche Schweigeverpflichtung keine § 203 StGB entsprechenden strafrechtlichen Wirkungen entfalten konnte.[188] Diese Problematik wurde durch die Reform des § 203 StGB behoben, der nun eine Schweigeverpflichtung sonstiger mitwirkender Personen mit strafrechtlichen Wirkungen vorsieht, welche auch den Anforderungen des § 48 Abs. 2 Nr. 2 LKHG BW genügt.

Zuletzt stellt § 48 Abs. 3 LKHG BW fest, dass sich die Patientendaten im ausschließlichen Gewahrsam des Krankenhauses befinden, in dessen Auftrag sie verarbeitet werden. Diese Fiktion soll ein Beschlagnahmeverbot nach § 97 StPO begründen, das nach § 97 Abs. 2 S. 1 StPO grund-

[187] Auch insoweit hat also Tabelle 3-1 zum auf Krankenhäuser anwendbaren Datenschutzrecht nach Bundesland und Trägerschaft mit den dortigen Angaben zur Aufsichtsbehörde in Kap. 3.4.17, S. 152 ff., eine Indizwirkung.

[188] Schneider, Sekundärnutzung klinischer Daten, S. 269 f.

sätzlich nur für Gegenstände im Gewahrsam eines Zeugnisverweigerungsberechtigten (wie eines Arztes) gilt. Eine rein landesrechtliche Fiktion könnte dieses Erfordernis nicht umgehen.[189] Allerdings erweitert § 97 Abs. 3 StPO das Beschlagnahmeverbot auch auf Gegenstände im Gewahrsam von Personen, die nach § 53a Abs. 1 S. 1 StPO an der beruflichen Tätigkeit der in § 53 Abs. 1 S. 1 Nr. 3 StPO genannten Angehörigen von Heilberufen mitwirken und vor diesem Hintergrund bereits ein Zeugnisverweigerungsrecht haben.[190] Diese Mitwirkung ist hier gleich wie nach § 203 Abs. 3 StGB auszulegen, auch wenn es für Zeugnisverweigerungsrecht und Beschlagnahmeverbot wohl nicht darauf ankommt, ob auch eine Schweigeverpflichtung nach dieser Vorschrift vorgenommen wurde.[191] Damit kommt es auf die Wirkungen der landesrechtlichen Regelung in § 48 Abs. 3 LKHG BW letztlich nicht an.

Gesetzgebungsvorhaben mit Aufhebung des § 48 LKHG BW

Die Vorschrift des § 48 LKHG BW könnte jedoch in naher Zukunft aufgehoben werden. Im Gegensatz zum LDSG BW wurden nach der Einführung der DSGVO viele andere Gesetze nur minimal durch den Landesgesetzgeber an diese angepasst und das LKHG BW noch überhaupt nicht. Der baden-württembergische Gesetzgeber plant jedoch, mit dem Gesetz zur Anpassung des bereichsspezifischen Datenschutzrechts die landesrechtlichen Datenschutzregelungen in naher Zukunft weiter an die DSGVO anzupassen. Momentan hat der Referentenentwurf die erste Phase der Online-Kommentierung verlassen.[192] Der Gesetzesentwurf sieht eine Aufhebung des § 48 LKHG BW vor.[193] Das Ziel dieses Entwurfs ist es, dass die landesrechtlichen Einschränkungen für die Auftragsverarbeitung aufgehoben werden und sich die Zulässigkeit der Auftragsverarbeitung nach Art. 28 DSGVO bestimmt. Die Aufhebung wird damit begründet, dass § 48 LKHG BW für den Datenschutz in der Praxis häufig große Probleme bei der Verarbeitung von Patientendaten bereite. Die datenschutzkonforme Beauftragung von Stellen, die keine Krankenhäuser bzw. Rechenzentren sind, würde von den Krankenhäusern als zu aufwändig und nicht zeitgemäß angesehen, obwohl viele Krankenhäuser aus betriebswirtschaftlichen

[189] Vgl. dazu den grds. gegebenen strafprozessualen Zugriff auf „Corona-Gästelisten" trotz strikter Bindung an Zwecke des Infektionsschutzes in den Rechtsverordnungen der Bundeländern auf Basis des Infektionsschutzgesetzes (IfSG) vor Inkrafttreten des Dritten Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite: Bloß/Kühhorn, Strafrechtliche Ermittlungen gestützt auf „Corona-Gästelisten", JA 2020, 1036 ff.; Antrag der Fraktion der Linkspartei zur strikten Zweckbindung für Corona-Gästelisten, Bundestags-Drucksache 19/23733, S. 1; Niedernhuber, Die Verwendung von Corona-Gästelisten zur Strafverfolgung, KriPoZ 2020, 318 ff.

[190] Dort werden folgende Heilberufe aufgezählt: Ärzte, Zahnärzte, Psychotherapeuten, Psychologische Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten, Apotheker und Hebammen. Zu den mitwirkenden Personen gehören neben den medizinischen Assistenzberufen oder den angestellten IT-Fachkräften im Krankenhaus auch die sonstigen mitwirkenden Personen außerhalb des Krankenhauses wie bspw. ein Cloud-Anbieter.

[191] Gesetzentwurf der Bundesregierung zur Umsetzung der Berufsanerkennungsrichtlinie und zur Änderung weiterer Vorschriften im Bereich der rechtsberatenden Berufe, Bundestags-Drucksache 18/9521, S. 233 f..

[192] Quelle: https://beteiligungsportal.baden-wuerttemberg.de/de/mitmachen/lp-16/anpassung-des-bereichsspezifischen-datenschutzrechts/ (Stand: Dezember 2020).

[193] Referentenentwurf des Gesetzes zur Anpassung des bereichsspezifischen Datenschutzrechts an die Verordnung (EU) 2016/679 im Geschäftsbereich des Sozialministeriums und zur Änderung des Landesgesundheitsgesetzes vom 13. Juni 2019, S. 14.

Gründen auf ein Outsourcing angewiesen seien.[194] Damit wäre dann zweifelslos auch die Beauftragung von Cloud-Anbietern erlaubt, wenn man hier in Bezug auf den gegenwärtig verwandten Rechenzentrums-Begriff eine restriktivere Auslegung verfolgen würde.

Baden-Württemberg würde im Falle einer solchen Neuregelung den Beispielen von Hamburg und Rheinland-Pfalz folgen. Andere Bundesländer wie Schleswig-Holstein oder Bremen planen ebenfalls neue Landeskrankenhausgesetze. Diese sehen jedoch weitere Vorgaben an die Auftragsverarbeitung als Ergänzung zu Art. 28 DSGVO vor und entsprechen eher den Beispielen des Saarlands oder von Sachsen-Anhalt. Es bleibt daher noch abzuwarten, ob § 48 LKHG BW letztendlich komplett aufgehoben oder lediglich modifiziert wird.

Das LDSG BW enthält, abgesehen von den bereits angesprochenen Vorschriften zu den technischen und organisatorischen Sicherheitsmaßnahmen in § 3 LDSG BW, keine speziellen Vorschriften zur Verarbeitung im Auftrag.

Subsidiär, also nachrangig, gelten überdies, auch ohne expliziten Verweis in § 48 LKHG BW, die allgemeinen Vorschriften zur Auftragsverarbeitung, also Art. 28 DSGVO. Denn § 48 LKHG BW bestimmt nur bereichsspezifisch zusätzliche Anforderungen an die Verarbeitung von Patientendaten im Auftrag von Krankenhäusern, ohne den Gesamtkomplex der Auftragsverarbeitung abschließend regeln zu wollen. Im Übrigen findet somit Art. 28 DSGVO Anwendung.

Eine Schweigeverpflichtung wäre dann aber ohne § 48 Abs. 2 Nr. 2 LKHG BW allein aufgrund § 203 Abs. 3 StGB nach wie vor erforderlich. Und auch technische und organisatorische Sicherheitsmaßnahmen müssten auch ohne § 48 Abs. 2 Nr. 3 LKHG BW aufgrund § 3 LDSG BW und in jedem Fall nach Art. 28 DSGVO getroffen werden. Lediglich die Pflicht zur Benachrichtigung der Aufsichtsbehörden nach § 48 Abs. 2 Nr. 1 LKHG BW würde entfallen.

In gesetzgeberischer Hinsicht sollte aber aufgrund der Sensibilität der outgesourcten Patientendaten überlegt werden, die Pflicht zur Benachrichtigung der eignen Datenschutzaufsichtsbehörde über die Auftragsverarbeitung durch die auftraggebenden Krankenhäuser beizubehalten. Diese Benachrichtigung könnte über entsprechend gesicherte Online-Formulare weitgehend standardisiert erfolgen und von der Behörde automatisiert ausgewertet werden. So

[194] Zum Ganzen: Begründung des Referentenentwurfs für die Anhörung vom 13. Juni 2019 zum Gesetz zur Anpassung des bereichsspezifischen Datenschutzrechts an die Verordnung (EU) 2016/679 im Geschäftsbereich des Sozialministeriums und zur Änderung des Landesgesundheitsgesetzes, S. 20. Diese Begründung verwundert insoweit, als dass die Beauftragung von Stellen, die keine Krankenhäuser bzw. Rechenzentren sind, mit der Verarbeitung personenbezogener Patientendaten nach dem geltenden § 48 LKHG BW überhaupt nicht nur aufwändig, sondern überhaupt nicht zulässig ist. Ein Zusatzaufwand könnte sich jedoch ergeben, soweit der Personenbezug durch Maßnahmen wie die Krankenhaus-interne Pseudonymisierung oder Verschlüsselung aufgehoben würde. Bei der Beauftragung von anderen Krankenhäusern würde allerdings nach geltendem Recht ohnehin über § 48 Abs. 1 LKHG BW letztlich auch nur Art. 28 DSGVO gelten. Und bei der Beauftragung von Krankenhäusern müssten zwar die Voraussetzungen des § 48 Abs. 2 LKHG BW eingehalten werden, die aber ohnehin inzwischen mit Ausnahme von Nr. 1 (Benachrichtigung der Aufsichtsbehörden) nur noch deklaratorisch sind: Eine Schweigeverpflichtung nach Nr. 2 müsste, jedenfalls wenn mit § 48 LKHG BW die bereichsspezifische Befugnisnorm wegfällt, bereits nach § 203 StGB erfolgen und technische und organisatorische Maßnahmen wie in Nr. 3 sind auch in Art. 28 DSGVO vorgesehen. Von daher dürfte es letztlich um die gesetzgeberische Zulassung der Nutzung bspw. der Dienste von externen Schreibbüros, Spracherkennungs- oder anderen Diensten aus der Cloud gehen, soweit man in Bezug auf Cloud-Angebote nicht von einem Rechenzentrumsdienst ausgehen würde.

hätte diese einen groben Überblick über Art und Ausmaß des Outsourcings im Krankenhausbereich und könnte dies als Ansatzpunkt für Stichprobenprüfungen nehmen.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

In Baden-Württemberg finden sich Regelungen zu technischen und organisatorischen Maßnahmen in § 3 LDSG BW.

Gemäß § 3 Abs. 1 S. 1 LDSG BW sind bei der Datenverarbeitung angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Dabei sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

§ 3 Abs. 1 S. 2 LDSG BW enthält einen nicht abschließenden Katalog solcher Maßnahmen. Nach § 3 Abs. 1 S. 2 LDSG BW gehören dazu insbesondere

1. technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt,
2. Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind,
3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der öffentlichen Stelle und von Auftragsverarbeitern,
5. die Pseudonymisierung personenbezogener Daten,
6. die Verschlüsselung personenbezogener Daten,
7. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen, einschließlich der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
8. die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung und
9. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung personenbezogener Daten für andere Zwecke die Einhaltung des LDSG sowie der DSGVO sicherstellen.

In der Begründung des Gesetzes wird zu § 3 LDSG BW ausgeführt, dass die DSGVO die Bedeutung des technischen und organisatorischen Datenschutzes herausstelle und hierzu entsprechende Maßnahmen verlange, die ein dem Risiko angemessenes Schutzniveau gewährleisten. Die aufgeführten Maßnahmen würden eine Konkretisierung der in Art. 32 Abs. 1 Buchst. a, b DSGVO als geeignet genannten Maßnahmen auf der Grundlage von Art. 5 Abs. 2 DSGVO darstellen. Sie trügen entscheidend dazu bei, bei der Verarbeitung personenbezogener Daten die Gefahren für die Rechte und Freiheiten der betroffenen Personen möglichst gering zu halten und damit die Grundrechte der betroffenen Personen zu wahren. Damit setze die Regelung zugleich das Erfordernis um, bei der Verarbeitung besonderer Kategorien personenbezogener

Daten nach Art. 9 DSGVO „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person" vorzusehen. In jedem Fall verpflichtende Maßnahmen wie z.B. die Beteiligung der oder des Datenschutzbeauftragten der öffentlichen Stelle seien nicht aufgeführt.[195] Mit dem Verweis auf den Stand der Technik seien technische Mindeststandards erfasst. Aus dem Wort „insbesondere" in § 3 Abs. 1 S. 3 ergebe sich der beispielhafte Charakter. Teilweise handele es sich um Wiederholungen aus Art. 32 DSGVO. Diese wurden jedoch im Interesse einer kohärenten Regelung als zulässig angesehen.[196]

Soweit keine Öffnungsklausel der DSGVO wie die in Art. 9 DSGVO genutzt werden kann, kommt § 3 Abs. 1 LDSG BW somit lediglich klarstellende Bedeutung mit Nachrang gegenüber der DSGVO zu. Der Maßnahmenkatalog in § 3 Abs. 1 S. 2 LDSG BW ist ohnehin insoweit unverbindlich, als dass nicht alle dort aufgezählten Maßnahmen getroffen werden müssen, sondern diese nur Beispiele für Maßnahmen darstellen, die nach den Kriterien des Satzes 1 dieser Vorschrift in Betracht gezogen werden sollten.

Und die generalklauselartigen Maßstäbe in § 3 Abs. 1 S. 1 LDSG BW entsprechen auch im Wortlaut Art. 32 Abs. 1 S. 1 Halbsatz 1 DSGVO. Diese wird durch die nicht abschließend aufgezählten Maßnahmen im eben beschriebenen Sinn weiter konkretisiert. Die Regelungen der §§ 3 Abs. 1 S. 2 Nr. 5, Nr. 6 LDSG BW entsprechen Art. 32 Abs. 1 Halbsatz 2 Buchst. a DSGVO. § 3 Abs. 1 S. 2 Nr. 7 LDSG BW entspricht Art. 32 Abs. 1 Halbsatz 2 Buchst. b, Buchst. c DSGVO und § 3 Abs. 1 S. 2 Nr. 8 LDSG BW entspricht Art. 32 Abs. 1 Halbsatz 2 Buchst. d DSGVO.

Fraglich ist, ob die Vorschrift des § 3 Abs. 1 LDSG BW auch für den Auftragsverarbeiter gilt. § 3 Abs. 1 S. 1 LDSG BW bestimmt, dass diese Regelung bei der Datenverarbeitung Anwendung findet. Es wird keine Unterscheidung zwischen Auftragsverarbeiter und Verantwortlichem vorgenommen. Nach obigen Ausführungen ist § 3 Abs. 1 S. 1 LDSG BW zudem im Wesentlichen eine Wiederholung des Art. 32 DSGVO. Art 32 DSGVO richtet sich sowohl an den Verantwortlichen als auch an den Auftragsverarbeiter. § 3 Abs. 1 S. 1 LDSG soll folglich auf beide Anwendung finden.

Die allgemeinen Vorgaben an die technischen und organisatorischen Maßnahmen auch bei der Verarbeitung von Patientendaten ergeben sich somit aus § 3 Abs. 1 LDSG BW und Art. 32 DSGVO. Die konkret getroffenen Maßnahmen müssen zudem geeignet sein, die Einhaltung der nach dem LKHG und anderen anwendbaren Vorschriften zum Datenschutz bestehenden Zulässigkeitsvoraussetzungen in hinreichend sicherer Weise auf technischer und organisatorischer Ebene zu gewährleisten.

[195] Gesetzentwurf der Landesregierung Baden-Württembergs zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679, Landtag Baden-Württemberg Drucksache: 16/3930 vom 19. April 2018, S. 92.

[196] Landesregierung Baden-Württemberg, Landtag Baden-Württemberg Drucksache: 16/3930 vom 19. April 2018, S. 63. Dies ist die Haltung der Landesregierung. In der Verbände- und Öffentlichkeitsbeteiligung zum Gesetzentwurf hatten mehrere Institutionen (der Landesbeauftragte für den Datenschutz, die Baden-Württembergische Krankenhausgesellschaft sowie die Universitätsklinika in Tübingen und Ulm) angemerkt, dass sie die Norm als Verstoß gegen das Wiederholungsverbot ansehen und daher um Klarstellung baten, dass es sich um eine nicht abschließende Aufzählung handele.

3.4.2 Bayern

Auf Krankenhäuser anwendbare Datenschutzvorschriften[197]

Das Bayerische Krankenhausgesetz (LKHG BY) ist nach seinem Art. 2 auf alle Krankenhäuser in Bayern anwendbar, soweit diese nach dem Krankenhausfinanzierungsgesetz des Bundes (KHG) förderfähig sind. Auf eine tatsächliche Förderung nach dem KHG kommt es somit nicht an.

Krankenhäuser öffentlicher Träger

Im öffentlichen Bereich ist allerdings zu beachten, dass Universitätsklinika nach § 5 Abs. 1 Nr. 1 KHG und Krankenhäuser des Bundes nach § 5 Abs. 1 Nr. 9 KHG grundsätzlich nicht förderfähig im Sinne des KHG sind.[198] Auf diese Kliniken ist daher das LKHG BY nicht anwendbar, soweit sie nicht durch andere Normen in dessen Anwendungsbereich einbezogen werden, was bei Krankenhäusern des Bundes nicht der Fall ist und aus Kompetenzgründen auch problematisch wäre. gemäß Jedoch ordnet Art 15 Abs. 2 des Bayerischen Universitätsklinikagesetzes die entsprechende Geltung der Datenschutzregeln des Art. 27 LKHG BY an, welche damit auch auf Universitätskliniken anwendbar sind.

Gilt subsidiär das LDSG oder das BDSG?

Nach Art. 27 Abs. 1 S. 2 LKHG BY ist das LKHG BY vorrangig und die im Übrigen jeweils geltenden Vorschriften über den Schutz personenbezogener Daten sind nachrangig anwendbar. Als nachrangig geltende Gesetze kommen das LDSG BY, das BDSG und die DSGVO in Betracht.

Das LDSG BY ist nach seinem Art. 1 Abs. 1 S. 1 auf Behörden und sonstige öffentliche Stellen des Freistaates Bayern, der Gemeinden, Gemeindeverbände und der sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts anwendbar. Unter der Aufsicht des Landes stehen alle juristischen Personen des öffentlichen Rechts, die nicht der Aufsicht des Bundes unterstehen. Unter Bundesaufsicht stehen im Klinikbereich lediglich die Bundeswehrkrankenhäuser. Das LDSG BY ist somit anwendbar auf Kliniken, die als Eigenbetriebe (ohne eigenständige Rechtspersönlichkeit) der genannten öffentlichen Stellen geführt werden, und Kliniken mit eigener Rechtspersönlichkeit, gleich ob öffentlichen Rechts (Anstalten, Körperschaften, Stiftungen) oder privaten Rechts (wie der einer GmbH oder AG), die in Trägerschaft der genannten öffentlichen Stellen stehen. Die in Art. 1 Abs. 1 BayUniKlinG aufgeführten Universitätskliniken werden als rechtsfähige Anstalten des öffentlichen Rechts mit dem Recht zur Selbstverwaltung geführt und unterfallen somit – subsidiär – ebenfalls dem Anwendungsbereich des LDSG BY nach Art. 1 Abs. 1 S. 1 LDSG BY.

---

[197] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 135 ff.

[198] Gemäß § 5 Abs. 1 Nr. 1 KHG ist eine Investitionsförderung von Universitätskliniken nach § 8 ff. KHG entbehrlich, wenn die spezielleren Landeshochschulförderungsgesetze eingreifen. Dies ist der Fall bei Universitätskliniken die sowohl der allgemeinen Versorgung der Bevölkerung als auch der Forschung und Lehre dienen. Nach § 5 Abs. 1 Nr. 1 Hs. 2 KHG gilt dies für Krankenhäuser, die Aufgaben der Ausbildung von Ärzten nach der Approbationsordnung für Ärzte erfüllen, nur hinsichtlich der nach den landesrechtlichen Vorschriften für Hochschulen förderfähige Maßnahmen. Dies stellt sicher, dass falls keine Förderung der Länder eingreift, die Krankenhäuser insoweit nach dem KHG gefördert werden können. Eine fehlende Förderfähigkeit schließt eine Aufnahme in Krankenhauspläne aber grundsätzlich nicht aus, da Universitätskliniken der allgemeinen Versorgung dienen können (zum Ganzen: *Würtenberger/Altschwager* in Dettling/Gerlach, Krankenhausrecht, 2. Auflage 2018, § 5 KHG, Rdnr. 4-6).

Gemäß Art. Art. 1 Abs. 2 LDSG BY gilt das LDSG BY auch für Kliniken in privater Rechtsform, wenn an ihnen eine in Art. 1 Abs. 1 LDSG BY genannte juristische Person des öffentlichen Rechts unmittelbar beteiligt ist. Denn die Krankenhausversorgung kann auch, wie es Art. 1 Abs. 2 LDSG BY erfordert, als Aufgabe der öffentlichen (Leistungs-)Verwaltung wahrgenommen werden. Im Unterschied zu § 2 Abs. 2 LDSG BW kommt es dabei nicht auf eine Mehrheitsbeteiligung der öffentlichen Hand an. Dies gilt auch, sofern daneben öffentlichen Stellen des Bundes beteiligt sind, wenn die Ziel-Gesellschaft, also die Stelle, an welcher die Beteiligung besteht, dadurch nicht nach § 2 Abs. 3 S. 1 BDSG als öffentliche Stelle des Bundes gilt. Die zuletzt genannte Unterstellung unter das BDSG setzt neben der privaten Rechtsform eine Tätigkeit in mehreren Bundesländern oder eine absolute Mehrheit der Anteile oder Stimmen des Bundes voraus.[199]

Soweit an sich dem LDSG BY unterworfene öffentliche Stellen allerdings als Unternehmen am Wettbewerb teilnehmen, gelten für sie sowie für ihre Zusammenschlüsse und Verbände die Vorschriften für nicht-öffentliche Stellen (Art. 1 Abs. 3 S. 1 LDSG BY).[200] Dies ist – wie schon in Baden-Württemberg[201] – auch für Krankenhäuser in Bayern anzunehmen, jedenfalls bzgl. der Primärnutzung zu Behandlungszwecken. Insoweit kommen damit die für nicht-öffentliche Stellen geltenden Vorschriften des BDSG Anwendung, soweit sie Öffnungsklauseln der DSGVO ausfüllen; im Übrigen gelten die entsprechenden Vorschriften der DSGVO direkt.

Die Zuständigkeit des Bayerischen Landesbeauftragten für den Datenschutz (LfD BY) nach Art. 15 LDSG BY bleibt von dieser Verweisung jedoch gemäß Art. 1 Abs. 3 S. 2 LDSG BY ausdrücklich unberührt. Die Aufsicht nach Art. 51 ff. DSGVO obliegt damit bei öffentlichen Krankenhäusern nicht dem für den nicht-öffentlichen Bereich nach § 40 BDSG, Art. 18 LDSG BY zuständigen Bayerische Landesamt für Datenschutzaufsicht (LDA).

Allerdings bleibt der Systematik nach auch Art. 1 Abs. 5 LDSG BY und damit der Vorrang besonderer Datenschutzvorschriften wie jener des LKHG BY von dieser Verweisung unberührt.

Ergebnis: Auf alle Krankenhäuser, die nach dem KHG förderfähig sind, ist vorrangig das LKHG BY anwendbar. Die Datenschutzvorschriften des LKHG BY gelten entsprechend für Universitätskliniken des Landes Bayern. Auf öffentliche Krankenhäuser sind nachrangig primär das BDSG sowie außerhalb der Öffnungsklauseln die DSGVO direkt und nur bzgl. der Aufsicht die Regelungen des LDSG BY anwendbar. Dies gilt auch für Kliniken in privater Rechtsform unter

[199] Eine entsprechende Regelung mit explizitem Verweis auf das BDSG bestand in Art. 2 Abs. 2 S. 1 Nr. 2 der alten Fassung des BayDSG: „Die Vorschriften dieses Gesetzes gelten auch für Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen – ungeachtet der Beteiligung öffentlicher Stellen – (…) außer einer oder mehrerer der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts auch eine oder mehrere der in § 2 Abs. 1 des Bundesdatenschutzgesetzes genannten juristischen Personen des öffentlichen Rechts oder Vereinigungen beteiligt sind, wenn sie keine öffentlichen Stellen des Bundes gemäß § 2 Abs. 3 Bundesdatenschutzgesetzes sind." Dieser Verweis wurde in der Neufassung des Gesetzes nicht übernommen. Trotz des Entfernens des Verweises, ändert sich nichts an der Rechtslage, da § 2 Abs. 3 S. 1 BDSG unverändert beibehalten wurde und Art. 1 Abs. 2 S. 1 LDSG BY nach wie vor keine Mehrheitsbeteiligung einer sonstigen bayerischen öffentlichen Stelle fordert.

[200] Durch das „soweit" wird wie im Bund (oder anderen Bundesländern) eine funktionelle Sichtweise der Wettbewerbsklausel nahegelegt, mit der sich daraus ergebende Problematik, dass diese für manche Tätigkeiten einer Stelle greifen könnte (mit der Folge der Anwendbarkeit des BDSG), für andere Tätigkeiten aber nicht (also das LDSG BY anwendbar ist).

[201] Dort (oben S. 80 f.) mit ausführlicherer Argumentation, welche auf die entsprechenden Klauseln anderen Bundesländer übertragen werden kann.

öffentlicher Beteiligung des Landes Bayern, wobei es nicht auf eine Mehrheitsbeteiligung der öffentlichen Hand ankommt.

Krankenhäuser privater Träger

Das LKHG BY ist, wie bereits beschrieben, nach seinem Art. 2 auf alle Krankenhäuser anwendbar, soweit diese nach dem Krankenhausfinanzierungsgesetz (KHG) förderfähig sind. Grundsätzlich sind auch Kliniken privater Träger KHG-förderfähig, so dass das LKHG BY auf sie anwendbar ist. Ist eine Privatklinik ausnahmsweise nicht KHG-förderfähig, ist das LKHG BY auf sie jedoch nicht anwendbar. Dies ist insbesondere der Fall, wenn sie nicht die Voraussetzungen des § 67 AO erfüllt (§ 5 Abs. 1 Nr. 2 KHG). Danach ist eine Klinik steuerbegünstigt, wenn bei ihr wenigstens 40 % der Belegungstage auf Patienten entfallen, bei denen die Entgelte für allgemeine Krankenhausleistungen (§ 7 KHEntgG, § 10 BPflV) berechnet werden oder nicht höher als diese ausfallen. Durch Landesrecht kann allerdings bestimmt werden, dass die KHG-Förderung auch solchen Kliniken gewährt wird (§ 5 Abs. 2 KHG), was jedoch im 3. Abschnitt des LKHG BY über die Investitionsförderung (Art. 9 – 21) nicht geschehen ist.

Gilt subsidiär das LDSG oder das BDSG?

Ist das LKHG BY anwendbar, weil eine Klinik KHG-förderfähig ist, so sind das LKHG BY vorrangig und die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten nachrangig anwendbar (Art. 27 Abs. 1 S. 2 LKHG BY). Als nachrangig geltende Gesetze kommen das LDSG BY, das BDSG und die DSGVO in Betracht.

Nach Art. 1 Abs. 1 und 3 LDSG BY ist dieses Gesetz an sich nicht auf private Kliniken anwendbar, weil diese keine öffentliche Stelle sind. Es wäre im Umkehrschluss nach Art. 1 Abs. 2 LDSG BY aber anwendbar, wenn an einer Klinik in privater Rechtsform die öffentliche Hand (des Landes) beteiligt ist, auch wenn es sich nur um eine Minderheitsbeteiligung handelt. Solche Kliniken werden wie Kliniken öffentlicher Träger behandelt, allerdings aufgrund ihrer Eigenschaft als öffentlich-rechtliche Wettbewerbsunternehmen doch wieder weitgehend den privaten Kliniken gleichgestellt und den Vorschriften über nicht-öffentliche Stellen unterstellt werden (Art. 1 Abs. 3 S. 1 LDSG BY).

Bei privaten Krankenhäusern handelt es sich um nicht-öffentliche Stellen nach § 2 Abs. 4 S. 1 BDSG. Auf sie sind daher das BDSG sowie außerhalb der Öffnungsklauseln die DSGVO direkt anwendbar, und zwar entweder nachrangig nach dem LKHG BY, wenn die Klinik KHG-förderfähig ist, oder direkt, d. h. ohne Vorrang des LKHG BY.

Die Aufsicht über Krankenhäuser in ausschließlich privater Trägerschaft liegt nach § 40 BDSG in Verbindung mit Art. 18 LDSG BY beim Bayerischen Landesamt für Datenschutzaufsicht.

Ergebnis: Auf alle Krankenhäuser, die nach KHG förderfähig sind, ist vorrangig das LKHG BY anwendbar. Private Kliniken sind grundsätzlich KHG-förderfähig, außer sie sind nicht nach § 67 AO steuerbegünstigt. Auf Kliniken in ausschließlich privater Trägerschaft sind das BDSG sowie außerhalb der Nutzung von Öffnungsklauseln die DSGVO direkt anwendbar, entweder nachrangig nach dem LKHG BY oder – mangels KHG-Förderfähigkeit bei reinen Privatkliniken – ohne Vorrang des LKHG BY. Auf Kliniken in privater Rechtsform unter öffentlicher Beteiligung

(des Landes) ist immer nachrangig neben dem BDSG und der DSGVO zum Teil (bzgl. der Aufsicht) auch das LDSG BY anwendbar, unabhängig davon, ob die öffentliche Hand in Mehrheit oder Minderheit beteiligt ist.

Öffnungsklausel für kirchliche Träger?

Eine Öffnungsklausel für Regelungen des Datenschutzes in kirchlichen Krankenhäusern durch Religionsgesellschaften besteht in Bayern nicht.

Zusammenfassung

Auf öffentliche wie private Krankenhäuser, die nach KHG förderfähig sind, ist vorrangig das LKHG BY anwendbar. Entsprechend gelten die Datenschutzregeln des LKHG BY auch für die bayerischen Universitätskliniken. Auf Krankenhäuser in zumindest teilweise öffentlicher Trägerschaft sind nachrangig das BDSG sowie außerhalb der Öffnungsklauseln die DSGVO direkt und nur bzgl. der Aufsicht das LDSG BY anwendbar. Auf Kliniken in ausschließlich privater Trägerschaft sind das BDSG sowie außerhalb der Öffnungsklauseln die DSGVO direkt[202] anwendbar, entweder nachrangig zum LKHG BY oder – bei reinen Privatkliniken – ohne dessen Vorrang. Es besteht keine Öffnungsklausel für kirchliche Krankenhäuser.

Vorschriften zur Auftragsverarbeitung[203]

Nach Art. 27 Abs. 4 S. 1 LKHG BY dürfen Krankenhausärzte Patientendaten nutzen, soweit dies im Rahmen des krankenhausärztlichen Behandlungsverhältnisses, zur Aus-, Fort- und Weiterbildung im Krankenhaus, zu Forschungszwecken im Krankenhaus oder im Forschungsinteresse des Krankenhauses erforderlich ist. Sie können gemäß Art. 27 Abs. 4 S. 2 Halbsatz 1 LKHG BY damit andere Personen im Krankenhaus beauftragen, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist. Nach Art. 27 Abs. 4 S. 2 Halbsatz 2 LKHG können die Krankenhausärzte zu Forschungszwecken nach Satz 1 anderen Personen die Nutzung von Patientendaten gestatten, soweit dies für die Forschung erforderlich ist und die Daten im Gewahrsam des Krankenhauses verbleiben. In beiden Fällen sind die anderen Personen nach Art. 27 Abs. 4 S. 3 LKHG BY zur Verschwiegenheit zu verpflichten.

Bei der Weitergabe zu Forschungszwecken handelt es sich regelmäßig um einen besonders privilegierten Fall der Datenübermittlung durch Gewährung von Zugriffsrechten, wenn zugriffsberechtigte Personen mit den Patientendaten in gewissem Umfang eigenverantwortlich (z.B. im Rahmen der Verbundforschung) umgehen. Wird durch einen solchen Zugriff ein rein weisungsgebundener Umgang mit personenbezogenen Daten ermöglicht, z.B. im Rahmen der rein technischen (Fern-)Wartung einer Forschungsdatenbank, liegt zudem ein Fall der Auftragsverarbeitung vor, auf den subsidiär die Regelungen zur Auftragsverarbeitung nach Art. 28 DSGVO Anwendung finden.[204]

[202] Europarechtskonforme Nutzung der in der DSGVO bestehenden Öffnungsklauseln jeweils vorausgesetzt.

[203] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 270 ff.

[204] Der ehemalige Art. 6 LDSG BY zur Auftragsdatenverarbeitung für öffentliche Stellen in Bayern wurde infolge der Reformen zur Anpassung an die DSGVO ersatzlos gestrichen. Es kommt hier somit ohne eine Unterscheidung zwischen privaten und öffentlichen Trägern allein auf Art. 28 DSGVO an.

Die Beauftragung anderer Personen nach Art. 27 Abs. 4 S. 2 Halbsatz 1 LKHG BY, also auch eine solche im Rahmen der Behandlung, ist hingegen auf andere Personen im Krankenhaus beschränkt. Sie gestattet somit nur eine krankenhausinterne Weitergabe der Patientendaten, sodass eine Weitergabe außerhalb des Krankenhauses nach dieser Vorschrift nicht stattfinden kann.

Auftragsverarbeitung zur verwaltungsmäßigen Abwicklung der Behandlung

Art. 27 Abs. 4 S. 4 LKHG BY bestimmt, dass die Krankenhausverwaltung Patientendaten nutzen darf, soweit dies zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich ist. Will sich das Krankenhaus zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedienen, so muss es gemäß Art. 27 Abs. 4 S. 5 LKHG BY sicherstellen, dass der Auftragnehmer besondere Schutzmaßnahmen nach Art. 27 Abs. 6 LKHG BY einhält und, solange keine Anhaltspunkte dafür bestehen, dass durch die Art und Ausführung der Auftragsverarbeitung keine schutzwürdigen Belange von Patienten beeinträchtigt werden. Die in Art. 27 Abs. 6 LKHG BY aufgeführten Schutzmaßnahmen sind Maßnahmen technischer und organisatorischer Art, durch die sichergestellt werden kann, dass Patientendaten nicht unberechtigt verwendet oder übermittelt werden.

Für die Auftragsverarbeitung im Rahmen von KIS, auch und gerade in der Cloud, bedeutet dies, dass auf Grundlage von Art. 27 Abs. 4 S. 5 LKHG BY nur administrative Module ausgesourct werden dürfen, so z.B. die Verwaltung der Patientenstammdaten oder DRG-Codes für die Abrechnung mit den Krankenkassen, nicht aber primär medizinische Module wie solche zur Arzneimitteltherapiesicherheit, soweit in diesen Patientendaten verarbeitet werden,[205] oder gar eine vollständige elektronische Patientenakte.

Auftragsverarbeitung durch andere Krankenhäuser

Auch ist zu beachten, dass Krankenhäuser gemäß Art. 27 Abs. 5 S. 6 LKHG BY nur andere Krankenhäuser mit der Verarbeitung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich sind, beauftragen dürfen. Diese Beschränkung greift daher auch beim Outsourcing von KIS, soweit diese nicht nur administrative Module wie insbesondere solche zur Verwaltung der Stammdaten und der Abrechnungsdaten von Patienten enthalten, sondern weitergehende Patientendaten wie Medikationen oder gar eine umfassende elektronische Patientenakte.

Vor diesem Hintergrund käme ein KIS-Betrieb durch einen spezialisierten Cloud-Anbieter zu diesen Zwecken, soweit personenbezogene Patientendaten in die Cloud gegeben werden, allenfalls mit Einwilligung der betroffenen Patienten in Betracht[206] – mit den dazu bereits ausgeführten praktischen Problemen. Anders sähe es aus, soweit ein Cloud-KIS bzw. ein entsprechendes Modul

- lediglich verwaltungsmäßig relevante Patientendaten oder

[205] Etwas anderes würde z.B. für die bloße Bereitstellung von nicht personenbezogenen Daten über unerwünschte Arzneimittelwirkungen aus Cloud-Repositories heraus gelten, was keinen Fall der Auftragsverarbeitung i.S.d. Datenschutzes darstellt.

[206] Falls man davon ausgeht, dass man vom gesetzlichen Leitbild des Art. 27 Abs. 5 S. 6 LKHG BY auch durch eine vorformulierte Einwilligung abweichen kann.

- nur für den Cloud-Anbieter nicht personenbezogene (Krankenhaus-intern nach dem Stand der Technik verschlüsselte oder pseudonymisierte) Patientendaten enthielte oder
- das Cloud-Angebot von einem anderen Krankenhaus betrieben würde.

Subsidiäre Regeln des LDSG BY

Das LDSG BY enthält in den Art. 11 bis 14 LDSG BY Regelungen für Auftragsverarbeiter. Dies ergibt sich aus der Kapitelüberschrift des Kapitels 4: „Verantwortlicher und Auftragsverarbeiter". Auf Krankenhäuser sind diese nach obigen Ausführungen jedoch nicht anwendbar, da primär das BDSG und nur hinsichtlich organisatorischer Regelungen das LDSG BY gilt. Die Regelungen zur Auftragsverarbeitung in Kapitel 8 des LDSG sind ebenfalls nicht anwendbar; sie beziehen sich allein auf Verarbeitungen im Anwendungsbereich der Richtlinie (EU) 2016/680,[207] die auf die Verarbeitung von Patientendaten durch Krankenhäuser keine Anwendung findet.

Subsidiär sind auch hier in jedem Fall die Regelungen zur Auftragsverarbeitung nach Art. 28 DSGVO zu beachten.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

Das LDSG BY enthält keine eigenständige Regelung zu technischen und organisatorischen Maßnahmen.

Das Kapitel 4 „Verantwortlicher und Auftragsverarbeiter" nimmt nur in Art. 11 Bezug auf Art. 32 Abs. 4 DSGVO. Im Umkehrschluss lässt sich daraus entnehmen, dass das LDSG BY keine eigenständigen Regelungen vorgeben soll, sondern auf Art. 32 Abs. 1 bis 3 DSGVO zurückgegriffen wird. Dies wird durch Art. 2 S. 1 LDSG BY klargestellt, wonach für die Verarbeitung personenbezogener Daten durch öffentliche Stellen vorbehaltlich anderweitiger Regelungen die Vorschriften der DSGVO auch außerhalb des sachlichen Anwendungsbereichs des Art. 2 Abs. 1, 2 DSGVO – und somit auch bei nicht automatisierter Verarbeitung außerhalb von Dateisystemen – gelten.

Die Vorgaben an die technischen und organisatorischen Maßnahmen bei der Verarbeitung von Patientendaten ergeben sich somit allein aus Art. 32 DSGVO.

3.4.3 Berlin

Auf Krankenhäuser anwendbare Datenschutzvorschriften[208]

Krankenhäuser öffentlicher Träger

Nach § 2 S. 1 LKHG BE gilt das LKHG BE für alle Krankenhäuser im Land Berlin, soweit im LKHG BE nichts anderes bestimmt ist. Die Bestimmungen des Teils 3 zur Krankenhausförderung gelten nur für Krankenhäuser und Einrichtungen von Krankenhäusern, die nach dem KHG förderfähig (§ 2 S. 1 LKHG BE). Die Datenschutzregeln der §§ 24 und 25 in Teil 5 des LKHG BE gelten

[207] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

[208] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 143 ff.

jedoch unabhängig von einer Förderung nach dem KHG.[209] Von der Geltung dieser wie auch vieler anderer Regeln des LKHG BE sind lediglich die Krankenhäuser des Justizvollzugs ausgenommen (§ 2 S. 3 LKGH BE).

§§ 24 und 25 LKHG BE enthalten besondere Vorschriften für die Verarbeitung von genetischen Daten und Gesundheitsdaten im Sinne der DSGVO in den erfassten Krankenhäusern. Hierbei hat der jeweils Verantwortliche sicherzustellen, dass neben den datenschutzrechtlichen Regeln explizit auch die ärztliche Schweigepflicht eingehalten wird (§ 24 Abs. 1 S. 1 LKHG BE).

Bei Sachverhalten die im LKHG BE nicht abschließend geregelt sind, gelten die Bestimmungen des BDSG oder das LDSG BE, soweit sie auf Krankenhäuser Anwendung finden (§ 24 Abs. 1 S. 2 LKHG BE). Bei dem Verweis in § 24 Abs. 1 LKHG BE handelt es sich, anders als in einigen anderen Ländern, aufgrund der „soweit"-Einschränkung um eine Rechtsgrundverweisung, d. h. die genannten Gesetze sind nur dann anwendbar, wenn ihre jeweiligen Anwendungsvoraussetzungen erfüllt sind.

Gilt subsidiär das LDSG oder das BDSG?

Das LDSG BE ist nach § 2 Abs. 1 S. 1 LDSG BE ausdrücklich auf Krankenhausbetriebe anwendbar, die im Gesetz als sonstige öffentliche Stellen aufgeführt werden, wobei als mögliche Träger das Land und landesunmittelbare Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts genannt sind. Das LDSG BE gilt somit für alle Krankenhäuser in öffentlicher Trägerschaft, wenn das Land mittelbar oder unmittelbar Träger ist.

Nach § 2 Abs. 2 LDSG BE gilt das LDSG BE auch für Vereinigungen des privaten Rechts, wenn sie Aufgaben der öffentlichen Verwaltung wahrnehmen. Die Krankenhausversorgung kann auch als Aufgabe der öffentlichen Verwaltung wahrgenommen werden.[210] Daher gilt das LDSG BE auch für Krankenhäuser in unmittelbarer oder mittelbarer Trägerschaft des Landes, die in einer privaten Rechtsform geführt werden.

Gemäß § 2 Abs. 8 LDSG BE können andere Landesgesetze Abweichungen vom LDSG BE vorschreiben; im Übrigen richtet sich der Datenschutz auch in diesen Fällen nach dem LDSG BE. Gemäß § 24 Abs. 1 LKHG BE i. V. m. § 2 Abs. 8 LDSG BE gilt somit das LKHG BE vorrangig und das LDSG BE nachrangig. Gemäß § 2 Abs. 5 LDSG BE findet das LDSG BE keine Anwendung, soweit Vorschriften der DSGVO unmittelbar gelten, was außerhalb der genutzten Öffnungsklauseln der Fall ist.

Gemäß § 2 Abs. 6 LDSG BE gelten öffentliche Stellen, die am Wettbewerb teilnehmen, jedoch als nicht öffentliche Stellen. Insoweit sind nur die §§ 4 bis 6 und § 20 sowie 22 des LDSG BE anwendbar. Im Übrigen findet für die für nicht-öffentlichen Stellen geltenden Vorschriften des BDSG mit Ausnahme von § 4 (Videoüberwachung öffentlich zugänglicher Räume) und § 38 (Datenschutzbeauftragter nicht-öffentlicher Stellen) BDSG Anwendung. Diese Ausnahme lässt

[209] Die Auskunftspflicht gegenüber der für das Gesundheitswesen zuständigen Senatsverwaltung, insbes. für Zwecke der Krankenhausplanung, nach § 26 LKHG BE wird vorliegend nicht als spezifisch datenschutzrechtliche Norm eingeordnet, da diese vollständig oder jedenfalls weitgehend ohne personenbezogene Daten erfüllt werden kann. DSGVO- und verfassungskonform etablierte gesetzliche Auskunfts- und Mitteilungspflichten gingen nach § 24 Abs. 1 S. 3 LKHG BE aber den Vorschriften dieses Gesetzes vor.

[210] Vgl. dazu nähere Ausführungen zu Baden-Württemberg, oben S. 81.

sich in Bezug auf die Videoüberwachung nach § 4 BDSG wohl mit der strittigen Frage der Konformität der Vorschrift mit der DSGVO erklären.[211] Die Ausnahme des § 38 BDSG lässt sich damit begründen, dass eine öffentliche Stelle nach Art. 37 Abs. 1 Buchst. a DSGVO verpflichtet ist, einen Datenschutzbeauftragten zu bestellen. Eine nicht-öffentliche Stelle wäre hingegen nur zu einer Bestellung unter den Voraussetzungen des § 38 BDSG verpflichtet. Diese Vorgabe der DSGVO sollte nicht durch eine Teilnahme am Wettbewerb umgangen werden können, auch da die DSGVO keine entsprechende Wettbewerbsklausel kennt. Die Anwendung des § 38 BDSG auf öffentliche Stellen, die am Wettbewerb teilnehmen, wird daher ausgeschlossen.

Eine vergleichbare Regelung besteht in Baden-Württemberg in § 2 Abs. 6 LDSG BW. Während dort jedoch als Voraussetzung von öffentlichen Stellen, die als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, die Rede ist, reicht es in Berlin aus, dass überhaupt eine öffentliche Stelle am Wettbewerb teilnimmt, sie braucht kein Unternehmen mit eigener Rechtspersönlichkeit zu sein. Außerdem wird in Baden-Württemberg für die fraglichen Stellen ohne explizite Einschränkungen auf das für nicht-öffentliche Stellen geltende Datenschutzrecht verwiesen, in Berlin dagegen nur teilweise auf das BDSG; im Übrigen verbleibt es in Berlin beim LDSG – gerade bzgl. der Aufsicht durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit. Nach dem vorrangigen LKHG BE gelten somit Teile des LDSG BE und Teile des BDSG gleichermaßen nachrangig; außerhalb der Anwendung von Öffnungsklauseln nimmt die DSGVO deren Stellung ein.

§ 2 Abs. 6 LDSG BE stellt darauf ab, ob am Wettbewerb teilgenommen wird. Dies trifft grundsätzlich auf alle Krankenhäuser zu. Es muss sich jedoch außerdem um eine öffentliche Stelle i. S. d. LDSG BE handeln. Dies trifft jedenfalls auf die in § 2 Abs. 1 S. 1 LDSG BE genannten Einrichtungen zu, weil diese als „Behörden und sonstige öffentliche Stellen" bezeichnet werden, somit auf Krankenhäuser, bei denen das Land oder eine landesunmittelbare Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts Träger ist.

Privatrechtliche Vereinigungen gelten gemäß § 2 Abs. 2 S. 1 LDSG BE ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen, wenn sie Aufgaben der öffentlichen Verwaltung wahrnehmen und das Land Berlin mit absoluter Mehrheit der Anteile oder Stimmen an ihnen beteiligt ist. Nehmen zudem nicht-öffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne von § 2 Abs. 2 S. 2 LDSG BE. Der Verweis in § 2 Abs. 6 LDSG BE gilt daher für alle in § 2 Abs. 1 und Abs. 2 LDSG BE genannten Einrichtungen, wenn sie am Wettbewerb teilnehmen, somit für alle Krankenhäuser in mittelbarer oder unmittelbarer Trägerschaft des Landes, unabhängig der gewählten Rechtsform. Nach § 8 Abs. 2 LDSG BE ist der Landesdatenschutzbeauftragte Aufsichtsbehörde nach § 40 BDSG für die Datenverarbeitung öffentlicher Stellen, soweit diese am Wettbewerb teilnehmen.

Ergebnis: Auf alle Krankenhäuser ist vorrangig das LKHG BE anwendbar. Auf öffentliche Krankenhäuser in mittelbarer oder unmittelbarer Trägerschaft des Landes gelten unabhängig ihrer Rechtsform bei Teilnahme am Wettbewerb nachrangig gleichermaßen Teile des LDSG BE §§ 4

[211] Die DSGVO enthält kein unmittelbares Äquivalent. Die Vorschrift ist vielmehr eine Sonderregelung des deutschen Gesetzgebers, die im Zuge der Neufassung beibehalten wurde. Eine ausdrückliche Regelungskompetenz des deutschen Gesetzgebers besteht nicht und ob sich eine solche aus dem Sachzusammenhang ergibt, ist umstritten. Zum Ganzen mit weiteren Nachweisen: Hullen/Krohm in: Plath, DSGVO/BDSG, 3. Aufl. 2018, § 4 BDSG Rdnr. 1.

- 6, 20 und 22 und Teile des BDSG sowie außerhalb der Anwendung von Öffnungsklauseln unmittelbar die DSGVO.

Krankenhäuser privater Träger

Auf Kliniken privater Träger gilt ebenso wie auf Kliniken öffentlicher Träger vorrangig das LKHG BE.

Gilt subsidiär das LDSG oder das BDSG?

Gemäß § 2 Abs. 2 S. 1 LDSG BE ist das LDSG BE auch auf natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts anwendbar, die Aufgaben der öffentlichen Verwaltung wahrnehmen.

Die Krankenhausversorgung kann auch als Aufgabe der öffentlichen Verwaltung wahrgenommen werden.[212] Dies ist jedoch bei Kliniken privater Träger grundsätzlich nicht der Fall.[213] Diese fallen deshalb nicht unter § 2 Abs. 2 S. 1 LDSG BE. Für sie gilt vielmehr nachrangig das BDSG und außerhalb der Nutzung von Öffnungsklauseln unmittelbar die DSGVO.

Ergebnis: Auf Krankenhäuser in privater Trägerschaft ist vorrangig das LKHG BE und nachrangig das BDSG sowie außerhalb der Anwendung von Öffnungsklauseln unmittelbar die DSGVO anwendbar.

Öffnungsklausel für kirchliche Träger?

Es besteht keine Öffnungsklausel für Regelungen des Datenschutzes in kirchlichen Krankenhäusern durch Religionsgesellschaften.

Zusammenfassung

Auf alle Krankenhäuser ist vorrangig das LKHG BE anwendbar.[214] Auf öffentliche Krankenhäuser (des Landes) gelten nachrangig gleichermaßen Teile des LDSG BE und Teile des BDSG, sowie außerhalb der Anwendung von Öffnungsklauseln unmittelbar die DSGVO. Auf private Krankenhäuser gilt nachrangig das BDSG sowie außerhalb der Anwendung von Öffnungsklauseln die DSGVO direkt.[215] Es besteht keine Öffnungsklausel für kirchliche Krankenhäuser.

Vorschriften zur Auftragsverarbeitung[216]

Verabschiedete Regelung in § 24 Abs. 7 LKHG BE (gültig ab Oktober 2022)

§ 24 Abs. 7 S. 1 des LKHG BE stellt den Grundsatz auf, dass genetische Daten und Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO im Krankenhaus oder im Auftrag durch ein anderes Krankenhaus oder durch mehrere Krankenhäuser als gemeinsam Verantwortliche im Sinne des Art. 26 DSGVO zu verarbeiten sind. Nach § 24 Abs. 7 S. 2 LKHG BE ist die Erteilung eines Auftrages im Sinne des Art. 28 DSGVO zum Zwecke der Verarbeitung von genetischen Daten und Gesundheitsdaten im Sinne des Art. 9 DSGVO nur zulässig, wenn (Nr. 1) der Auftragsverarbeiter

[212] Vgl. dazu nähere Ausführungen zu Baden-Württemberg, s.o. S. 81.

[213] Zur Ausnahme der Beleihung s.o. S. 81, Fn. 174.

[214] Mit Ausnahme der Krankenhäuser des Justizvollzugs, welche hier nicht weiter betrachtet werden.

[215] Europarechtskonforme Nutzung der in der DSGVO bestehenden Öffnungsklauseln jeweils vorausgesetzt.

[216] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 272

der gleichen Unternehmensgruppe nach Art. 4 Nr. 19 DSGVO oder der Unternehmensgruppe eines anderen Krankenhauses, das in den Anwendungsbereich dieses Gesetzes fällt, angehört und (Nr. 2) gewährleistet ist, dass die Verarbeitung der genetischen Daten und Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO ausschließlich durch Personen erfolgt, die nach dem Unionsrecht oder dem Recht eines Mitgliedstaates der Europäischen Union einer Geheimhaltungspflicht unterliegen. Liegen diese Voraussetzungen nicht vor, so erlaubt § 24 Abs. 7 S. 3 LKHG BE eine Verarbeitung von genetischen Daten und Gesundheitsdaten im Sinne des Art. 9 DSGVO durch andere Stellen im Auftrag des Krankenhauses nur, wenn durch technische Schutzmaßnahmen sichergestellt ist, dass der Auftragnehmer keine Möglichkeit hat, beim Zugriff auf Patientendaten den Personenbezug herzustellen.

Zu beachten ist jedoch, dass § 24 Abs. 7 LKHG BE zwar schon vom Berliner Abgeordnetenhaus verabschiedet und auch im Gesetzblatt verkündet wurde, aber noch nicht in Kraft getreten ist. Diese Vorschrift wurde erst im Oktober 2020 durch das BlnDSAnpG-EU[217] angepasst. Art. 57 Abs. 2 BlnDSAnpG-EU bestimmt, dass § 24 Abs. 7 LKHG erst zwei Jahre nach der Verkündung des Gesetzes in Kraft treten soll. Eine solche Einschränkung existierte im Erstentwurf zum Gesetz noch nicht.[218] Erst durch einen späteren, im Plenum des Abgeordnetenhauses angenommenen Änderungsantrag der Fraktion der SPD, der Fraktion Die Linke und der Fraktion Bündnis 90/Die Grünen wurde das Inkrafttreten des § 24 Abs. 7 LKHG BE auf zwei Jahre nach der Verkündung festgesetzt.[219] Der Hintergrund dieser Änderung war wohl die Kritik der Berliner Krankenhausgesellschaft, dass die Bereichsausnahme des § 24 Abs. 7 LKHG zu einschränkend für externe Dienstleister sei. Die Datenschutzbeauftragte des Landes Berlin hatte in ihrer Stellungnahme dagegen angegeben, dass die Einschränkung des § 24 Abs. 7 LKHG BE insbesondere sicherstellen solle, dass global agierende externe Dienstleister, die nicht dem Geheimnisschutz unterliegen, nicht mit der Auftragsverarbeitung betraut werden. Der Forderung der Berliner Krankenhausgesellschaft nach der Öffnung der Auftragsverarbeitung auf alle Unternehmen, die die Bedingungen des § 24 Abs. 7 S. 2 Nr. 2 LKHG BE erfüllen, könne deshalb nicht entsprochen werden. Für solche Unternehmen sei eine Auftragsverarbeitung nur nach § 24 Abs. 7 S. 3 LKHG BE möglich.[220] Abzuwarten bleibt jedoch, ob § 24 Abs. 7 LKHG BE tatsächlich so im Oktober 2022 in Kraft treten wird. Dies ist war nach geltendem Recht der Fall. Angesichts der starken Kritik an der Vorschrift, könnte es sein, dass der Gesetzgeber diese noch einmal vor Inkrafttreten „anpackt" bzw. ändert, die endgültige Entscheidung also lediglich vertagt hat.

Es stellt sich die Frage, welche Vorschriften bis zum Inkrafttreten des § 24 Abs.7 LKHG BE im Oktober 2022 gelten sollen. Eine Anwendung der alten Vorschriften des LKHG BE kommt nicht in Betracht, da das neue Gesetz die §§ 24, 25 LKHG BE nicht modifiziert, sondern vollumfänglich mit Wirkung zum 25. Oktober 2020 neu gefasst hat. Andere Vorschriften existieren in einer solchen Form jedoch nicht. Somit ist in diesem Bereich auf Art. 28 DSGVO abzustellen.

[217] Gesetz zur Anpassung datenschutzrechtlicher Bestimmungen in Berliner Gesetzen an die Verordnung (EU) 2016/679 (Berliner Datenschutz-Anpassungsgesetz-EU – BlnDSAnpG-EU) vom 12.10.2020 (GVBl. S. 807).

[218] Der Senat von Berlin, Abgeordnetenhaus Berlin Drucksache 18/2598 vom 01. April 2020.

[219] Der Senat von Berlin, Abgeordnetenhaus Berlin Drucksache 18/2598-1 vom 30. September 2020.

[220] Der Senat von Berlin, Abgeordnetenhaus Berlin Drucksache 18/2598 vom 01. April 2020, S. 118 f.

Bereits geltende Regelungen

§ 24 Abs. 1 LKHG BE bestimmt, dass subsidiär das LDSG BE oder das BDSG Anwendung finden, soweit ein Sachverhalt nicht abschließend geregelt wurde. Das LDSG BE enthält eine Regelung zur Auftragsverarbeitung in § 26 LDSG BE. Gemäß §§ 26 Abs. 1, Abs. 2 LDSG BE hat der Verantwortliche, soweit die Verarbeitung personenbezogener Daten automatisiert erfolgt, technische und organisatorische Maßnahmen zu treffen.

Werden Systeme und Dienste, die für Verarbeitungen nach § 26 Abs. 1 Abs. 1 LDSG BE genutzt werden, gewartet, so ist gemäß § 26 Abs. 3 LDSG BE durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass nur auf die für Wartung erforderlichen personenbezogenen Daten zugegriffen werden kann. Diese Maßnahmen müssen insbesondere gewährleisten, dass

1. die Wartung nur durch autorisiertes Personal erfolgt,
2. jeder Wartungsvorgang nur mit Wissen und Wollen der speichernden Stelle erfolgt,
3. die unbefugte Entfernung oder Übertragung im Rahmen der Wartung verhindert wird und
4. sichergestellt ist, dass alle Wartungsvorgänge kontrolliert und nach der Durchführung nachvollzogen werden können.

Soweit eine Wartung durch Auftragsverarbeiter erfolgt, muss gemäß § 26 Abs. 3 S. 3 LDSG BE der Vertrag oder das Rechtsinstrument nach Art. 28 Abs. 3 DSGVO Regelungen enthalten, die sicherstellen, dass der Auftragsverarbeiter keine personenbezogenen Daten, die ihm zur Kenntnis gelangen, an andere Stellen übermittelt. Die Durchführung von Wartungsarbeiten mit der Möglichkeit der Kenntniserlangung personenbezogener Daten durch Stellen außerhalb des Geltungsbereichs der DSGVO ist nur zulässig, wenn sie erforderlich sind und bei einer Übermittlung die Voraussetzungen des Art. 45 oder 46 der DSGVO vorliegen.

Gemäß § 26 Abs. 4 LDSG BE werden die Regelungen der DSGVO durch die Absätze 1 bis 3 nicht eingeschränkt.

Im Übrigen findet Art. 28 DSGVO Anwendung.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

Das LDSG BE enthält eine Regelung der spezifischen technischen und organisatorischen Maßnahmen zur Gewährleistung einer rechtmäßigen Verarbeitung in § 26 LDSG BE.

Nach § 26 Abs. 1 LDSG BE hat der Verantwortliche, soweit die Verarbeitung personenbezogener Daten automatisiert erfolgt, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung Maßnahmen zu ergreifen, die gewährleisten, dass

1. personenbezogene Daten jederzeit ihrem Ursprung zugeordnet werden können,
2. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat,
3. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarerer Zeit nachvollzogen werden können und

4. bei der Bereitstellung personenbezogener Daten eine Trennung der Daten nach den jeweils verfolgten Zwecken und betroffenen Personen möglich ist.

Gemäß § 26 Abs. 2 LDSG BE Sind vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung einer automatisierten Verarbeitung personenbezogener Daten die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse zu ermitteln und in einem Datenschutzkonzept zu dokumentieren. Entsprechend der technischen Entwicklung und bei Änderungen der mit den Verarbeitungsvorgängen verbundenen Risiken ist die Ermittlung der Maßnahmen in angemessen Abständen zu wiederholen.

§ 26 Abs. 3 S. 1 LDSG BE bestimmt, dass, wenn Systeme und Dienste, die für die Verarbeitung nach § 26 Abs. 1 LDSG BE genutzt werden, gewartet werden, durch geeignete technische und organisatorische Maßnahmen sicherzustellen ist, dass nur auf die für die Wartung erforderlichen personenbezogenen Daten zugegriffen werden kann. Diese Maßnahmen müssen gemäß § 26 Abs. 3 S. 2 LDSG BE insbesondere gewährleisten, dass

1. die Wartung nur durch autorisiertes Personal erfolgt,
2. jeder Wartungsvorgang nur mit Wissen und Wollen der speichernden Stelle erfolgt,
3. die unbefugte Entfernung oder Übertragung personenbezogener Daten im Rahmen der Wartung verhindert wird und
4. sichergestellt wird, dass alle Wartungsvorgänge kontrolliert und nach der Durchführung nachvollzogen werden können.

Ferner regelt § 26 Abs. 3 S. 3 LDSG BE, dass, soweit eine Wartung durch Auftragsverarbeiter erfolgt, der Vertrag oder das Rechtsinstrument nach Art. 28 Abs. 3 DSGVO Regelungen enthalten muss, die sicherstellen, dass der Auftragsverarbeiter keine personenbezogenen Daten, die ihm zur Kenntnis gelangen, an andere Stellen übermittelt. Die Durchführung von Wartungsarbeiten mit der Möglichkeit der Kenntniserlangung personenbezogener Daten durch Stellen außerhalb des Geltungsbereichs der DSGVO ist gemäß § 26 Abs. 3 S. 4 LDSG BE nur zulässig, wenn sie erforderlich sind und bei einer Übermittlung die Voraussetzungen der Art. 45,46 DSGVO vorliegen.

Nach § 26 Abs. 4 LDSG BE werden die Regelungen der DSGVO durch die Absätze 1 bis 3 nicht eingeschränkt.

Im Gegensatz zu Baden-Württemberg führt das LDSG BE keine generellen Maßnahmen als Wiederholung des Art. 32 DSGVO auf, sondern beschränkt sich allein auf ergänzende Vorgaben für automatisierte Verfahren und die Wartung durch einen Auftragsverarbeiter. § 26 Abs. 4 LDSG BE stellt aber klar, dass im Übrigen die DSGVO gilt. Solange im Zusammenhang mit der Verarbeitung von Patientendaten kein automatisiertes Verfahren oder eine Wartung gegeben ist, findet Art. 32 DSGVO alleinige Anwendung.

Die technischen und organisatorischen Maßnahmen auch bei der Verarbeitung von Patientendaten ergeben sich somit bei automatisierten Verfahren und der Wartung durch einen Auftragsverarbeiter aus § 26 LDSG BE und im Übrigen aus Art. 32 DSGVO.

3.4.4 Brandenburg

Auf Krankenhäuser anwendbare Datenschutzvorschriften[221]

Krankenhäuser öffentlicher Träger

Das brandenburgische Krankenhausentwicklungsgesetz (KHEG BB) regelt den eigenen Anwendungsbereich nicht ausdrücklich. In § 1 Abs. 4 KHEG BB heißt es jedoch: „Die Krankenhausversorgung wird von öffentlichen, freigemeinnützigen und privaten Krankenhäusern getragen. Bei der Durchführung dieses Gesetzes ist diese Vielfalt der Krankenhausträger zu beachten." Demnach fallen sowohl Krankenhäuser in öffentlicher wie in privater Trägerschaft unter das KHEG BB. Für Krankenhäuser des Straf- oder Maßregelvollzugs gelten allerdings lediglich die Vorschriften zur Krankenhaushygiene (§ 39 Abs. 2 KHEG BB), nicht also jene zum Datenschutz.

Gemäß § 27 Abs. 1 KHEG BB sind die Regelungen des KHEG BB und anderer Spezialgesetze, welche die Verarbeitung von Patientendaten durch Krankenhäuser betreffen, ergänzend zur DSGVO vorrangig anzuwenden. Soweit die Spezialgesetze nichts anderes bestimmten, also nachrangig, gilt ergänzend zur DSGVO das LDSG BB. Die DSGVO findet damit letztlich, europarechtskonforme Nutzung ihrer Öffnungsklauseln angenommen, nur mit Nachrang nach dem KHEG BB und dem LDSG BB Anwendung.

Gilt subsidiär das LDSG oder das BDSG?

Gemäß § 27 Abs. 1 LKHG BB gilt das LDSG, soweit im LKHG BB oder anderen Spezialgesetzen, die Regelungen über die Datenverarbeitung von Patientendaten durch Krankenhäuser treffen, nichts anderes bestimmt ist.

Das LDSG BB gilt gemäß § 2 Abs. 1 LDSG BB für öffentliche Stellen, die personenbezogene Daten verarbeiten. Das LDSG BB definiert die öffentlichen Stellen als Behörden, Einrichtungen oder sonstige öffentlichen Stellen des Landes, die Gemeinden und Gemeindeverbände sowie für die sonstigen der Aufsicht des Landes oder der Gemeinden oder Gemeindeverbände unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen.

Nach § 2 Abs. 3 LDSG BB findet das LDSG BB keine Anwendung, soweit öffentliche Stellen nach Absatz 1 am Wettbewerb teilnehmen und personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten. Für diese Stellen gelten insoweit die auf nicht-öffentliche Stellen anzuwendenden Vorschriften. Gemäß § 2 Abs. 4 gelten öffentliche Stellen des Landes, die als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen als nicht-öffentliche Stellen. Im Vergleich zu anderen Bundesländern stellt sich die Frage, weshalb neben der Wettbewerbsteilnahme in § 2 Abs. 3 LDSG BB weitere Voraussetzungen gefordert werden. Das LDSG BB nimmt eine Unterscheidung zwischen einer öffentlichen Stelle nach §§ 2 Abs. 1, Abs. 3 LDSG BB und einer öffentlichen Stelle als öffentlich-rechtliches Unternehmen nach § 2 Abs. 4 LDSG BB vor. Öffentliche Stellen, die als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten bereits nach § 2 Abs. 4 LDSG BB als nicht-öffentliche Stellen. Nimmt also eine öffentlich-rechtliche Stelle gerade nicht als öffentlich-rechtliches Unternehmen am Wettbewerb teil, so

[221] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 151 ff.

bedarf es der weiteren Voraussetzungen des § 2 Abs. 3 LDSG BB. Der umfassendere Anwendungsbereich des § 2 Abs. 1 LDSG BB wird somit durch § 2 Abs. 3 LDSG BB wieder eingeschränkt.

Nach obigen Ausführungen nehmen grundsätzlich alle Krankenhäuser am Wettbewerb teil. Fraglich ist, ob auf öffentliche Krankenhäuser als öffentlich-rechtliche Unternehmen § 2 Abs. 4 LDSG BB oder als öffentliche Stelle nach § 2 Abs. 1 LDSG BB der § 2 Abs. 3 LDSG BB mit den weiteren Voraussetzungen Anwendung findet. Der Begriff öffentlich-rechtliches Unternehmen ist im LDSG BB nicht definiert worden. Nach der hier vertretenen Auffassung ist ein öffentlich-rechtliches Unternehmen ein solches, das unabhängig von seiner Rechtsform, grundsätzlich wirtschaftliche Ziele und Zwecke verfolgt. Dies lässt sich damit begründen, dass § 2 Abs. 3 LDSG BB andere öffentliche Stellen mit einem öffentlich-rechtlichen Unternehmen gleichsetzt, soweit diese wirtschaftliche Ziele oder Zwecke verfolgen. Diese Stellen verfolgen diese also grundsätzlich nicht. Krankenhäuser in privater Trägerschaft verfolgen grundsätzlich wirtschaftliche Ziele und Zwecke, sodass man auch bei öffentlichen Krankenhäusern die Verfolgung solcher bejahen kann. Öffentliche Krankenhäuser sind als öffentlich-rechtliche Unternehmen anzusehen. Somit findet § 2 Abs. 4 LDSG BB Anwendung. Lehnt man diese Ansicht hingegen ab, so sind auch die weiteren Voraussetzungen des § 2 Abs. 3 LDSG BB erfüllt. Es ist davon auszugehen, dass die personenbezogenen Daten zu wirtschaftlichen Zielen oder Zwecken verarbeitet werden. Nach dem Wortlaut wird gerade nicht verlangt, dass die Daten selbst als Ware gehandelt werden. Es genügt, dass die Verarbeitung wirtschaftlichen Zwecken dient, was erfüllt ist, wenn die Daten im Rahmen der im Wettbewerb getätigten Behandlung verarbeitet werden. Zudem sind wesentliche Teile der Daten auch für die Abrechnung mit den Krankenkassen (§ 301 SGB V) relevant.[222]

Fraglich ist, welche Regelungen mit „als die auf nicht-öffentliche Stellen anzuwendenden Vorschriften" in §§ 2 Abs. 3, Abs. 4 LDSG BB gemeint sind. Ein Verweis auf andere Gesetze zur Regelung von nicht-öffentlichen Stellen wird im LDSG BB nicht direkt vorgenommen. § 18 Abs. 3 LDSG BB bestimmt, dass der oder die Landesbeauftragte auch zuständige Aufsichtsbehörde nach § 40 BDSG für die Datenverarbeitung nicht-öffentlicher Stellen im Land Brandenburg ist. Vergleichbare Regelungen in anderen Bundesländern zur Wettbewerbsteilnahme verweisen hier meistens komplett oder teilweise auf die Vorschriften des BDSG, was zur Folge hat, dass auf öffentliche Krankenhäuser - soweit sie am Wettbewerb teilnehmen – und auf Krankenhäuser in privater Trägerschaft dieselben Vorschriften Anwendung finden. Es ist daher davon auszugehen, dass nach dem Willen des Gesetzgebers bei Vorliegen der Voraussetzungen der §§ 2 Abs. 3, Abs. 4 LDSG BB die Vorschriften des BDSG anzuwenden sind.

Ergebnis: Auf alle öffentlichen Krankenhäuser ist vorrangig das KHEG BB anwendbar. Nachrangig finden das LDSG BB und außerhalb der Öffnungsklauseln die DSGVO direkt Anwendung. Das LDSG BB findet jedoch keine Anwendung, soweit die Krankenhäuser als öffentlich-rechtli-

[222] Im Ergebnis finden auf Krankenhäuser die Vorschriften über nicht-öffentliche Stellen Anwendung. Interessant könnte diese Unterscheidung hinsichtlich der Regelung über die Aufsichtsbehörde sein. § 2 Abs. 4 LDSG BB verweist komplett auf die Vorschriften über nicht-öffentliche Stellen, wohingegen § 2 Abs. 3 LDSG BB nur „insoweit" auf diese verweist. Die Aufsichtsbehörde wäre daher bei § 2 Abs. 4 LDSG wohl nach § 40 BDSG und bei § 2 Abs. 3 LDSG wohl nach dem LDSG zu bestimmen.

ches Unternehmen am Wettbewerb teilnehmen oder als öffentliche Stelle am Wettbewerb teilnehmen und personenbezogene Daten zu wirtschaftlichen zwecken oder Zielen verarbeiten. Dann gelten nachrangig das BDSG und außerhalb der Öffnungsklauseln die DSGVO direkt.

Krankenhäuser privater Träger

Die vorrangige Geltung des KHEG BB und die nachrangige Geltung des LDSG sowie die direkte Anwendung der DSGVO im Übrigen, also außerhalb von Öffnungsklauseln, stimmt für Krankenhäuser in privater Trägerschaft mit deren Geltung bei öffentlichen Kliniken überein.

Das BDSG gilt somit für private Kliniken bei Patientendaten nicht unmittelbar, weil der Landesgesetzgeber diesen Bereich in § 27 Abs. 1 KHEG BB einschließlich der Anordnung der subsidiären Geltung des LDSG BB an sich gezogen hat. Hiergegen könnte man zwar verfassungsrechtliche Bedenken im Hinblick auf die Gesetzgebungskompetenz des Landes in Abgrenzung zu jener des Bundes vorbringen. Vollkommen unvertretbar erscheint das Vorgehen des Landesgesetzgebers hier jedoch aufgrund einer möglichen Annexgesetzgebungskompetenz im Gesundheitsbereich nicht. Daher soll der Wortlaut des § 27 Abs. 1 KHEG BB als gültig zugrunde gelegt werden.

Auch hier ist ein Verweis auf das BDSG über §§ 2 Abs. 3, Abs. 4 LDSG BB möglich. Nach der hier vertretenen Auffassung ist auch hier § 2 Abs. 4 LDSG BB und nicht § 2 Abs. 3 LDSG BB einschlägig. Bei den privaten Krankenhäusern ist eine Verarbeitung der personenbezogenen Daten zu wirtschaftlichen Zielen und Zwecken erst recht zu bejahen. Der Begriff der Wirtschaftlichkeit setzt nicht zwingend eine Gewinnerzielungsabsicht voraus. Es genügt wohl eine Einnahmeerzielungsabsicht zur Kostendeckung, denn selbst gemeinnützige Häuser – gleich ob freigemeinnützig oder kirchlich – dürfen gewisse Gewinne erzielen. Sie dürfen diese lediglich nicht an ihre Gesellschafter ausschütten.

Öffnungsklausel für kirchliche Träger?

Mit § 25 KHEG BB besteht eine Öffnungsklausel zur Regelung des Datenschutzes in Krankenhäusern von Religionsgemeinschaften. Nach § 25 Abs. 1 KHEG BB gelten die Regelungen zum Datenschutz nicht für Krankenhäuser, die von Religionsgemeinschaften oder diesen gleichgestellten oder ihnen zuzuordnenden Einrichtungen betrieben werden. Die Religionsgemeinschaften haben diese in eigener Zuständigkeit zu schaffen. Nach § 25 Abs. 2 KHEG BB muss hierbei sichergestellt sein, dass die Standards des Datenschutzes nicht hinter den ansonsten geltenden staatlichen Vorschriften zum Datenschutz zurückbleiben.

Zusammenfassung

Auf alle Krankenhäuser gelten vorrangig das KHEG BB und nachrangig das LDSG BB, was wiederum über die Wettbewerbsklausel auf das BDSG verweist. Außerhalb der Anwendung der Öffnungsklauseln gilt die DSGVO unmittelbar. Es besteht eine Öffnungsklausel für kirchliche Krankenhäuser in § 25 KHEG BB.

Vorschriften zur Auftragsverarbeitung[223]

In Bezug auf die Auftragsverarbeitung enthält das KHEG BB keine Regelung.

[223] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 272

Nach § 27 Abs. 1 KHEG BB sind daher insoweit die Vorschriften des LDSG BB und der DSGVO zu beachten. § 24 LDSG BB gibt nicht abschließend Maßnahmen zum Schutze der personenbezogenen Daten nach Art. 9 Abs. 1 DSGVO vor. § 24 S. 2 Nr. 4 LDSG BB führt aus, dass eine solche Maßnahme bei Auftragsverarbeitern die Beschränkung des Zugangs zu den personenbezogenen Daten sein kann. Mangels weiterer Ausführungen zur Auftragsverarbeitung in beiden Gesetzen ist nach § 27 Abs. 1 KHEG BB im Übrigen auf die Vorgaben des Art. 28 DSGVO abzustellen.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

Das LDSG BB enthält in § 24 LDSG BB eine Vorschrift zur Verarbeitung besonderer Kategorien personenbezogener Daten mit einer Regelung zu technischen und organisatorischen Maßnahmen.

Nach § 24 S. 1 LDSG BB sind von der oder dem Verantwortlichen angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorzusehen, wenn auf der Grundlage des LDSG BB besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO verarbeitet werden.

Gemäß § 24 S. 2 LDSG BB können unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen dazu insbesondere gehören:

1. technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt,
2. Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind,
3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der öffentlichen Stelle und von Auftragsverarbeitern,
5. die Pseudonymisierung personenbezogener Daten,
6. die Verschlüsselung personenbezogener Daten,
7. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen, einschließlich der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
8. die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung und
9. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung personenbezogener Daten für andere Zwecke die Einhaltung des LDSG sowie der DSGVO sicherstellen.

Die Regelung des LDSG BB entspricht im Wesentlichen der Regelung des LDSG BW. Auf die obigen Ausführungen wird entsprechend verwiesen. Der einzige Unterschied besteht darin,

dass sich die Vorschrift des § 24 LDSG BB nicht auf die Datenverarbeitung bezieht, sondern nur Vorgaben an den Verantwortlichen bestimmt. Es stellt sich daher die Frage, ob die Vorgaben des § 24 LDSG BB entweder unmittelbar, mittelbar oder keine Anwendung auf den Auftragsverarbeiter finden. Gegen eine unmittelbare Anwendung spricht der Wortlaut des § 24 LDSG BB, da ausschließlich von der oder dem Verantwortlichen gesprochen wird. Auch der Begriff der Übermittlung in § 24 S. 2 Nr. 9 LDSG BB bezieht den Auftragsverarbeiter wohl nicht mit ein. Im alten BDSG wurde zwischen Auftragsverarbeitung und Übermittlung unterschieden. Eine Übermittlung lag dann vor, wenn der Empfänger eigenständig und somit nicht auf Weisung des Übermittlers die Daten verwenden konnte, was die Auftragsverarbeitung gerade nicht umfasste. Es ist davon auszugehen, dass der Gesetzgeber bei der Neufassung des § 24 S. 2 Nr. 9 LDSG BB wohl an dieser Unterscheidung festhält. Eine unmittelbare Anwendung des § 24 LDSG BB ist daher wohl nicht gegeben. Es kommt aber eine mittelbare Anwendung in Betracht. Der oder die Verantwortliche wird die Einhaltung der Vorschriften des § 24 LDSG BB praktisch wohl nur gewährleisten können, wenn er seinerseits die Auftragsverarbeiter zumindest vertraglich den Vorgaben des § 24 LDSG BB unterwirft. Über diese vertragliche Unterwerfung des Auftragsverarbeiters fände der § 24 LDSG BB somit zumindest mittelbare Anwendung auf den Auftragsverarbeiter.

3.4.5 Bremen

Auf Krankenhäuser anwendbare Datenschutzvorschriften[224]

Krankenhäuser öffentlicher Träger

Nach § 1 S. 1 LKHG HB gilt dieses Gesetz für alle Krankenhäuser im Lande Bremen, soweit nichts anderes bestimmt ist. Gemäß § 1 S. 2 LKHG HB gelten die Vorschriften des Dritten Abschnitts (Krankenhausförderung) nur für Krankenhäuser, die nach dem Zweiten Abschnitt (Krankenhausplan) in den Krankenhausplan aufgenommen worden sind. Der Datenschutz wird in Abschnitt 8 behandelt, sodass das LKHG HB grundsätzlich für alle Krankenhäuser gilt.

§ 36 LKHG HB behandelt den Anwendungsbereich der Datenschutzvorschriften. Gemäß § 36 Abs. 1 S. 1 LKHG HB finden die datenschutzrechtlichen Vorschriften des LKHG HB keine Anwendung, soweit das Recht der Europäischen Union, im Besonderen die DSGVO, unmittelbar gilt. Nach § 36 Abs. 1 S. 2 LKHG HB finden die Vorschriften des Bremischen Ausführungsgesetzes zur DSGVO Anwendung. Nach § 36 Abs. 2 LKHG HB gelten die Datenschutzvorschriften des LKHG HB nicht für Krankenhäuser oder Teile eines Krankenhauses, deren Träger der Bund ist oder die dem Straf- und Maßregelvollzug dienen.

Gilt subsidiär das LDSG oder das BDSG?

Das bisherige Bremische Datenschutzgesetz (LDSG HB a.F.) ist mit Ablauf des 24.05.2018 außer Kraft getreten.[225] Zum 25.05.2018 trat das Bremische Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (DSGVOAG HB) in Kraft.[226] Gemäß § 2 Abs. 7 DSGVOAG HB gehen andere

[224] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 156 ff.

[225] Bremische Datenschutzgesetz (BremDSG) vom 23.12.1977, zuletzt geändert durch Gesetz vom 25.06.2013 (Brem.GBl. S. 351); letztlich aufgehoben. durch § 26 S. 2 des Gesetzes vom 8. Mai 2018 (Brem.GBl. S. 131).

[226] Dieses Gesetz wird in den Abbildungen und Tabellen dieses Gutachtens teils auch mit LDSG angesprochen.

Rechtsvorschriften des Landes über die Verarbeitung personenbezogener Daten den Vorschriften des DSGVOAG HB vor. Das DSGVOAG HB findet jedoch Anwendung, wenn die Vorschriften des vorgehenden Gesetzes den Sachverhalt nicht oder nicht abschließend regeln. Dabei handelt es sich für Krankenhäuser um das LKHG HB. Mit dieser Vorschrift korrespondiert auch § 36 Abs. 1 S. 2 LKHG HB, wonach das DSGVOAG HB ergänzend Anwendung findet.

Nach § 2 Abs. 1 DSGVOAG HB gilt dieses Gesetz nur für öffentliche Stellen im Sinne dieses Gesetzes. Öffentliche Stellen sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Landes, einer Gemeinde oder sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Nach § 2 Abs. 2 S. 1 DSGVOAG HB gelten auch hier nicht-öffentliche Stellen als öffentliche Stelle, soweit diese Aufgaben der öffentlichen Verwaltung wahrnehmen. Öffentliche Stellen gelten gemäß § 2 Abs. 3 DSGVOAG HB allerdings als nicht-öffentliche Stellen, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Gilt eine Stelle als nicht-öffentlich im Sinne des DSGVOAG HB, so sollen die Regelungen des BDSG Anwendung finden.[227]

Das DSGVOAG HB gilt somit für Krankenhäuser mit öffentlicher Trägerschaft, soweit keine Wettbewerbsteilnahme vorliegt. Bei Wettbewerbsteilnahme gelten insoweit die Vorschriften des BDSG.

Ergebnis: Mithin gilt für öffentliche Krankenhäuser in Bremen vorrangig das LKHG HB und nachrangig das DSGVOAG HB. Im Übrigen, d.h. außerhalb der Öffnungsklauseln der DSGVO, gilt diese unmittelbar.

Krankenhäuser privater Träger

Die vorrangige Geltung des LKHG HB sowie die nachrangige Geltung des DSGVOAG HB, sowie die direkte Anwendung der DSGVO außerhalb der Öffnungsklauseln, stimmt für Krankenhäuser in privater Trägerschaft mit deren Geltung bei öffentlichen Kliniken überein. Das LKHG HB verweist in seinem § 36 Abs. 1 S. 2 LKHG HB HB auf das DSGVOAG HB. Dies wird damit begründet, dass die Krankenhäuser im Land Bremen unabhängig davon, welche Rechtsform sie haben und ob sie in öffentlicher oder privater Trägerschaft stehen, durch die Sicherstellung der Krankenhausversorgung Aufgaben der öffentlichen Verwaltung vornehmen.[228]

Für Krankenhäuser in privater Trägerschaft gilt somit primär das LKHG HB und nachrangig das DSGVOAG HB sowie im Übrigen die DSGVO. Nimmt ein Krankenhaus in privater Trägerschaft am Wettbewerb teil, so gilt es insoweit als nicht-öffentliche Stelle und das BDSG wäre anwendbar.

Ergebnis: Das LKHG HB gilt für Krankenhäuser in privater Trägerschaft vorrangig. Das DSGVOAG HB findet grundsätzlich nachrangig Anwendung, soweit das private Krankenhaus nicht

[227] Senatsvorlage zum Entwurf eines Bremischen Ausführungsgesetzes zur EU-Datenschutzverordnung vom 30. Januar 2018, S. 2.

[228] Mitteilung des Senats an die Bremische Bürgerschaft, S. 28.

am Wettbewerb teilnimmt. Im Übrigen, außerhalb der Öffnungsklauseln, gilt die DSGVO unmittelbar.[229]

Öffnungsklausel für kirchliche Träger?

Nach § 36 Abs. 3 LKHG HB gelten die Datenschutzvorschriften des LKHG HB für Krankenhäuser, die von kirchlichen oder religiösen Vereinigungen oder Gemeinschaften oder diesen zuzuordnenden Einrichtungen betrieben werden, nur soweit die kirchlichen oder religiösen Vereinigungen oder Gemeinschaften keinen Regeln unterliegen, die den Anforderungen des Art. 91 DSGVO genügen.

Zusammenfassung

Im Ergebnis gilt für alle Krankenhäuser in Bremen vorrangig das LKHG HB und nachranging das DSGVOAG HB mit Ausnahme von dessen Wettbewerbsklausel. Im Übrigen, d.h. außerhalb der Nutzung von Öffnungsklauseln der DSGVO, gilt diese unmittelbar.

Auf die Sonderregeln des ÖGDG HB für die psychiatrischen Behandlungszentren wird vorliegend nicht weiter eingegangen.[230]

Vorschriften zur Auftragsverarbeitung[231]

Nach § 41 Abs. 1 LKHG HB darf der oder die Verantwortliche nach § 38 Abs. 2 LKHG HB die Verarbeitung von Patientendaten einem Auftragsverarbeiter insbesondere übertragen, wenn

1. Störungen im Betriebsablauf, insbesondere in der Patientenversorgung sonst nicht vermieden werden können, oder
2. die Datenverarbeitung dadurch erheblich kostengünstiger gestaltet werden kann, oder
3. die Datenverarbeitung vom Krankenhaus nicht oder nur mit einem großen Aufwand geleistet werden könnte, oder
4. Patientenakten oder ähnliche Unterlagen in Papierform einzuscannen und zu digitalisieren sind.

§ 38 Abs. 2 LKHG HB bestimmt, dass die in dem Krankenhaus tätigen Mitarbeiterinnen und Mitarbeiter Patientendaten nur einsehen und verarbeiten dürfen, soweit dies für die rechtmäßige Erfüllung der ihnen obliegenden Aufgaben erforderlich ist.

Gemäß § 41 Abs. 2 S. 1 LKHG HB hat der Auftragsverarbeiter die Datenschutzbestimmungen dieses Gesetzes und die nach § 203 StGB geltende Schweigepflicht einzuhalten. Nach § 41 Abs. 2 S. 2 LKHG HB regelt Art. 28 DSGVO die Ausgestaltung der Datenverarbeitung durch den Auftragsverarbeiter.

Das DSGVOAG HB enthält – abgesehen von Vorgaben für technische und organisatorische Maßnahmen in § 11 DSGVOAG HB – keine weiterführenden Regelungen zur Auftragsverarbeitung.

Im Übrigen ist auch hier Art. 28 DSGVO anzuwenden.

---

[229] Europarechtskonforme Nutzung der in der DSGVO bestehenden Öffnungsklauseln jeweils vorausgesetzt.

[230] Vgl. § 36 ÖGDG (Datenverarbeitung für Forschungszwecke) und § 36a ÖGDG (Datenverarbeitung im Auftrag).

[231] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 273.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

§ 11 DSGVOAG HB enthält eine Vorschrift zur Verarbeitung besonderer Kategorien personenbezogener Daten mit einer Regelung zu technischen und organisatorischen Maßnahmen. § 11 Abs. 1 DSGVOAG HB behandelt die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten, wozu auch solche über die Gesundheit zählen.

Nach § 11 Abs. 2 S. 1 sind in den Fällen des § 11 Abs. 1 DSGVOAG HB und in den weiteren Fällen der Verarbeitung besonderer Kategorien personenbezogener Daten nach Abschnitt 4 DSGVOAG HB angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte, Freiheit und Interessen der betroffenen Personen vorzusehen.

Gemäß § 11 Abs. 2 S. 2 DSGVOAG HB können unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen insbesondere gehören:

1. technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt,
2. Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind,
3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der öffentlichen Stelle und von Auftragsverarbeitern,
5. die Pseudonymisierung personenbezogener Daten,
6. die Verschlüsselung personenbezogener Daten,
7. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen, einschließlich der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
8. die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung und
9. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung personenbezogener Daten für andere Zwecke die Einhaltung des LDSG sowie der DSGVO sicherstellen.

Gemäß § 11 Abs. 2 S. 3 DSGVOAG HB sollen der Verantwortliche und der Auftragsverarbeiter insbesondere die Maßnahmen gemäß §§ 11 Abs. 2 S. 2 Nr. 1, Nr. 4, Nr. 7, Nr. 8, Nr. 9 DSGVOAG HB treffen.

§ 11 Abs. 1 DSGVOAG HB stellt eine Wiederholung und Konkretisierung von Art. 9 Abs. 2 DSGVO und dort insbesondere Buchst. b, h und i dar. Ist der Anwendungsbereich des § 11 Abs. 1 DSGVOAG HB eröffnet – werden also besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO verarbeitet – sind die Maßnahmen nach § 11 Abs. 2 DSGVOAG HB zu treffen. Aus § 11 Abs. 2 S. 3 DSGVOAG HB ergibt sich, dass die Vorgaben des § 11

Abs. 2 DSGVOAG HB sowohl für den Verantwortlichen als auch für den Auftragsverarbeiter gelten sollen. Greifen § 11 Abs. 1 DSGVOAG HB oder andere Fälle der Verarbeitung besonderer Kategorien des Abschnitts nicht ein, so richten sich die Maßnahmen wiederum allein nach Art. 32 DSGVO.

Die Verarbeitung von Patientendaten unterfällt dem Anwendungsbereich des § 11 Abs. 1 Nr. 3 DSGVOAG HB.

Die Vorgaben für technische und organisatorische Maßnahmen ergeben sich bei der Verarbeitung von Patientendaten aus § 11 Abs. 2 DSVOAG HB und im Übrigen aus Art. 32 DSGVO.

3.4.6 Hamburg

Auf Krankenhäuser anwendbare Datenschutzvorschriften[232]

Krankenhäuser öffentlicher Träger

Nach § 2 LKHG HH gilt dieses Gesetz für alle Krankenhäuser, die an der allgemeinen stationären Versorgung der Bevölkerung teilnehmen. Der Patientendatenschutz ist dort im Zweiten Abschnitt, also in den §§ 7 ff. LKHG HH geregelt.

Eine Klinik nimmt jedenfalls dann an der allgemeinen Versorgung der Bevölkerung teil, wenn sie gemäß § 108 SGB V zur Abrechnung mit den Krankenkassen zugelassen ist. Dies setzt eine Aufnahme in den Landeskrankenhausplan oder den Abschluss eines Versorgungsvertrags mit den Krankenkassen voraus. Das Merkmal der Teilnahme an der allgemeinen Versorgung könnte dagegen zu verneinen sein, wenn keine Zulassung zur GKV-Abrechnung nach § 108 SGB V besteht, weil diese Kliniken lediglich Privatpatienten behandeln, welche nur einen Anteil von ca. 10 % an der Bevölkerung ausmachen. Eine Förderfähigkeit oder gar eine Förderung nach dem KHG ist zwar keine explizite Voraussetzung für die geforderte Teilnahme an der Versorgung. Nach § 5 Abs. 1 Nr. 2 KHG ist eine Klinik jedoch dann nicht förderfähig, wenn sie nicht nach § 67 AO steuerbegünstigt ist. Dies ist der Fall, wenn bei ihr weniger als 40 % der Belegungstage auf Patienten entfallen, bei denen die Entgelte für allgemeine Krankenhausleistungen (§ 7 KHEntgG, § 10 BPflV) berechnet werden oder nicht höher als diese ausfallen. Bei einer Klinik, die diese 40 %-Marke nicht unterschreitet, kann man damit noch von einer Teilnahme an der allgemeinen Versorgung ausgehen. Lediglich für reine Privatkliniken nach § 5 Abs. 1 Nr. 2 KHG ist dies zu verneinen, welche aber von öffentlichen Trägern in aller Regel nicht betrieben werden.

Gilt subsidiär das LDSG oder das BDSG?

Gemäß § 7 Abs. 3 LKHG HH gelten die allgemeinen Datenschutzvorschriften ergänzend. Dafür kommen das LDSG HH, das BDSG und ferner die DSGVO in Betracht.

Das LDSG HH gilt nach § 2 Abs. 1 LDSG HH für öffentlich-rechtlich organisierte Einrichtungen des Landes, der Landesaufsicht unterstehende juristische Personen des öffentlichen Rechts und deren öffentlich-rechtlich organisierte Einrichtungen. Werden Krankenhäuser in öffentlicher Trägerschaft in einer solchen Rechtsform betrieben, fallen sie somit in den Anwendungsbereich des LDSG HH.

[232] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 162 ff.

Dann ist jedoch auch § 2 Abs. 3 LDSG HH zu beachten: Wenn eine Stelle nach § 2 Abs. 1 LDSG HH als Unternehmen am Wettbewerb teilnimmt, sind auf diese, unbeschadet anderer Rechtsgrundlagen, die Vorschriften der DSGVO sowie des BDSG über nichtöffentliche Stellen in ihrer jeweils geltenden Fassung anzuwenden. Grundsätzlich nehmen auch Krankenhäuser am Wettbewerb teil.[233] Von einer Wettbewerbsteilnahme ist gerade im Behandlungsbereich auszugehen. Dem Merkmal der Unternehmenseigenschaft kommt dabei zumindest im Krankenhausbereich wohl keine weitere Bedeutung zu. Dabei kann es sich auch um Eigenbetriebe oder juristische Personen des öffentlichen Rechts handeln, die ebenfalls unter die Definition der öffentlichen Stellen nach § 2 Abs. 1 LDSGH HH fallen. Die öffentlich-rechtliche Eigenschaft solcher öffentlichen Stellen schließt die das Vorliegend eines Wettbewerbsunternehmens nicht aus, weil ansonsten § 2 Abs. 3 LDSG HH keinen Sinn machen würde. Es kann für ein Wettbewerbsunternehmen daher nicht gefordert werden, dass die öffentliche Stelle in privater Rechtsform organisiert ist.

Dies ergibt sich im Umkehrschluss aus § 2 Abs. 2 LDSG HH zeigt, der für privatrechtliche Vereinigungen, an denen die Hansestadt Hamburg oder eine ihrer Aufsicht unterstehende juristische Person beteiligt ist, immer auf die Vorschriften der DSGVO sowie diejenigen des BDSG für nicht-öffentliche Stellen verweist. In beiden Fällen, also bei Vorliegen einer öffentlichen Stelle in privater Rechtsform (§ 2 Abs. 2 LDSG HH) oder eines öffentlich-rechtlichen Wettbewerbsunternehmens (§ 2 Abs. 3 LDSG HH), verweist das LDSG HH auf die Regelungen der DSGVO sowie diejenigen des BDSG für nicht-öffentliche Stellen. Somit finden die genannten Regeln auf alle öffentlichen Krankenhäuser in Hamburg Anwendung.

Im Fall einer öffentlichen Stelle in privater Rechtsform als Träger eines Krankenhauses in Hamburg würde das LDSG HH jedoch nicht gelten, wenn es sich um eine öffentliche Stelle des Bundes nach § 2 Abs. 3 BDSG handelt, was eine absolute Bundesmehrheit oder eine Tätigkeit in mehreren Ländern voraussetzt. Erst recht würde das LDSG HH nicht gelten, wenn es sich um eine öffentlich-rechtlich organisierte Stelle des Bundes wie bspw. das Bundeswehrkrankenhaus Hamburg handelt.

Es gelten dann das LKHG HH vorrangig, Teile des LDSG HH nachrangig und im Übrigen Teile des BDSG und außerhalb der Nutzung von Öffnungsklauseln die DSGVO direkt.

Ergebnis: Die Datenschutzregeln des LKHG HH gelten vorrangig für alle Krankenhäuser, die an der allgemeinen stationären Versorgung der Bevölkerung teilnehmen. Für diese Kliniken gelten nachrangig, außerhalb der Anwendung der genutzten Öffnungsklauseln, die DSGVO sowie die Vorschriften des BDSG für nicht-öffentliche Stellen.

Krankenhäuser privater Träger

Das LKHG HH gilt – wie bereits zu den öffentlichen Krankenhäusern ausgeführt – gemäß § 2 LKHG HH für alle Krankenhäuser, die an der allgemeinen stationären Versorgung der Bevölkerung teilnehmen. Dies gilt auch für den Abschnitt zum Patientendatenschutz (§§ 7 ff. LKHG HH). Zur Teilnahme an der allgemeinen Versorgung der Bevölkerung kann auf die vorigen Ausführungen zu öffentlichen Kliniken verwiesen werden. Lediglich für reine Privatkliniken nach § 5 Abs. 1 Nr. 2 KHG wird dies zu verneinen sein; für diese gilt dann das LKHG HH nicht, sondern

[233] Zur vergleichbaren Rechtslage in Baden-Württemberg mit entspr. Argumenten, s.o. S. 80 f.

die Vorschriften des BDSG für nicht-öffentliche Stellen sowie außerhalb der Öffnungsklauseln die DSGVO direkt.

Gilt subsidiär das LDSG oder das BDSG?

Ist auf eine Klinik das LKHG HH anwendbar, weil sie an der allgemeinen stationären Versorgung der Bevölkerung teilnimmt, so gelten nach § 7 Abs. 3 LKHG HH die allgemeinen Datenschutzvorschriften ergänzend. Bei einer Klinik in privater Trägerschaft handelt es sich dabei um die Vorschriften des BDSG für nicht-öffentliche Stellen sowie, außerhalb der Anwendung von Öffnungsklauseln, um die DSGVO.

Ergebnis: Das LKHG HH gilt vorrangig für alle Krankenhäuser in Hamburg, die an der allgemeinen stationären Versorgung der Bevölkerung teilnehmen. Bei privaten Kliniken ist dies zumindest dann gegeben, wenn sie nach § 108 SGB V zur GKV-Abrechnung berechtigt sind (Landeskrankenhausplan oder Versorgungsvertrag). Eine KHG-Förderung oder Förderfähigkeit ist hierfür nicht erforderlich. Maßgeblich dürfte aber die 40 %-Marke nach § 67 AO sein. Auf private Kliniken sind außerdem das BDSG und außerhalb der Öffnungsklauseln die DSGVO anzuwenden, entweder nachrangig nach dem LKHG HH oder – für reine Privatkliniken – ausschließlich.

Öffnungsklausel für kirchliche Träger?

Die Datenschutzvorschriften des LKHG HH gelten nach dessen § 7 Abs. 4 für kirchliche Krankenhäuser nur, soweit die Religionsgesellschaften keine gleichwertigen Regelungen getroffen haben.

Zusammenfassung

Das LKHG HH gilt mit Vorrang für alle öffentlichen und privaten Krankenhäuser, die an der allgemeinen stationären Versorgung der Bevölkerung teilnehmen. Für diese Kliniken gelten nachrangig die Vorschriften des BDSG für nicht-öffentliche Stellen und außerhalb der Anwendung von Öffnungsklauseln die DSGVO. Für reine Privatkliniken gelten allein die DSGVO sowie die Regelungen des BDSG für nicht-öffentliche Stellen. Es besteht eine Öffnungsklausel für kirchliche Krankenhäuser.

Vorschriften zur Auftragsverarbeitung[234]

Die ursprüngliche Regelung des § 9 LKHG HH, welche die Auftragsverarbeitung geregelt hat, wurde mittlerweile aufgehoben. Zur Begründung führte der Gesetzgeber an, dass die Regelung zur Datenverarbeitung nunmehr direkt in Art. 28 DSGVO erfolgt.[235] Dies geschieht wohl vor dem Hintergrund, dass mit der Neufassung des § 203 StGB und der Einführung der DSGVO eigenständige Regelungen der Landesgesetzgeber nicht mehr notwendig sind. Im Gegensatz zu anderen Landesgesetzgebern unterließ es Hamburg hier die Vorschrift entsprechend anzupassen oder eigene Vorgaben zu erlassen. Entsprechend ist auch keine Regelung im LDSG HH zu finden. Die Verarbeitung von Patientendaten im Auftrag richtet sich also nur nach Art. 28 DSGVO.

[234] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 273 f.

[235] Hamburger Senat: Mitteilung des Senats an die Bürgerschaft: „Entwurf eines Gesetzes zur Anpassung gesundheitsrechtlicher Vorschriften an die Verordnung (EU) 2016/679", Drucksache 21/11987 vom 13.02.18, S. 8.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

Das LDSG HH enthält keine Regelung mit einer Aufzählung von technischen und organisatorischen Maßnahmen. Gemäß § 1 LDSG HH gilt das LDSG HH nur als Ergänzung zu den Regelungen der DSGVO. Soweit keine Regelungen bestimmt sind, gilt diese unmittelbar. Die technischen und organisatorischen Maßnahmen bei der Verarbeitung von Patientendaten richten sich allein nach Art. 32 DSGVO.

3.4.7 Hessen

Auf Krankenhäuser anwendbare Datenschutzvorschriften[236]

Krankenhäuser öffentlicher Träger

Gemäß § 2 Abs. 1 LKHG HE gilt dieses Gesetz grundsätzlich für alle Krankenhäuser, die der allgemeinen vollstationären, teilstationären und ambulanten Versorgung dienen, soweit nichts anderes bestimmt ist. Ein Krankenhaus dient der allgemeinen Versorgung im genannten Sinne, wenn es – ähnlich der Terminologie des LKHG HH[237] – an der allgemeinen Versorgung der Bevölkerung teilnimmt.

Dies ist jedenfalls gegeben, wenn das Krankenhaus gemäß § 108 SGB V zur Abrechnung mit den Krankenkassen zugelassen ist. Voraussetzung hierfür ist deren Aufnahme in den Landeskrankenhausplan oder der Abschluss eines Versorgungsvertrags mit den Krankenkassen. Ausreichend ist jedoch auch vorliegend, dass das Krankenhaus die Bedingungen des § 67 AO erfüllt, also nicht als reine Privatklinik von der Förderfähigkeit nach § 5 Abs. 1 Nr. 2 KHG per se ausgeschlossen ist. Dies ist dann gegeben, wenn bei ihm 40 % oder mehr der Belegungstage auf Patienten entfallen, bei denen die Entgelte für allgemeine Krankenhausleistungen (§ 7 KHEntgG, § 10 BPflV) berechnet werden oder nicht höher als diese ausfallen. Davon ist bei öffentlichen Kliniken in der Regel auszugehen.

Der Datenschutz im Krankenhaus ist in § 12 LKHG HE geregelt.

Gilt subsidiär das LDSG oder das BDSG?

§ 12 Abs. 1 LKHG HE bestimmt, dass für Krankenhäuser die Bestimmungen der DSGVO sowie des LDSG HE abweichend von dessen § 2 Abs. 2 LDSG HE uneingeschränkt nach den Maßgaben der Abs. 2 bis 5 gelten.

Gemäß § 1 Abs.2, Abs. 3 LDSG HE gehen besondere Rechtsvorschriften dem LDSG HE vor. Für Krankenhäuser genießt damit auch mit Blick auf den Datenschutz das LKHG HE Vorrang. Dies wird auch durch § 12 Abs. 1 LKHG HE bestätigt, wonach die Absätze 2 bis 5 dieses Paragrafen vorrangig gelten.

Zu beachten ist dabei, dass gerade § 2 Abs. 2 LDSG HE auf Krankenhäuser gemäß § 12 Abs. 1 LKHG HE keine Anwendung findet. Soweit öffentlich-rechtliche Unternehmen in Landesträgerschaft am Wettbewerb teilnehmen, verweist die genannte Regelung des LDSG HE teilweise auf das BDSG. Für Krankenhäuser in Hessen verbleibt es aber – anders als nach den Regeln vieler

[236] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 167 ff.

[237] S. oben S. 114 f.

anderer Bundesländer – auch in diesen Fällen bei der von § 12 Abs. 1 LKHG HE angeordneten Geltung des LDSG HE ohne Verweis auf das BDSG.

Ergebnis: Für öffentliche Krankenhäuser gelten das LKHG HE vorrangig und das LDSG HE nachrangig, sowie – außerhalb der Öffnungsklauseln – die DSGVO direkt und zwar ohne dass es darauf ankäme, ob ein Krankenhaus ansonsten in den Anwendungsbereich des LDSG HE fiele. Dabei gilt der Verweis des LDSG HE für öffentlich-rechtliche Wettbewerbsunternehmen auf das BDSG für Krankenhäuser nicht.

Krankenhäuser privater Träger

Auch für Krankenhäuser in privater Trägerschaft, die nach § 2 Abs. 1 LKHG HE der allgemeinen Versorgung dienen, gilt – wie bei öffentlichen Kliniken – vorrangig das LKHG HE und nachrangig das LDSG HE. Das Merkmal der allgemeinen Versorgung ist wie bei öffentlichen Kliniken auszulegen und lediglich bei reinen Privatkliniken, welche weniger als 40 % ihrer Patienten zu GKV-Sätzen behandeln, zu verneinen. Zu beachten ist außerdem, dass nach § 12 Abs. 1 LKHG HE die Ausnahme des § 2 Abs. 2 LDSG HE für öffentlich-rechtliche Wettbewerbsunternehmen bei privaten Kliniken ohnehin nicht zum Tragen käme.

Für private Kliniken, welche nach § 2 Abs. 1 LKHG HE der allgemeinen Versorgung dienen, ist die Geltung des BDSG ausgeschlossen, weil der Landesgesetzgeber diesen Bereich mit § 12 Abs. 1 LKHG HE an sich gezogen hat. Dies bedeutet, dass in diesem Fall für die Aufsicht über Krankenhäuser privater Träger nach §§ 13 ff. LDSG HE der Landesdatenschutzbeauftragte zuständig ist.

Für reine Privatkliniken, die nach § 2 Abs. 1 LKHG HE nicht der allgemeinen Versorgung dienen, gilt dieses Gesetz nicht. Bei privaten Kliniken handelt es sich nicht um öffentliche Stellen nach § 2 Abs. 1 LDSG HE, so dass das LDSG HE auch nicht direkt anwendbar ist. Vielmehr gilt für private Kliniken, die nicht der allgemeinen Versorgung dienen, ausschließlich das BDSG sowie – außerhalb der Öffnungsklauseln - die DSGVO.

Ergebnis: Für private Kliniken, die der allgemeinen Versorgung der Bevölkerung dienen, gelten das LKHG HE vorrangig und das LDSG HE sowie – außerhalb von Öffnungsklauseln - die DSGVO nachrangig, und zwar ohne, dass es darauf ankäme, ob ein Krankenhaus ansonsten in den Anwendungsbereich des LDSG HE fiele. Das BDSG gilt für sie nicht nachrangig, auch nicht die Regelung zu Aufsichtsbehörden in § 40 BDSG. Die Aufsicht führt in diesem Fall der Landesdatenschutzbeauftragte nach §§ 13 ff. LDSG HE. Für private Kliniken, die nicht der allgemeinen Versorgung der Bevölkerung dienen, gelten weder das LKHG HE noch das LDSG HE, sondern das BDSG sowie – außerhalb der Öffnungsklauseln - die DSGVO.[238]

Öffnungsklausel für kirchliche Träger?

Nach § 12 Abs. 5 LKHG HE treffen die Religionsgemeinschaften für ihre Krankenhäuser in eigener Zuständigkeit Datenschutzregelungen, die denen des § 12 Abs. 1-4 LKHG HE entsprechen.

[238] Europarechtskonforme Nutzung der in der DSGVO bestehenden Öffnungsklauseln jeweils vorausgesetzt.

Zusammenfassung

Für öffentliche wie private Kliniken, die der allgemeinen Versorgung der Bevölkerung dienen, gelten das LKHG HE vorrangig und die DSGVO sowie das LDSG HE nachrangig, und zwar ohne dass es darauf ankäme, ob ein Krankenhaus ansonsten in den Anwendungsbereich des LDSG HE fiele. Die Verweisung des LDSG HE für öffentlich-rechtliche Wettbewerbsunternehmen auf das BDSG gilt nicht für Krankenhäuser. Das BDSG gilt für private Kliniken, die der allgemeinen Versorgung der Bevölkerung dienen, nicht nachrangig, auch nicht § 40 BDSG (Aufsichtsbehörde). Die Aufsicht über sie hat der Landesdatenschutzbeauftragte nach §§ 8 ff. LDSG HE. Für reine Privatkliniken, die nicht der allgemeinen Versorgung der Bevölkerung dienen, gelten weder das LKHG HE noch das LDSG HE, sondern lediglich das BDSG sowie die DSGVO. Es existiert eine Öffnungsklausel für kirchliche Krankenhäuser.

Vorschriften zur Auftragsverarbeitung[239]

Das LKHG HE enthält keine Regelungen für die Verarbeitung im Auftrag. Somit finden gemäß § 12 Abs. 1 LKHG HE neben der DSGVO die Vorschriften des LDSG HE Anwendung.

Die in § 57 LDSG HE geregelte Auftragsverarbeitung ist nicht anwendbar, da sie sich auf die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung von personenbezogenen Daten im Rahmen der Strafverfolgung oder Prävention von Straftaten bezieht, welche auf Krankenhäuser nicht anwendbar ist.

Gemäß § 3 Abs. 2 LDSG HE gelten als Auftragsverarbeiter auch Personen und Stellen, die im Auftrag Wartungsarbeiten und vergleichbare Hilfstätigkeiten bei der Verarbeitung personenbezogener Daten erledigen.

Im Übrigen findet Art. 28 DSGVO Anwendung.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

§ 20 LDSG HE enthält eine Vorschrift zur Verarbeitung besonderer Kategorien personenbezogener Daten mit einer Regelung zu technischen und organisatorischen Maßnahmen.

Nach § 20 Abs. 1 LDSG HE ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO abweichend von Art. 9 Abs. 1 DSGVO durch öffentliche Stellen unter anderem dann zulässig, wenn einer der dort genannten Fälle vorliegt, wozu auch die medizinische Versorgung gehört. In diesen Fällen sind gemäß § 20 Abs. 2 S. 1 LDSG HE angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen.

Gemäß § 20 Abs. 2 S. 2 LDSG HE können unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen insbesondere gehören:

1. technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt,

[239] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 274 f.

2. Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind,
3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der öffentlichen Stelle und von Auftragsverarbeitern,
5. die Pseudonymisierung personenbezogener Daten,
6. die Verschlüsselung personenbezogener Daten,
7. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen, einschließlich der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
8. die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung und
9. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung personenbezogener Daten für andere Zwecke die Einhaltung des LDSG sowie der DSGVO sicherstellen.

Nach § 20 Abs. 3 LDSG HE sind, wenn personenbezogene Daten nicht automatisiert verarbeitet werden, insbesondere Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

Vergleichbar mit dem LDSG von Bremen bestimmt auch das LDSG HE nur besondere Maßnahmen, wenn eine Verarbeitung besonderer Kategorien personenbezogener Daten vorliegt, die nicht bereits nach Art. 9 Abs. 1 DSGVO zulässig ist. Andernfalls verbleibt es bei der Anwendung des Art. 32 DSGVO für technische und organisatorische Maßnahmen. Die Vorschrift richtet sich wie in Brandenburg direkt an den Verantwortlichen. Eine mittelbare Anwendung auf den Auftragsverarbeiter hinsichtlich der technischen und organisatorischen Maßnahmen ist hier aber ebenfalls anzunehmen.

Die Verarbeitung von Patientendaten ist nach § 20 Abs. 1 Nr. 2 LDSG HE umfasst.

Die Vorgaben an die technischen und organisatorischen Maßnahmen bei der Verarbeitung von Patientendaten ergeben sich aus § 20 Abs. 2 LDSG HE und im Übrigen aus Art. 32 DSGVO.

3.4.8 Mecklenburg-Vorpommern

Auf Krankenhäuser anwendbare Datenschutzvorschriften[240]

Krankenhäuser öffentlicher Träger

Gemäß § 3 Abs. 1 S. 1 LKHG MV gilt dieses Gesetz für alle Krankenhäuser, die der allgemeinen akut stationären, teilstationären oder tagesklinischen Versorgung dienen, soweit nichts anderes bestimmt ist. Der Begriff des Dienens der allgemeinen Versorgung ist entsprechend dem LKHG HE auszulegen, also letztlich nur im Falle reiner Privatkliniken zu verneinen, die einen

[240] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 172 ff.

Anteil von Patienten, die nach GKV-Sätzen abgerechnet werden, von unter 40 % aufweisen (vgl. § 67 AO).

Die für Universitätsklinika geltenden Besonderheiten des § 3 Abs. 2 LKHG MV betreffen den Datenschutz nicht. Das LKHG MV ist somit auf alle Krankenhäuser sowohl in öffentlicher als auch in privater Trägerschaft anwendbar, sofern diese die genannten Voraussetzungen erfüllen. § 32 Abs. 1 S. 1 LKHG MV regelt, dass im Krankenhaus erhobene Patientendaten unabhängig von der Art ihrer Verarbeitung dem Datenschutz unterliegen.

Gilt subsidiär das LDSG oder das BDSG?

Gemäß § 32 Abs. 2 LKHG MV unterliegt die Verarbeitung von Patientendaten der DSGVO und ergänzend den datenschutzrechtlichen Bestimmungen das Abschnitts 7. Das Wort „ergänzend" lässt sich dahingehend auslegen, dass das LKHG MV vorrangig anzuwenden ist, soweit die Regelungen spezieller als die Regelungen der DSGVO sind. § 38 in Verbindung mit § 6 Abs. 4, Abs. 5 S. 2 und Abs. 6 des BDSG gelten entsprechend. Der Krankenhausträger ist dabei Verantwortlicher gemäß Art. 4 Nr. 7 der DSGVO.

Das LDSG MV findet gemäß §§ 2 Abs. 1, Abs. 2 LDSG MV für öffentliche Stellen im Sinne dieses Gesetzes Anwendung. Eine Subsidiaritätsklausel wie in anderen Bundesländern findet sich hier nicht.[241] Ziel dieses Gesetzes ist es gemäß § 1 LDSG MV die DSGVO zu ergänzen. In § 2 Abs. 5 LDSG MV besteht auch hier eine Ausschlussklausel für öffentliche Stellen, insoweit sie am Wettbewerb teilnehmen. Ähnlich dem LKHG MV ist den „ergänzenden" Regelungen des LDSG MV der Vorrang vor der DSGVO zu geben. Die hierdurch entstehende Rangproblematik zwischen LKGH MV und LDSG MV lässt sich durch den Vorrang der spezielleren Regelung lösen. Das LKHG MV ist als das speziellere Gesetz des gleichen Gesetzgebers somit vorrangig vor dem allgemeineren LDSG MV anzuwenden. Das LDSG MV ist jedoch nachrangig anwendbar, soweit ein Sachverhalt durch das LKHG MV nicht abschließend geregelt wird.

§ 32 LKHG bestimmt, dass § 38 BDSG in Verbindung mit § 6 BDSG entsprechende Anwendung findet. § 38 BDSG regelt den Datenschutzbeauftragten für nichtöffentliche Stellen. Diese Vorschrift gilt somit für öffentliche und private Krankenhäuser, sodass öffentliche Krankenhäuser insoweit wie nichtöffentliche Stellen behandelt werden.

§ 32 LKHG MV verweist aber nicht auf § 40 BDSG, weshalb es fraglich ist, ob bei öffentlichen Krankenhäusern sich die Vorschriften über die Aufsichtsbehörde nach den Vorschriften des BDSG oder des LDSG MV richten. Gemäß § 40 Abs. 1 BDSG überwachen die nach Landesrecht zuständigen Behörden im Anwendungsbereich der DSGVO bei den nichtöffentlichen Stellen die Anwendung der Vorschrift über den Datenschutz. Gemäß §§, 15, 19 Abs. 1 LDSG MV ist der Landesbeauftragte zuständige Aufsichtsbehörde im Sinne der DSGVO. Nach §§ 19 Abs. 2, 15 LDSG MV ist der Landesbeauftragte für Datenschutz auch zuständige Aufsichtsbehörde für nichtöffentliche Stellen gemäß § 40 BDSG. Das LDSG unterscheidet bei den Aufgaben also nach öffentlichen und nicht-öffentlichen Stellen und bezieht den § 40 BDSG hierbei mit ein. Der Landesdatenschutzbeauftragte ist somit nach dem LDSG MV bei Krankenhäusern, die als nicht-

[241] Das alte LDSG MV enthielt eine solche in § 2 Abs. 4 S. 1 LDSG MV.

öffentlichen Stelle im Sinne des LDSG MV gelten, Aufsichtsbehörde nach § 40 BDSG. Eine direkte Anwendung des § 40 BDSG auf Krankenhäuser in öffentlicher Trägerschaft durch den Teilverweis in § 32 LKHG MV auf § 38 BDSG scheidet aber aus.

Ergebnis: Das LKHG MV gilt für öffentliche Krankenhäuser vorrangig. Nachrangig gilt – für nicht am Wettbewerb teilnehmende Krankenhäuser - das LDSG MV sowie - außerhalb der Öffnungsklauseln - die DSGVO direkt. Aufsichtsbehörde ist für öffentliche Krankenhäuser der Landesdatenschutzbeauftragte nach dem LDSG MV. § 38 in Verbindung mit § 6 Abs. 4, Abs. 5 S. 2 und Abs. 6 des BDSG gelten entsprechend.

Krankenhäuser privater Träger

Die vorrangige Geltung des LKHG MV und die nachrangige Geltung des LDSG MV, des BDSG sowie die direkte Anwendung der DSGVO außerhalb der Öffnungsklauseln stimmt für Krankenhäuser in privater Trägerschaft, die nach § 3 Abs. 1 S. 1 LKHG MV der allgemeinen Versorgung dienen, mit deren Geltung bei öffentlichen Kliniken - insoweit sie in den Anwendungsbereich des § 2 Abs. 2 LDSG MV fallen - überein. Ist der Anwendungsbereich hingegen nicht eröffnet, sind nachrangig das BDSG sowie – außerhalb der Öffnungsklauseln - die DSGVO direkt anzuwenden. Das LKHG gilt grundsätzlich nicht für private Krankenhäuser, die nach § 3 Abs. 1 S. 1 LKHG MV nicht der allgemeinen Versorgung dienen. Private Krankenhäuser sind aber auch keine öffentlichen Stellen nach § 2 Abs. 1 und 2 LDSG MV. Das LDSG MV ist somit nicht anwendbar. Für private Krankenhäuser, die nicht der allgemeinen Versorgung dienen, gilt grundsätzlich vielmehr das BDSG sowie – außerhalb der Öffnungsklauseln - die DSGVO direkt, d. h. ohne Vorrangigkeit des LKHG MV.

Ergebnis: Für private Krankenhäuser, die der allgemeinen Versorgung der Bevölkerung dienen, gelten das LKHG MV und nachrangig das BDSG sowie – außerhalb der Öffnungsklauseln - die DSGVO direkt. Für private Krankenhäuser der akut stationären Versorgung, die nicht in den Landeskrankenhausplan aufgenommen sind, gelten lediglich (insbesondere aber die Datenschutz-)Teile des LKHG MV vorrangig und im Übrigen das BDSG sowie – außerhalb der Öffnungsklauseln - die DSGVO direkt. Für private Krankenhäuser, die nicht der allgemeinen Versorgung der Bevölkerung dienen, gilt nicht das LKHG MV, sondern das BDSG sowie die DSGVO, es sei denn, sie bieten akut stationäre Versorgung an. Selbst wenn (materiell) ausschließlichen das BDSG und die DSGVO Anwendung finden, bleibt dennoch organisatorisch der LfD für die Datenschutzaufsicht zuständig (§ 40 Abs. 1 BDSG, § 19 Abs. 2 LDSG MV.

Öffnungsklausel für kirchliche Träger?

Eine Öffnungsklausel für Datenschutz-Regelungen in kirchlichen Krankenhäusern durch Religionsgesellschaften besteht nicht. Dies ergibt sich auch aus § 3 Abs. 3 LKHG MV, wonach der 4. Abschnitt des LKHG MV (Innere Struktur der Krankenhäuser) bei kirchlichen Krankenhäusern nicht anwendbar ist. Im Umkehrschluss bedeutet dies, dass der übrige Teil des LKHG MV, somit auch der 7. Abschnitt über den Patientendatenschutz, bei ihnen Anwendung findet. Die Öffnungsklausel des § 2 Abs. 6 LDSG MV findet ebenfalls keine Anwendung, da das LKHG MV als spezielleres Gesetz vorgeht.

Zusammenfassung

Für öffentliche wie private Krankenhäuser, die der allgemeinen Versorgung der Bevölkerung dienen, gilt das LKHG MV vorrangig. Zudem gelten nachrangig Teile des LDSG MV und des BDSG, sowie außerhalb der Öffnungsklauseln die DSGVO direkt. Auch für nicht in den Landeskrankenhausplan aufgenommene private Kliniken der akut stationären Versorgung gelten die Datenschutzvorschriften des LKHG MV vorrangig. Im Übrigen bleibt es bei der nachrangigen Geltung des LDSG MV oder des BDSG und der direkten Anwendung der DSGVO außerhalb der Öffnungsklauseln. Für private Krankenhäuser, die nicht der allgemeinen Versorgung der Bevölkerung und auch nicht der akut-stationären Versorgung dienen, gelten weder das LKHG MV noch das LDSG MV, sondern das BDSG und die DSGVO – außerhalb der Öffnungsklauseln – direkt. Eine Öffnungsklausel für kirchliche Krankenhäuser besteht nicht.

Vorschriften zur Auftragsverarbeitung[242]

In Mecklenburg-Vorpommern ist die Auftragsverarbeitung in § 38 des LKHG MV geregelt. Demnach dürfen Krankenhausträger Patientendaten nur unter den folgenden Voraussetzungen von einem Auftragnehmer verarbeiten lassen, wenn:

1. Störungen im Betriebsablauf sonst nicht vermieden werden können,
2. die Datenverarbeitung kann dadurch erheblich kostengünstiger gestaltet werden, oder
3. das Krankenhaus stellt seinen Betrieb ein.

§ 38 Abs. 1 S. 2 LKHG MV schreibt vor, dass dem Auftragnehmer Patientendaten nur insoweit offenbar werden dürfen, als dies für die Auftragserfüllung erforderlich ist.

Die Speicherung von Patientendaten durch einen Auftragnehmer, die über einen Zeitraum von drei Monaten hinausgeht, ist außerhalb des Krankenhauses gemäß§ 38 Abs. 2 LKHG MV nur zulässig, wenn diese Patientendaten auf vom Auftragnehmer für das Krankenhaus verwahrten, getrennten Datenträgern gespeichert sind.

Nach § 38 Abs. 3 LKHG ist, soweit die Auftragsverarbeitung nicht auf eine ausdrückliche Einwilligung der Patientinnen und Patienten gestützt werden kann, die Verarbeitung im Auftrag nur durch Personen zulässig, die einem Berufsgeheimnis nach §§ 203 Abs. 1, Abs. 2 StGB unterliegen oder nach § 203 Abs. 4 StGB zur Verschwiegenheit verpflichtet sind.

Für die Übernahme von Patientendaten nach der Betriebseinstellung regelt § 38 Abs. 4 LKHG MV folgendes: „Übernimmt ein Auftragnehmer nach einer Betriebseinstellung eines Krankenhauses den gesamten Bestand der Patientendaten, gelten für ihn als verantwortliche Stelle hinsichtlich der Verarbeitung dieser Daten die Vorschriften [des siebten Abschnitts des LKHG MV]". Zur Aufbewahrung der Patientendaten führt Absatz 4 weiter aus: „Bei der Übernahme ist vertraglich sicherzustellen, dass die Patientinnen und Patienten für die Dauer von zehn Jahren nach Abschluss der Behandlung oder Untersuchung auf Verlangen in gleicher Weise wie bisher beim Krankenhaus Auskunft und Einsicht erhalten".

Nach § 38 Abs. 5 LKHG MV ist eine Auftragsverarbeitung außerhalb des Geltungsbereichs des Grundgesetzes nur zulässig, wenn die Patientin oder der Patient in die Auftragsverarbeitung

[242] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 275 f.

im Ausland ausdrücklich eingewilligt hat oder der Auftragsverarbeiter nach dem Recht seines Sitzlandes selbst einer gesetzlichen Geheimhaltungspflicht unterliegt.

Subsidiär sind die Regelungen zur Verarbeitung besonderer Kategorien personenbezogener Daten nach § 8 LDSG MV zu beachten, die sich grundsätzlich an den Verantwortlichen richten. § 8 S. 2 Nr. 4 LDSG MV führt in diesem Zusammenhang aber auch den Auftragsverarbeiter auf. Im Übrigen gilt Art. 28 DSGVO.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

Das LDSG MV enthält mit § 8 eine Vorschrift zur Verarbeitung besonderer Kategorien personenbezogener Daten samt einer Regelung zu technischen und organisatorischen Maßnahmen.

Nach § 8 S. 1 LDSG MV sind die dort aufgeführten angemessenen und spezifischen Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen aber nur dann vorzusehen, wenn auf der Grundlage des Teils 4 des Gesetzes besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO verarbeitet werden. Dieser umfasst aber nicht die Verarbeitung von Patientendaten zu Behandlungszwecken, sodass die Vorschrift mit ihren Vorgaben nicht einschlägig ist.

Gemäß § 1 Abs. 1 LDSG MV regelt das LDSG MV nur die notwendigen Ergänzungen zur Durchführung der DSGVO und regelt gleichzeitig in den Grenzen der DSGVO die spezifischen Anforderungen an die Verarbeitung personenbezogener Daten. Ist keine abweichende Regelung im LDSG MV gegeben, so gilt folglich die DSGVO.

Die Vorgaben an die technischen und organisatorischen Maßnahmen richten sich deshalb allein nach Art. 32 DSGVO.

3.4.9 Niedersachsen

Auf Krankenhäuser anwendbare Datenschutzvorschriften[243]

Krankenhäuser öffentlicher Träger

Krankenhäuser im Sinne des § 1 Abs. 1 LKHG NI sind solche im Sinne des § 2 Nr. 1 des Krankenhausfinanzierungsgesetzes (KHG), mit Ausnahme der in § 3 S. 1 KHG genannten Einrichtungen und der Vorsorge- und Rehabilitationseinrichtungen im Sinne des § 107 Abs. 2 des Fünften Buchs des Sozialgesetzbuchs (SGB V). Demnach sind Krankenhäuser Einrichtungen, in denen durch ärztliche und pflegerische Hilfeleistung Krankheiten, Leiden oder Körperschäden festgestellt, geheilt oder gelindert werden sollen oder Geburtshilfe geleistet wird und in denen die zu versorgenden Personen untergebracht und verpflegt werden können, mit Ausnahme von Vorsorge- und Rehabilitationseinrichtungen, Krankenhäuser im Straf- oder Maßregelvollzug, Polizeikrankenhäuser, Krankenhäusern bei denen der Träger der allgemeine Rentenversicherung und, soweit die gesetzliche Unfallversicherung die Kosten trägt, Krankenhäuser der Träger der gesetzlichen Unfallversicherung und ihrer Vereinigungen dienen.

§ 1 LKHG NI sieht vor, dass die Landkreise und kreisfreien Städte die Krankenhausversorgung der Bevölkerung als Aufgabe des eigenen Wirkungskreises nach Maßgabe des Krankenhausplans und nach § 2 LKHG NI sicherstellen und eigene Krankenhäuser errichten und unterhalten,

[243] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 178 ff.

soweit nicht durch andere Träger die Krankenhausversorgung gewährleistet wird. Im LKHG NI bestehen keine Datenschutzvorschriften für Krankenhäuser.

Gilt subsidiär das LDSG oder das BDSG?

Besondere Vorschriften über die Verarbeitung personenbezogener Daten gehen den Bestimmungen des LDSG NI gemäß § 1 Abs. 6 LDSG NI vor. Allerdings gibt es, wie eben ausgeführt keine Datenschutzbestimmungen im LKHG NI, sodass das LDSG NI nicht auf das LKHG NI verweist. Deshalb kommen für den Datenschutz in Krankenhäusern vor allem das LDSG NI, das BDSG und die DSGVO in Betracht, die allerdings nicht in Nachrangigkeit zu einem spezielleren Gesetz stehen.

Nach § 1 Abs. 1 S. 1 LDSG NI trifft dieser Teil des Gesetzes ergänzende Regelungen zur DSGVO für die Verarbeitung personenbezogener Daten

1. durch Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen (öffentliche Stellen)
   a) des Landes,

   b) der Kommunen und
   c) der sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts
      sowie
2. durch Personen und Stellen außerhalb des öffentlichen Bereichs, soweit ihnen Aufgaben der öffentlichen Verwaltung übertragen sind,

soweit die Datenverarbeitung in den sachlichen Anwendungsbereich der DSGVO fällt oder nach § 2 (Erweiterte Anwendung der DSGVO) auf die Datenverarbeitung die Regelungen der DSGVO anzuwenden sind.

Gemäß § 1 Abs. 1 S. 2 LDSG NI sind Personen und Stellen nach S. 1 Nr. 2 öffentliche Stellen im Sinne der Vorschiften dieses Teils, soweit ihnen Aufgaben der öffentlichen Verwaltung übertragen sind. Eine Übertragung setzt aber nicht zwangsläufig eine Beleihung voraus, da die Krankenhausversorgung auch als Aufgabe der öffentlichen Leistungsverwaltung wahrgenommen werden kann.

Nach § 1 Abs. 1 S. 3 LDSG NI sind auch Vereinigungen des privaten Rechts öffentliche Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in Satz 1 genannten juristischen Personen des öffentlichen Rechts unmittelbar oder durch eine solche Vereinigung beteiligt sind. Ein Krankenhaus fällt somit unabhängig von seiner Rechtsform in den Anwendungsbereich des LDSG NI, solange eine unmittelbare oder mittelbare Landesträgerschaft gegeben ist.

Nach § 1 Abs. 4 LDSG NI finden für öffentliche Stellen und ihre Zusammenschlüsse und Verbände die für nicht öffentlichen Stellen geltenden Vorschriften Anwendung, soweit sie als Unternehmen am Wettbewerb teilnehmen.

Ergebnis: Das LKHG NI enthält keine Vorschriften über den Datenschutz in Krankenhäusern. Für öffentliche Kliniken in mittelbarer oder unmittelbarer Landesträgerschaft, auch in privater

Rechtsform, gilt das LDSG NI; im Übrigen gilt außerhalb der Öffnungsklauseln die DSGVO direkt[244].

Krankenhäuser privater Träger

Die Ausführungen zu öffentlichen Krankenhäusern bezüglich des LKHG NI, insbesondere, dass in dieses Gesetz keine Datenschutzvorschriften für Krankenhäuser enthält, sind auf Kliniken in privater Trägerschaft übertragbar.

Gilt subsidiär das LDSG oder das BDSG?

Ein Krankenhaus in privater Trägerschaft ist keine Stelle, die unter das LDSG NI fällt, insbesondere keine Stelle außerhalb des öffentlichen Bereichs, der Aufgaben der öffentlichen Verwaltung übertragen sind (§ 1 Abs. 1 S. 2 LDSG NI). Grundsätzlich kann zwar auch die Krankenhausversorgung als Aufgabe der öffentlichen Verwaltung wahrgenommen werden. Dafür wäre bei einem privaten Krankenhausträger aber eine Beleihung erforderlich. Die Aufnahme in den Landeskrankenhausplan allein ist dafür aber nicht ausreichend. Außerdem findet eine solche Beleihung im Krankenhausbereich üblicherweise nicht statt. Somit ist auf Kliniken privater Träger das BDSG sowie - außerhalb der Öffnungsklauseln -die DSGVO direkt anzuwenden.[245]

Ergebnis: Das LKHG NI enthält keine Datenschutzvorschriften für Krankenhäuser. Auf private Kliniken ist das BDSG sowie – außerhalb der Öffnungsklauseln - die DSGVO direkt anzuwenden.

Öffnungsklausel für kirchliche Träger?

Es besteht keine Öffnungsklausel für kirchliche Krankenhäuser, mangels spezifischer Datenschutzvorgaben im LKHG NI ist dies allerdings auch nicht nötig. Die Rechtsvorschriften kirchlicher Krankenhäuser gehen dem LDSG NI vor, soweit sie den Patientendatenschutz spezifisch regeln und sofern das verfassungs- und europarechtlich gebotene Minimum an Datenschutz im Ergebnis gewährleistet ist.

Zusammenfassung

Das LKHG NI enthält keine Datenschutzvorschriften für Krankenhäusern. Für öffentliche Kliniken in mittelbarer oder unmittelbarer Landesträgerschaft, auch in privater Rechtsform, gelten das LDSG NI und bei Wettbewerbsteilnahme im Übrigen das BDSG sowie – außerhalb der Öffnungsklauseln - die DSGVO direkt Auf private Kliniken findet ausschließlich das BDSG sowie – außerhalb der Öffnungsklauseln die DSGVO direkt Anwendung.

Vorschriften zur Auftragsverarbeitung[246]

Im LKHG NI finden sich keine bereichsspezifischen Regelungen für Krankenhäuser für die Verarbeitung personenbezogener Daten im Auftrag.

Die Regelungen zur Auftragsverarbeitung in § 45 LDSG NI sind nicht anwendbar, da es sich um Regelungen im Zusammenhang mit der Richtlinie (EU) 2016/680 handelt. Dies ergibt sich aus der systematischen Stellung im zweiten Kapitel des zweiten Teils des Gesetzes.

[244] Europarechtskonforme Nutzung der in der DSGVO bestehenden Öffnungsklauseln jeweils vorausgesetzt.

[245] Europarechtskonforme Nutzung der in der DSGVO bestehenden Öffnungsklauseln jeweils vorausgesetzt.

[246] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 276

Sofern ein Krankenhaus nach § 1 LDSG NI nicht in den Anwendungsbereich des LDSG NI fällt, ist Art. 28 DSGVO anzuwenden.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

Das LDSG NI enthält eine Regelung zu technischen und organisatorischen Maßnahmen in § 17 LDSG NI. § 17 LDSG NI enthält Vorgaben zur Verarbeitung besonderer Kategorien personenbezogener Daten, die auch auf die Auftragsverarbeitung anwendbar sind. § 17 Abs. 2 LDSG NI bestimmt, dass wenn im Rahmen der Datenverarbeitung nach dem zweiten Kapitel oder nach anderen datenschutzrechtlichen Bestimmungen besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO verarbeitet werden, von den Verantwortlichen und den Auftragsverarbeitern zur Wahrung der Grundrechte und Interessen der betroffenen Personen die folgenden Maßnahmen zu treffen sind:

1. Sicherstellung, dass nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten verarbeitet worden sind,
2. Beschränkung der Befugnisse für den Zugriff auf personenbezogene Daten auf das erforderliche Maß, sowie die Dokumentation der Befugnisse,
3. Sensibilisierung der Personen, die Zugang zu den personenbezogenen Daten haben. § 17 Abs. 3 S. 1 LDSG NI bestimmt, dass die Verantwortlichen und Auftragsverarbeiter ergänzend zu Abs. 2 weitere angemessene und spezifische Maßnahmen zu treffen haben, soweit dies zum Schutz besonderer Kategorien personenbezogener Daten erforderlich ist.

Als Maßnahmen kommen gemäß § 17 Abs. 3 S. 2 LDSG NI insbesondere in Betracht:

1. Sicherstellung, dass die personenbezogenen Daten zur Verarbeitung nur im Vier-Augen-Prinzip freigegeben werden,
2. Sicherstellung, dass auf die personenbezogenen Daten nur nach einer Zwei-Faktor-Authentisierung zugegriffen wird,
3. Sicherstellung, dass die elektronische Übermittlung von personenbezogenen Daten nur mit einer Verschlüsselung erfolgt,
4. Sicherstellung, dass in einem vernetzten IT-System die personenbezogenen Daten nur mit Verschlüsselung gespeichert werden,
5. Sicherstellung, dass durch eine redundante Auslegung der Systeme, der Energieversorgung und der Datenübertragungseinrichtungen ein Datenverlust vermieden wird,
6. Sicherstellung, dass Daten nicht unbefugt verändert werden und ihre Integrität gewahrt ist, etwa durch Einsatz einer elektronischen Signatur,
7. Schulung der Personen, die Zugang zu den personenbezogenen Daten haben. Gemäß § 17 Abs. 4 LDSG NI richtet sich die Art und der Umfang der Maßnahmen nach den Absätzen 2 und 3 nach dem Stand der Technik und den Implementierungskosten, nach der Art, dem Umfang, den Umständen und dem Zweck der Datenverarbeitung sowie nach der Eintrittswahrscheinlichkeit und der Schwerer der mit der Datenverarbeitung verbundenen Risiken für die Grundrechte und Interessen der betroffenen Personen.

Gemäß § 1 Abs. 1 S. 1 LDSG NI trifft das LDSG NI ergänzende Regelungen zur DSGVO. Soweit das Gesetz keine Regelungen enthält gelten die Vorschriften der DSGVO. Die technischen und

organisatorischen Maßnahmen nach Art. 32 DSGVO sind für die Verarbeitung von Patientendaten anzuwenden.

3.4.10 Nordrhein-Westfalen[247]

Auf Krankenhäuser anwendbare Datenschutzvorschriften

In Nordrhein-Westfalen ist der Datenschutz in Krankenhäusern nicht im Landeskrankenhausgesetz, dem sog. Krankenhausgestaltungsgesetz (KHGG NW), sondern in einem speziellen Gesundheitsdatenschutzgesetz (GDSG NW) geregelt. Gemäß § 2 Abs. 1 S. 1 Nr. 1 GDSG NW gilt dieses Gesetz für die Verarbeitung personenbezogener Daten von Personen, die, auch aufgrund eines gesonderten ärztlichen Behandlungsvertrages, in einem i. S. v. § 107 Abs. 1, § 108 zugelassenen Krankenhaus oder einer Vorsorge- und Rehabilitationseinrichtung gemäß § 107 Abs. 2, § 111 SGB V, ambulant oder stationär untersucht oder behandelt werden, deren Träger nicht der Bund oder eine bundesunmittelbare Körperschaft gemäß Art. 87 Abs. 2 GG ist. Vom Anwendungsbereich des GDSG NW ausgenommen sind nach dieser umfassenden Definition als nur Kliniken des Bundes und nicht zur Abrechnung mit der GKV zugelassene reine Privatkliniken. Für diese Kliniken sind ausschließlich das BDSG und – außerhalb der Öffnungsklauseln - die DSGVO direkt anwendbar.

Krankenhäuser öffentlicher Träger

Das LDSG NW gilt gemäß § 3 S. 1 GDSG NW gilt für Krankenhäuser öffentlicher Träger subsidiär, soweit das GDSG NW nichts anderes bestimmt. Besondere Rechtsvorschriften, die die Verarbeitung personenbezogener Daten regeln, gehen dem LDSG NW vor (§ 5 Abs. 6LDSG NW). Somit gilt für öffentliche Kliniken GDSG NW vorrangig und das LDSG NW nachrangig, sowie – außerhalb der Öffnungsklauseln – die DSGVO direkt.

Für Patientendaten in Krankenhäusern, die unter § 2 Abs. 1 GDSG NW fallen, kommt es aufgrund der Rechtsfolgenverweisung des § 3 S. 1 GDSG NW nicht auf den Anwendungsbereich des § 5 Abs. 1 LDSG NW (öffentliche Stelle) an. Dass es sich bei § 3 S. 1 GDSG NW um eine Rechtsfolgenverweisung handelt, lässt sich insbesondere daran erkennen, dass in § 3 S. 2 GDSG NW für Krankenhäuser privater Träger nicht der Zweite Teils des LDSG NW für anwendbar erklärt wird, sondern § 38 BDSG. Daraus lässt sich im Umkehrschluss folgern, dass im Übrigen das LDSG NW, welches eigentlich nur für öffentliche Stellen gilt, insoweit auch auf Krankenhäuser privater Träger anwendbar sein soll.[248]

Zwar wird in § 2 Abs. 2 LDSG NW die Weiterverweisung auf das BDSG für öffentlich-rechtliche Wettbewerbsunternehmen durch § 3 GDSG NW nicht explizit ausgeschlossen. Allerdings wird der Verweis des § 2 Abs 2 LDSG NW aufgrund des eben hergeleiteten Charakters von § 3 GDSG

[247] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 183 ff.

[248] Bundesverfassungsrechtliche Bedenken im Hinblick auf die Kompetenz des Landesgesetzgebers zur Regelung nicht krankenhausspezifischer Datenschutzbelange im privaten Krankenhaus durch die subsidiäre Anwendbarkeit des LDSG auch für Krankenhäuser privater Träger sollen hier dahinstehen und der Wille des Landesgesetzgebers insoweit ernst genommen werden. Den rechtsunterworfenen Krankenhausträgern wird jedenfalls kein Verschuldensvorwurf gemacht werden können, wenn sie sich auf die Gültigkeit des Landesrechts verlassen, solange dieses nicht gerichtlich für unwirksam erklärt wurde.

NW als Rechtsfolgenverweisung in Bezug auf die Anwendbarkeit des LDSG implizit ausgeschlossen.[249]

Krankenhäuser privater Träger

Für private Krankenhäuser im Anwendungsbereich des GDSG NW gelten somit das GDSG NW, sowie nachrangig das LDSG NW, sowie - außerhalb der Öffnungsklauseln – die DSGVO direkt. Für reine Privatkliniken gelten das BDSG, sowie – außerhalb der Öffnungsklauseln – die DSGVO direkt.

Öffnungsklausel für kirchliche Träger?

Kirchen und Religionsgemeinschaften treffen nach § 2 Abs. 3 GDSG NW für Krankenhäuser und Einrichtungen im Sinne des GDSG NW, die ihrem Bereich zuzuordnen sind, eigene Regelungen, die den Zielen des GDSG NW entsprechen.

Zusammenfassung

Für alle Krankenhäuser außer solchen des Bundes oder nicht zur Abrechnung mit der GKV zugelassenen, reinen Privatkliniken gilt das GDSG NW. Das LDSG NW gilt gegenüber dem GDSG NW nachrangig. Für Krankenhäuser des Bundes und reine Privatkliniken gelten das BDSG und – außerhalb der Öffnungsklauseln - die DSGVO direkt[250]. Es besteht eine Öffnungsklausel für kirchliche Krankenhäuser (verbunden mit der Maßgabe der Zielentsprechung).

Vorschriften zur Auftragsverarbeitung[251]

In Nordrhein-Westfalen ist die Auftragsverarbeitung in § 7 GDSG NW geregelt. Gemäß § 7 Abs. 1 GDSG NW sind Patientendaten grundsätzlich in der Einrichtung oder öffentlichen Stelle zu verarbeiten. Eine Verarbeitung im Auftrag ist nur unter den Voraussetzungen des § 7 Abs. 2 bis 4 GDSG NW zulässig.

Demnach setzt die Zulässigkeit der Auftragsverarbeitung von Patientendaten voraus, dass Störungen im Betriebsablauf anderenfalls nicht vermieden oder Teilvorgänge der automatischen Datenverarbeitung dadurch erheblich kostengünstiger vorgenommen werden können.

Vor Vergabe eines Auftrages zur Verarbeitung von Personendaten hat sich der Auftraggeber gemäß § 7 Abs. 3 S. 1 GDSG NW zudem zu vergewissern, dass die Wahrung der Datenschutzbestimmungen des GDSGG NW und der ärztlichen Schweigepflicht beim Auftragnehmer sichergestellt ist.

Patientendaten aus dem ärztlichen Bereich muss der Auftragnehmer gemäß § 7 Abs. 3 S. 2 GDSG NW in physisch getrennten Dateien verarbeiten. Er darf Patientendaten zudem nur im

[249] Vgl. dazu nähere Ausführungen zu Brandenburg, oben S. 104. So im Ansatz auch VG Gelsenkirchen, Beschl. v. 14.10. 2013 – 17 L 304/13, juris Rdnr. 12 ff. (Nichtanwendbarkeit des § 27 BDSG aufgrund § 3 GDSG NW), wobei hier dahingestellt bleiben kann, ob das Verwaltungsgericht aus diesem zutreffenden Ansatz die angenommene Einschränkung der Datenschutzkontrolle nach § 38 Abs. 1 BDSG a.F. überzeugend abgeleitet hat. Allgemein zeigt diese Problematik aber auch, dass das Zusammenspiel von vorrangigem LKGH bzw. GDSG mit nachrangigem LDSG bzw. BDSG gerade bei uneinheitlicher Terminologie im Einzelnen zu nicht einfach zu prognostizierenden Auslegungsergebnissen führt.

[250] Europarechtskonforme Nutzung der in der DSGVO bestehenden Öffnungsklauseln jeweils vorausgesetzt.

[251] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 276 f.

Rahmen der Weisungen des Auftraggebers verarbeiten, wobei der Auftraggeber dem Auftragnehmer gemäß § 7 Abs. 3 S. 4 GDSG NW erforderlichenfalls auch Vorgaben zur Ergänzung seiner technischen und organisatorischen Einrichtungen und Maßnahmen zu erteilen hat.

Zudem sind die Bestimmungen zur Auftragsverarbeitung nach Art. 28 DSGVO (bei reinen Privatkliniken) oder dem LDSG NW (bei öffentlicher Trägerschaft und Plankrankenhäusern in privater Trägerschaft) subsidiär anzuwenden. Das LDSG NW enthält nur eine Regelung zu technischen und organisatorischen Maßnahmen zur Auftragsverarbeitung in § 15 LDSG NW, welche auf Krankenhäuser anwendbar sein kann. Denn § 52 LDSG NW findet keine Anwendung, da dieser die Verarbeitung im Auftrag im Rahmen der Richtlinie (EU) 2016/680 behandelt.

Ist der Auftragnehmer eine nichtöffentliche Stelle und findet die Verarbeitung im Geltungsbereich des GDSG NW statt, so hat der Auftraggeber gemäß § 7 Abs. 4 S. 1 GDSG NW sicherzustellen, dass sich der Auftragnehmer der Kontrolle durch den Landesbeauftragten für den Datenschutz unterwirft. Bei Datenverarbeitungen außerhalb des Geltungsbereichs des GDSG NW muss nach § 7 Abs. 4 S. 2 GDSG NW die jeweils zuständige Datenschutzkontrollbehörde unterrichtet werden.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

Das LDSG NW enthält in § 15 LDSG NW Garantien zum Schutz besonderer Kategorien personenbezogener Daten, wozu nach Art. 9 Abs. 1 DSGVO auch Gesundheitsdaten gehören. Demnach sind vom Verantwortlichen angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorzusehen, wenn solche Datenkategorien verarbeitet werden.

Gemäß § 15 S. 2 LDSG NW sind das, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen:

1. technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt,
2. Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind,
3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der öffentlichen Stelle und von Auftragsverarbeitern,
5. die Pseudonymisierung personenbezogener Daten,
6. die Verschlüsselung personenbezogener Daten,
7. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen, einschließlich der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
8. die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung und

9. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung personenbezogener Daten für andere Zwecke die Einhaltung des LDSG sowie der DSGVO sicherstellen.

Das LDSG NW stellt, wie in Baden-Württemberg, mangels einschränkenden Anwendungsbereichs im Wesentlichen eine Wiederholung des Art. 32 DSGVO dar, welcher durch konkrete Vorschläge für Maßnahmen erweitert wird.

Die technischen und organisatorischen Maßnahmen bei der Verarbeitung von Patientendaten richten sich nach § 15 LDSG NW und im Übrigen nach Art. 32 DSGVO.

3.4.11 Rheinland-Pfalz

Auf Krankenhäuser anwendbare Datenschutzvorschriften[252]

Krankenhäuser öffentlicher Träger

Nach § 3 Abs. 1 LKHG RP gilt das LKHG RP für Krankenhäuser nach der weit gefassten Definition des § 2 Nr. 1 KHG, die allerdings nach dem KHG gefördert werden müssen. Dazu zählen ausdrücklich auch Tageskliniken. Es ist somit erforderlich, dass die Klinik tatsächlich nach dem KHG gefördert wird, eine bloße-Förderfähigkeit reicht nicht aus. Krankenhäuser des Bundes sind nach § 5 Abs. 1 Nr. 9 KHG allerdings grundsätzlich schon nicht KHG-förderfähig. Das LKHG RP ist u.a. auch deshalb schon nicht anwendbar, weil auch keine anderen Normen sie in dessen Anwendungsbereich einbeziehen.[253]

Mit Ausnahme der §§ 11 bis 21 (3. Abschnitt: Öffentliche Förderung der Krankenhäuser) und des § 23 Abs. 1 und 2 (Fachrichtungen, Regelung der inneren Struktur und Organisation) gilt das LKHG RP nach § 3 Abs. 3 auch für Universitätskliniken, soweit diese der Versorgung der Bevölkerung dienen. Somit gelten die den Datenschutz betreffenden §§ 35-38 LKHG RP auch für diese Kliniken, allerdings nur, wenn sie der Versorgung der Bevölkerung dienen. Anderenfalls gilt das LKHG RP für sie nicht, weil Universitätskliniken nach § 5 Abs. 1 Nr. 1 KHG schon grundsätzlich nicht förderfähig sind und sie deshalb nicht allgemein in den Anwendungsbereich nach § 3 Abs. 1 LKHG RP fallen. Die Anforderung der Versorgung der Bevölkerung ist bei Universitätskliniken jedoch in aller Regel erfüllt, da sie als Krankenhäuser der (Maximal-)Versorgung der Bevölkerung dienen.

Die jeweils geltenden Datenschutzvorschriften, insbesondere die Bestimmungen der DSGVO und des LDSG (§ 36 Abs. 1 S. 1 LKHG RP) sind anzuwenden, soweit das LKHG RP nichts anderes bestimmt.

Gilt subsidiär das LDSG oder das BDSG?

Besondere Rechtsvorschriften des Bundes oder des Landes gehen den Bestimmungen des LDSG RP vor, soweit sie die Verarbeitung personenbezogener Daten regeln (§ 2 Abs. 9 S. 1 LDSG RP).

[252] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 188 ff.

[253] Von Gesetzgebungskompetenzen ganz abgesehen, vgl. oben S. 105.

Gemäß § 2 Abs. 1 S. 1 gilt das LDSG RP u. a. für die Behörden, die sonstigen öffentlich-rechtlich organisierten Einrichtungen des Landes, die kommunalen Gebietskörperschaften, die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und die Vereinigungen der vorgenannten Stellen ungeachtet ihrer Rechtsform.

Nach § 2 Abs. 1 S. 2 LDSG RP fallen auch juristische Personen und sonstige privatrechtliche Vereinigungen der in § 2 Abs. 1 S. 1 genannten Stellen unter das LDSG RP, soweit ihnen die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht, ungeachtet der Beteiligung nicht öffentlicher Stellen. Kliniken öffentlicher Träger fallen somit in den Anwendungsbereich des LDSG RP, wenn sie die in § § 2 Abs. 1 S. 1 oder S. 2 LDSG RP aufgeführten Voraussetzungen erfüllen.

Ein Krankenhaus nimmt keine hoheitlichen Aufgaben wahr, wenngleich es sein kann, dass es Aufgaben der öffentlichen Verwaltung erfüllt. Deshalb es nicht auf Grundlage des § 2 Abs. 1 S. 3 LDSG RP unter das LDSG RP.

Gemäß § 2 Abs. 4 LDSG RP sind auf öffentliche Stellen, die als Unternehmen am Wettbewerb teilnehmen § 20 LDSG RP (Datenverarbeitung bei Dienst- und Beschäftigungsverhältnissen) und, unbeschadet anderer Rechtsgrundlagen, die Vorschriften des BDSG für nicht-öffentliche Stellenanzuwenden. Grundsätzlich nehmen alle Krankenhäuser am Wettbewerb teil,[254] wobei zumindest im Krankenhausbereich dem Merkmal der Unternehmenseigenschaft keine weitere Bedeutung zukommt. Es kann sich dabei insbesondere auch um Eigenbetriebe oder juristische Personen des öffentlichen Rechts handeln.[255]

Auch Vereinigungen des Privatrechts fallen unter den Verweis des § 2 Abs. 4 LDSG RP, da sie nach von der Definition der öffentlichen Stellen nach § 2 Abs. 1 S. 2 LDSG RP erfasst sind. Der Verweis gilt für Krankenhäuser also immer dann, wenn sie in einer der in § 2 Abs. 1 LDSG RP genannten Formen organisiert sind. Dann gilt das LKHG RP vorrangig, Teile des LDSG RP nachrangig und im Übrigen Teile des BDSG sowie – außerhalb der Öffnungsklauseln – die DSGVO direkt.

Ergebnis: Für nach dem KHG geförderte Krankenhäuser – ausdrücklich einschließlich Tageskliniken –gilt das LKHG RP vorrangig. Für Universitätsklinken bestehen Besonderheiten, wonach auf diese, jedenfalls bei der Sekundärnutzung von Behandlungsdaten, auch die im LKHG RP enthaltenen Vorschriften zum Schutz personenbezogener Daten Anwendung finden. Für öffentliche Kliniken in mittelbarer oder unmittelbarer Trägerschaft des Landes gelten nachrangig das LDSG RP und im Übrigen das BDSG sowie die DSGVO. Dies gilt auch für öffentliche Kliniken in privater Rechtsform bei mittelbarer oder unmittelbarer, absoluter Mehrheitsbeteiligung der öffentlichen Hand.

Krankenhäuser privater Träger

Das LKHG RP gilt, wie bereits ausgeführt, gemäß § 3 Abs. 1 für Krankenhäuser, die nach dem KHG gefördert werden. Dabei muss es sich um eine tatsächliche KHG-Förderung des jeweiligen Krankenhauses handeln, die bloße Förderfähigkeit reicht nicht aus.

[254] Vgl. dazu oben zu Baden-Württemberg S. 80 f.

[255] Vergleichbar der Rechtslage in Hamburg, s.o. S. 112 f., oder Baden-Württemberg, s.o. S. 80 f.

Auch Kliniken in privater Trägerschaft sind grundsätzlich KHG-förderfähig, weshalb das LKHG RP im Falle einer tatsächlichen KHG-Förderung auf sie anwendbar ist. Auf reine Privatklinik, die aufgrund des zu geringen Anteils der nach GKV-Sätzen abgerechneten Patienten ausnahmsweise nicht KHG-förderfähig (keine Steuerbegünstigung nach § 67 AO) sind, ist das LKHG RP nicht anwendbar.[256] Durch landesrechtliche Bestimmungen kann die KHG-Förderung zwar auch solchen Kliniken gewährt werden (§ 5 Abs. 2 KHG), jedoch ist dies im 2. und 3. Abschnitt des LKHG RP über die Krankenhausplanung und öffentliche Förderung (§§ 6 – 21) nicht geschehen.

Die Vorschriften der DSGVO und ergänzend die Regelungen des LDSG RP finden Anwendung, soweit im LKHG RP nichts anderes bestimmt ist (§ 36 Abs. 1 S. 1 LKHG RP).

Gilt subsidiär das LDSG oder das BDSG?

Da sie keine öffentlichen Stellen i.S.v. § 2 Abs. 1 LDSG RP sind, fallen Kliniken in privater Trägerschaft nicht unter das LDSG RP. Insbesondere ist § 2 Abs. 1 S. 3 LDSG RP, nach dem nicht-öffentliche Stellen bei Wahrnehmung hoheitlicher Aufgaben unter das LDSG RP fallen, nicht auf sie anwendbar. Ein Krankenhaus nimmt keine hoheitlichen Aufgaben wahr, wenngleich es sein kann, dass es Aufgaben der öffentlichen Leistungsverwaltung erfüllt. Der Landesbeauftragte für Datenschutz und Informationsfreiheit ist jedoch auch für nicht-öffentliche Stellen Aufsichtsbehörde im Sinne des § 40 BDSG gemäß § 15 Abs. 2 LDSG.

Auf reine Privatkliniken ist daher das BDSG, sowie - außerhalb der Öffnungsklauseln – DSGVO direkt anzuwenden.

Ergebnis: Das LKHG RP gilt vorrangig für KHG-geförderte Krankenhäuser, ausdrücklich einschließlich Tageskliniken. Auch Kliniken privater Träger sind grundsätzlich KHG-förderfähig, außer bei fehlender Steuerbegünstigung nach § 67 AO. Für private Krankenhäuser gelten entweder das LKGH und außerhalb der Öffnungsklauseln die DSGVO direkt, sowie teilweise das LDSG RP oder bei reinen Privatkliniken das BDSG und außerhalb der Öffnungsklauseln die DSGVO direkt.

Öffnungsklausel für kirchliche Träger?

Für kirchliche Krankenhäuser besteht eine Öffnungsklausel: Gemäß § 38 LKHG RP können Religionsgemeinschaften anstelle der datenschutzrechtlichen Bestimmungen des LKHG RP unter Berücksichtigung ihres kirchlichen Selbstverständnisses vergleichbare eigene bereichsspezifische Bestimmungen erlassen.

Zusammenfassung

Für KHG-geförderte Krankenhäuser i. S. v. § 2 Nr. 1 KHG, ausdrücklich einschließlich Tageskliniken, gilt das LKHG RP vorrangig. Zudem gelten nachrangig Teile des LDSG RP und im Übrigen Teile des BDSG sowie die DSGVO für öffentliche Krankenhäuser in mittelbarer oder unmittelbarer Trägerschaft des Landes. Selbiges gilt für öffentliche Krankenhäuser in privater Rechtsform, sofern eine mittelbare oder unmittelbare absolute Mehrheitsbeteiligung der öffentlichen

[256] Vgl. dazu nähere Ausführungen zu Bayern, oben S. 93 f.

Hand des Landes besteht. Für private Kliniken gilt das BDSG und die DSGVO, entweder nachrangig zum LKHG RP oder (bei reinen Privatkliniken) ausschließlich.

Vorschriften zur Auftragsverarbeitung[257]

Gemäß § 36 Abs. 9 S. 1 LKHG RP können sich Krankenhäuser zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedienen. Die Ausgestaltung der Auftragsverarbeitung durch den Auftragsverarbeiter regelt gemäß § 36 Abs. 9 S. 2 LKHG RP der Art. 28 DSGVO. Art. 28 DSGVO findet daher bei allen Krankenhäusern Anwendung.

Das LDSG RP enthält hinsichtlich der Auftragsverarbeitung lediglich Regelungen zur Verarbeitung personenbezogener Daten nach Maßgabe der Richtlinie (EU) 2016/680 in den §§ 51 ff. LDSG RP. Diese finden keine Anwendung auf Krankenhäuser, sodass es bei Art. 28 DSGVO bleibt.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

§ 19 LDSG RP enthält eine Vorschrift zur Verarbeitung besonderer Kategorien personenbezogener Daten mit einer Regelung zu technischen und organisatorischen Maßnahmen.

§ 19 Abs. 1 und 2 LDSG RP regeln die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO, teils in Wiederholung der DSGVO (so bei der ausdrücklichen Einwilligung nach § 19 Abs. 1 S. 1 LDSG RP), teils in Ausfüllung von Öffnungsklauseln der DSGVO (z.B. im Hinblick auf das Schriftformerfordernis für die Einwilligung nach § 19 Abs. 1 S. 2 LDSG RP oder der gesetzlichen Erlaubnisse in § 19 Abs. 2 LDSG RP).

Nach § 19 Abs. 3 S. 1 LDSG RP haben die Verantwortlichen bei der Verarbeitung genetischer oder biometrischer Daten oder Gesundheitsdaten angemessene und spezifische Maßnahmen, insbesondere technische und organisatorische Maßnahmen, zur Wahrung der Grundrechte und Interessen der betroffenen Person vorzusehen.

Gemäß § 19 Abs. 3 S. 2 LDSG RP haben die Verantwortlichen mindestens

1. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem die Daten eingegeben, verändert oder entfernt worden sind,
2. die an Verarbeitungsvorgängen Beteiligten zu sensibilisieren,
3. den Zugang zu den Daten beim Verantwortlichen und von Auftragsverarbeitern zu beschränken,
4. die Grundsätze der Datenminimierung und Speicherbegrenzung sowie die Notwendigkeit einer Datenschutz-Folgenabschätzung zu berücksichtigen,
5. die Daten im Fall der Übermittlung zu verschlüsseln,
6. die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der Daten sicherzustellen,
7. die Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
8. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzurichten und

[257] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 277 f.

9. im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung des LDSG sowie der DSGVO durch spezifische Verfahrensregelungen sicherzustellen.

§ 19 Abs. 3 S. 3 LDSG RP bestimmt, dass Art. 32 DSGVO unberührt bleibt.

Nach § 19 Abs. 4 LDSG RP ist die Verarbeitung von genetischen Daten oderbiometrischen Daten oder Gesundheitsdaten im Auftrag nur zulässig, wenn der Auftragsverarbeiter entsprechend dem Schutzbedarf der Daten angemessene Vorkehrungen zum Datenschutz im Sinne des § 19 Abs. 3 LDSG RP getroffen hat und keine überwiegenden schutzwürdigen Interessen der betroffenen Person einer Auslagerung der Datenverarbeitung entgegenstehen. Die Beauftragung von Stellen außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung ist unzulässig.

Im Gegensatz zu anderen Bundesländern bezieht sich § 19 Abs. 3 LDSG RP nicht auf die vorangestellten Absätze, sodass die technischen und organisatorischen Maßnahmen nach dem Katalog immer dann anzuwenden sind, wenn genetische oder biometrische Daten oder Gesundheitsdaten verarbeitet werden. § 19 Abs. 1 LDSG RP bestimmt jedoch, dass es einer ausdrücklichen und schriftlichen Einwilligung der betroffenen Person bedarf. Der Katalog selbst entspricht im Wesentlichen dem anderer Bundesländer. Unterschiede bestehen darin, dass die Regelung der technischen und organisatorischen Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt, nicht enthalten ist. Die Pseudonymisierung wird nicht verlangt. Daten sind nur im Fall der Übermittlung zu verschlüsseln. Und die gängige Regelung zur Anforderung an das System wurde in zwei Punkte (Nr. 6 und 7) aufgeteilt. Zudem bestimmt das LDSG RP eigenständig, dass die Grundsätze der Datenminimierung und Speicherbegrenzung sowie die Notwendigkeit einer Datenschutz-Folgenabschätzung zu berücksichtigen sind. Über § 19 Abs. 4 LDSG RP findet § 19 Abs. 3 LDSG RP auch Anwendung auf den Auftragsverarbeiter. Im Übrigen soll nach § 19 Abs. 3 S. 3 LDSG RP der Art. 32 DSGVO Anwendung finden.

Die Verarbeitung von Patientendaten unterfällt grundsätzlich dem § 19 Abs. 1 LDSG RP, sodass für die Zulässigkeit der Verarbeitung von Patientendaten nach dem LDSG RP eine ausdrückliche Einwilligung notwendig wäre. Für die technischen und organisatorischen Maßnahmen bei der Verarbeitung von Patientendaten gelten somit § 19 Abs. 3 LDSG RP und im Übrigen Art. 32 DSGVO.

3.4.12 Saarland

Auf Krankenhäuser anwendbare Datenschutzvorschriften[258]

Gemäß § 2 Abs. 1 S. 1 gilt das LKHG SL, soweit nichts anderes bestimmt ist, für alle Krankenhäuser im Saarland.

Krankenhäuser öffentlicher Träger

Die saarländische Klinik für Forensische Psychiatrie ist gemäß § 2 Abs. 1 S. 4 vom Anwendungsbereich des LKHG SL und den darin enthaltenen Vorschriften zum Schutz personenbezogener Daten ausgenommen. Die besonderen Rechtsverhältnisse dieser Maßregelvollzugseinrichtung

[258] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 195 ff.

im Besonderen, sowie entsprechender Einrichtungen im Allgemeinen, zu den psychisch kranken oder suchtkranken Straftätern, die dort untergebracht sind, werden im Folgenden nicht weiter betrachtet.[259]

Der saarländische Landesgesetzgeber verfügt, insbesondere hinsichtlich des Datenschutzes, kaum über Regelungskompetenz über Krankenhäuser des Bundes. Da der Landesgesetzgeber nach hier vertretener Auffassung zumindest bezüglich datenschutzrechtlicher Regelungen keine Gesetzgebungskompetenz für Krankenhäuser des Bundes und insbesondere Bundeswehrkrankenhäuser hat, fallen diese nicht unter das LKHG SL. Insoweit gelten das BDSG und – außerhalb der Öffnungsklauseln - die DSGVO direkt.

Ansonsten gilt für öffentliche Krankenhäuser im Saarland aber das LKHG SL. Patientendaten im Krankenhaus unterliegen gemäß § 13 Abs. 1 S. 1 LKHG SL dem Datenschutz, ungeachtet der Art ihrer Verarbeitung. Soweit im LKHG SL nichts anderes bestimmt ist, findet nach § 13 Abs. 1 S. 3 LKHG SL die DSGVO unmittelbar Anwendung.

Gilt subsidiär das LDSG oder das BDSG?

Soweit das LKHG SL nichts anderes bestimmt, sind, wie bereits ausgeführt, gemäß § 13 Abs. 1 S. 3 LKHG SL die jeweils geltenden Vorschriften der DSGVO anzuwenden. Nach § 13 Abs. 8 S. 6 LKHG SL ergeben sich die Aufgaben der Beauftragten für Datenschutz im Krankenhaus aus dem BDSG in der jeweils geltenden Fassung. Dementsprechend sieht auch § 2 Abs. 5 S. 1 LDSG SL vor, dass besondere Rechtsvorschriften des Bundes oder des Landes über den Datenschutz den Vorschriften des LDSG SL vorgehen.

Gemäß § 2 Abs. 1 S. 1 gilt das LDSG SL für die Verarbeitung personenbezogener Daten durch die Behörden und sonstigen öffentlichen Stellen des Landes, der Gemeinden und Gemeindeverbände sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts. Nach § 2 Abs. 1 S. 2 LDSG SL fallen, ungeachtet ihrer Rechtsform, auch Vereinigungen, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der vorgenannten Stellen mit absoluter Mehrheit der Anteile oder absoluter Stimmmehrheit beteiligt ist bzw. sind unter das LDSG SL. Somit können auch Personen des Privatrechts davon erfasst sein.

Es ist möglich, dass die Krankenhausversorgung als Aufgabe der öffentlichen Verwaltung wahrgenommen wird.[260] Somit fällt ein Krankenhaus in öffentlicher Trägerschaft, das gemäß § 2 Abs. 1 S. 1 oder S. 2 LDSG SL geführt wird, unter das LDSG SL. Da die Krankenhausversorgung aber keine hoheitliche Aufgabe darstellt, fallen Krankenhäuser nicht generell durch § 2 Abs. 1 S. 3 LDSG SL unter das LDSG SL.

Soweit ein öffentlich-rechtliches Unternehmen am Wettbewerb teilnimmt, gelten gemäß § 2 Abs. 3 LDSG SL diese als nicht öffentliche Stellen. Mit Ausnahme der Vorschriften über die

[259] Hierbei handelt es sich auch nicht um Behandlungsverhältnisse im üblichen Sinn. Rechtsgrundlagen für die entsprechende Unterbringung finden sich in §§ 63, 64, 67h StGB und §§ 81, 126a, 453c StPO. Daneben gibt es noch öffentlich-rechtliche bzw. verwaltungsrechtliche Grundlagen für eine Unterbringung, die hier ebenfalls nicht näher beleuchtet werden.

[260] Vgl. dazu nähere Ausführungen bei Baden-Württemberg, S. 81.

Aufsichtsbehörde sind ergänzend zur DSGVO die für nicht-öffentliche Stellen geltenden Vorschriften des BDSG, einschließlich der Straf- und Bußgeldvorschriften anwendbar. Grundsätzlich nehmen alle Krankenhäuser am Wettbewerb teil, wobei dem Merkmal der Unternehmenseigenschaft zumindest im Krankenhausbereich keine weitere Bedeutung zukommt.[261] Insbesondere kann es sich dabei auch um Eigenbetriebe oder juristische Personen des öffentlichen Rechts handeln.

Der in § 2 Abs. 3 LDSG SL enthaltene Teilverweis auf das BDSG und die DSGVO gilt ausdrücklich nur für öffentlich-rechtliche Unternehmen, wenngleich der Anwendungsbereich des LDSG SL nach § 2 Abs. 1 S. 2 in bestimmten Fällen auch juristische Personen des Privatrechts umfasst. Es ist deshalb fraglich, ob es sich für den Begriff der öffentlich-rechtlichen Unternehmen um juristische Personen des öffentlichen Rechts handeln muss oder ob auch juristische Personen des Privatrechts unter bestimmten Voraussetzungen als öffentlich-rechtliche Unternehmen anzusehen sind. Ein Ausschluss privater Rechtsformen vom Teilverweis auf das BDSG und die DSGVO würde zu dem nicht stimmigen Ergebnis führen, dass auf diese nur das LDSG SL nachrangig gilt, während für juristische Personen des öffentlichen Rechts unter den Voraussetzungen des § 2 Abs. 3 LDSG SL teilweise auf das BDSG verwiesen wird.

In vergleichbaren Regelungen anderer Länder ist von öffentlichen Stellen die Rede, was dann per Definition auch private Rechtsformen einschließen kann. Zwar wird auch in Hessen und Mecklenburg-Vorpommern der Begriff der öffentlich-rechtlichen Unternehmen verwendet. Allerdings die die entsprechende Norm für Krankenhäuserdort schon durch das LKHG ausgeschlossen. Ein solches Verständnis kommt aber vorliegend schon aufgrund der Rechtsgrundverweisung in § 13 Abs. 1 S. 3 LKHG SL nicht in Betracht.

Zur Erzielung eines stimmigen Ergebnisses muss deshalb davon ausgegangen werden, dass grundsätzlich alle unter § 2 Abs. 1 LDSG SL fallenden Stellen und somit auch private Rechtsformen vom Teilverweis des § 2 Abs. 3 LDSG SL auf das BDSG und die DSGVO erfasst sind, sofern sie die übrigen Voraussetzungen erfüllen. Somit kommt es für die öffentlich-rechtliche Eigenschaft des Unternehmens nicht auf die Rechtsform, sondern auf die Trägerschaft an.

Der Teilverweis auf das BDSG und die DSGVO in § 2 Abs. 3 LDSG SL gilt somit nach der hier vertretenen Meinung immer dann für Krankenhäuser, wenn diese nach § 2 Abs. 1 S. 1 oder S. 2 LDSG SL organisiert sind. Sodann gilt das LKHG SL vorrangig, Teile des LDSG SL nachrangig und im Übrigen Teile des BDSG und – außerhalb der Öffnungsklauseln- die DSGVO.

Ergebnis: Das LKHG SL gilt für alle Krankenhäuser vorrangig und verweist nachrangig auf die Vorschriften der DSGVO. Für öffentliche Kliniken in mittelbarer oder unmittelbarer Landesträgerschaft gelten nachrangig Teile des LDSG SL (insbes. zur Kontrolle durch den LfD) und im Übrigen Teile des BDSG und – außerhalb der Öffnungsklauseln – die DSGVO direkt.[262]. Selbiges gilt für öffentliche Kliniken in privater Rechtsform bei mittelbarer oder unmittelbarer absoluter Mehrheitsbeteiligung der öffentlichen Hand des Landes.

[261] Vergleichbar der Rechtslage in Hamburg, s.o. S. 112 f., oder Baden-Württemberg, s.o. S. 80 f.

[262] Europarechtskonforme Nutzung der in der DSGVO bestehenden Öffnungsklauseln jeweils vorausgesetzt.

Krankenhäuser privater Träger

Das LKHG SL ist auch auf Kliniken in privater Trägerschaft anwendbar.[263]

Gilt subsidiär das LDSG oder das BDSG?

Da sie keine öffentliche Stelle nach § 2 Abs. 1 LDSG SL sind, fallen Kliniken in privater Trägerschaft nicht unter das LDSG SL. Insbesondere § 2 Abs. 1 S. 3 LDSG SL, nach dem nicht-öffentliche Stellen unter das LDSG SL fallen, wenn sie hoheitliche Aufgaben wahrnehmen, ist auf sie nicht anwendbar. Denn ein Krankenhaus nimmt – abgesehen von der Ausnahme der Zwangsunterbringung und -behandlung – keine hoheitlichen Aufgaben wahr, wenngleich es möglich ist, dass es Aufgaben der öffentlichen Verwaltung erfüllt. Auf rein private Kliniken sind daher nachrangig das BDSG sowie – außerhalb der Öffnungsklauseln – die DSGVO direkt anzuwenden.

Ergebnis: Für alle Krankenhäuser gilt das LKHG SL vorrangig, das nachrangig auf die jeweils geltenden Datenschutzvorschriften verweist. Auf private Kliniken ist nachrangig das BDSG sowie – außerhalb der Öffnungsklauseln - die DSGVO direkt anzuwenden.

Öffnungsklausel für kirchliche Träger?

Es besteht eine Öffnungsklausel für kirchliche Krankenhäuser in § 2 Abs. 2 LKHG SL. Danach gelten die §§ 6 Abs. 3, Abs. 4, 8, 13, 13a, 14, 16 – 19 LKHG SL nicht für Krankenhäuser, die von Religionsgemeinschaften oder diesen gleichgestellten oder ihnen zugeordneten Einrichtungen unabhängig von deren Rechtsform betrieben werden. Die Religionsgemeinschaften treffen für ihre Krankenhäuser in eigener Zuständigkeit Regelungen, die den Zielen dieser Vorschriften entsprechen.

Zusammenfassung

Für alle Krankenhäuser gilt das LKHG SL vorrangig, das nachrangig auf die jeweils geltenden Vorschriften der DSGVO verweist. Für öffentliche Kliniken in mittelbarer oder unmittelbarer Landesträgerschaft gelten nachrangig Teile des LDSG SL. Dies gilt auch für öffentliche Kliniken in privater Rechtsform, sofern eine mittelbare oder unmittelbare absolute Mehrheitsbeteiligung der öffentlichen Hand des Landes vorliegt. Auf Kliniken privater Träger ist nachrangig das BDSG sowie – außerhalb der Öffnungsklauseln - die DSGVO anzuwenden. Zudem besteht für kirchliche Krankenhäuser eine Öffnungsklausel.

Vorschriften zur Auftragsverarbeitung[264]

Der Patientendatenschutz ist im Saarland in den §§ 13, 13a LKHG SL geregelt. § 13 Abs. 4 LKHG SL erlaubt eine Übermittlung von Patientendaten an Personen und Stellen außerhalb des Krankenhauses unter den genannten Voraussetzungen. Die Auftragsverarbeitung fällt jedoch nicht unter die Übermittlung von Patientendaten, da es sich bei der Übermittlung um weisungsunabhängige Empfänger handelt, was sich aus dem Kontext der Vorschrift ergibt. Die Auftragsverarbeitung ist deshalb eigenständig in § 13a LKHG SL geregelt worden.

[263] Vgl. zum Anwendungsbereich die Ausführungen zu öffentlichen Krankenhäusern, s. soeben S. 132 ff.

[264] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 278

Nach § 13a Abs. 1 S. 1 LKHG SL darf der Krankenhausträger die Verarbeitung von Patientendaten einem Auftragnehmer übertragen, wenn

1. Störungen im Betriebslauf sonst nicht vermieden werden können,
2. die Datenverarbeitung dadurch erheblich kostengünstiger gestaltet werden kann oder
3. das Krankenhaus seinen Betrieb einstellt.

§ 13a Abs. 1 S. 2 LKHG SL bestimmt ferner, dass vor der Erteilung eines Auftrags zur Verarbeitung von Patientendaten außerhalb des Krankenhauses zu prüfen ist, ob dies im wohlverstandenen Interesse der Patientin oder des Patienten liegt oder der Zweck auch mit verschlüsselten oder pseudonymisierten Patientendaten erreicht werden kann.

§ 13a Abs. 2 LKHG SL regelt die Speicherung und Löschung von Patientendaten. Danach ist eine über drei Monate hinausgehende Speicherung von Patientendaten durch einen Auftragnehmer außerhalb des Krankenhauses nur zulässig, wenn die Patientendaten auf getrennten Datenträgern gespeichert sind, die der Auftragnehmer für den Krankenhausträger verwahrt.

§ 13a Abs. 3 LKHG SL legt die Auswahlkriterien und die zu treffenden Vereinbarungen fest. Der Auftragnehmer ist vom Krankenhausträger sorgfältig auszuwählen und die Einzelheiten des Auftrags und die vom Auftragnehmer zu treffenden technischen und organisatorischen Sicherungsmaßnahmen sind schriftlich zu vereinbaren. Eine Abschrift dieser Vereinbarung hat der Krankenhausträger dem Unabhängigen Datenschutzzentrum Saarland und der Krankenhausaufsichtsbehörde unverzüglich zu übersenden.

§§ 13a Abs. 4 bis Abs. 6 LKHG SL bestimmen die Pflichten des Auftragnehmers. Nach § 13a Abs. 4 LKHG SL darf der Auftragnehmer die ihm überlassenen Patientendaten nur im Rahmen des Auftrags und der Weisungen des Krankenhausträgers verarbeiten. Sofern die §§ 13, 14 LKHG SL für den Auftragnehmer nicht gelten, hat der Krankenhausträger sicherzustellen, dass der Auftragnehmer diese Vorschriften entsprechend anwendet und sich insoweit der Kontrolle des/der Landesbeauftragten für Datenschutz und Informationsfreiheit unterwirft. Nach § 13a Abs. 5 LKHG SL ist eine Übertragung des Auftrags auf Dritte oder die Erteilung von Unteraufträgen nur mit Zustimmung des Krankenhausträgers zulässig, wobei die Abs. 2 bis 4 entsprechend gelten. Übernimmt ein Auftragnehmer nach einer Betriebsaufgabe eines Krankenhauses oder nach einer Umwandlung eines Krankenhauses in eine nicht akutstationäre Versorgungseinrichtung den gesamten Bestand der Patientendaten, gelten für ihn als verantwortliche Stelle gemäß § 13a Abs. 6 LKHG SL hinsichtlich der Verarbeitung dieser Daten die Vorschriften des Abschnitts 4 (§§ 12 – 15 LKHG SL). Bei der Übernahme ist vertraglich sicherzustellen, dass die Patientinnen und Patienten für die Dauer von zehn Jahren nach Abschluss der Behandlung oder Untersuchung auf Verlangen in gleicher Weise wie bisher beim Krankenhaus Auskunft und Einsicht erhalten.

Die konkrete Ausgestaltung der Auftragsverarbeitung wird gemäß § 13a Abs. 7 LKHG SL durch Art. 28 DSGVO geregelt.

Die Regelungen des LDSG SL finden keine Anwendung, da nach obigen Ausführungen das LKHG SL einen Rückgriff auf diese versperrt. Somit gilt subsidiär allein Art. 28 DSGVO.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

Das LDSG SL regelt die technischen und organisatorischen Maßnahmen in § 8 Abs. 2 LDSG SL. Nach § 8 Abs. 2 S. 1 LDSG SL sind bei der Verarbeitung besonderer Kategorien personenbezogener Daten angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen vorzusehen. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:

1. technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt,
2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
5. Pseudonymisierung personenbezogener Daten,
6. Verschlüsselung personenbezogener Daten,
7. dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten einschließlich der Fähigkeit, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall unverzüglich wiederherzustellen,
8. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder
9. spezifische Verfahrensregelungen, die im Falle einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben des LDSG sowie der DSGVO sicherstellen.

Ähnlich wie in Rheinland-Pfalz bezieht sich § 8 Abs. 2 LDSG SL nicht auf § 8 Abs. 1 LDSG SL, der eine ergänzende Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten bestimmt. Diese Regelung gilt somit grundsätzlich für alle Verarbeitungen besonderer Kategorien personenbezogener Daten. § 8 Abs. 2 LDSG SL nimmt keine Unterscheidung zwischen dem Verantwortlichen und Auftragsverarbeiter vor. Die Vorschrift findet daher nach obigen Ausführungen zu Baden-Württemberg auch auf den Auftragsverarbeiter Anwendung.

3.4.13 Sachsen

Auf Krankenhäuser anwendbare Datenschutzvorschriften[265]

Krankenhäuser öffentlicher Träger

Gemäß § 2 Abs. 1 gilt das LKHG SN für KHG-geförderte Krankenhäuser i.S.v. § 2 Nr. 1 KHG.[266] Somit muss ein Krankenhaus tatsächlich gefördert werden, die bloße Förderfähigkeit reicht nicht aus. Krankenhäuser des Bundes grundsätzlich nicht KHG-förderfähig gemäß § 5 Abs. 1 Nr. 9 KHG. Das LKHG SN ist – neben Kompetenzgründen – auch deshalb nicht auf sie anwendbar.

Die jeweils geltenden Datenschutzvorschriften sind gemäß § 33 Abs. 1 S. 1 LKHG SN anzuwenden, soweit das KKHG SN nichts anderes bestimmt.

Mit Ausnahme der §§ 8 - 20 (Förderung) und des § 21 Abs. 1 und 2 (Fachabteilungen, Leitung) gilt das LKHG SN gemäß § 2 Abs. 3 auch für Universitätskliniken, soweit sie der Versorgung der Bevölkerung dienen. Für diese gelten unter den eben genannten Voraussetzungen somit auch die Datenschutzbestimmungen der §§ 32 – 34 LKHG SN Anderenfalls gilt das LKHG SN mangels KHG-Förderfähigkeit gem. § 5 Abs. 1 Nr. 1 KHG nicht für Unikliniken, sodass diese schon deshalb nicht unter den Anwendungsbereich des LKHG SN nach § 2 Abs. 1 LKHG SN fallen. Jedenfalls beim Umgang mit Behandlungsdaten ist aber in aller Regel davon auszugehen, dass sie der (Maximal-)Versorgung der Bevölkerung dienen.

Gilt subsidiär das LDSG oder das BDSG?

Soweit das LKHG SN nichts anderes bestimmt, sind nach dessen § 33 Abs. 1 S. 1 die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden.

Das LDSG SN[267] gilt nur noch für die Datenverarbeitung durch öffentliche Stellen des Landes Sachsen zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung im Rahmen der Datenschutz-Richtlinie (EU) 680/2016,[268] welche auf die Datenverarbeitung durch Krankenhäuser nicht anwendbar ist. Im Übrigen gilt für öffentliche Stellen des Landes Sachsen seit dem 25. Mail 2018 ergänzend zur DSGVO das Sächsisches Datenschutzdurchführungsgesetz (DSDG SN).[269]

---

[265] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 206 ff.

[266] Vgl. zu dieser weiten Begriffsbestimmung von Krankenhäusern in § 2 Nr. 1 KHG, die praktisch alle Krankenhäuser im natürlichsprachlichen Sinn umfasst. Allerdings stellt das weitere Erfordernis der Förderung nach dem KHG eine zusätzliche Einschränkung dar.

[267] Sächsisches Datenschutzgesetz vom 25. August 2003 (SächsGVBl. S. 330), das zuletzt durch Artikel 9 des Gesetzes vom 22. August 2019 (SächsGVBl. S. 663) geändert worden ist.

[268] Gemäß Art. 46 Nr. 2 a) aa) des Gesetzes zur Anpassung landesrechtlicher Vorschriften an die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG vom 26. April 2018 (SächsGVBl. S. 198). Vgl. auch https://www.saechsdsb.de/umsetzung.

[269] Gesetz zur Durchführung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Sächsisches Datenschutzdurchführungsgesetz – SächsDSDG), erlassen als Art. 1 des Gesetzes zur Anpassung landesrechtlicher Vorschriften an die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG vom 26. April 2018 (SächsGVBl. S. 198).

Gemäß § 2 Abs. 1 S. 1 gilt das DSDG SN für die Verarbeitung personenbezogener Daten durch die Behörden und sonstigen öffentlichen Stellen des Landes, der Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts. Nach § 2 Abs. 2 DSDG SN fallen auch juristische Personen und sonstige Vereinigungen des privaten Rechts unter das DSDG SN, wenn eine oder mehrere der in § 2 Abs. 1 DSDG SN genannten Stellen mit absoluter Mehrheit der Anteile oder absoluter Mehrheit der Stimmen an ihnen beteiligt sind. Somit fällt eine Klinik eines öffentlichen Trägers unter das DSDG SN, wenn sie die in § 2 Abs. 1 oder Abs. 2 LDSG SN aufgeführten Voraussetzungen erfüllt.

Gemäß § 2 Abs. 3 DSDG SN gelten für öffentlich-rechtliche Unternehmen mit eigener Rechtspersönlichkeit und Stellen nach Absatz 2, die am Wettbewerb teilnehmen, ergänzend zur DSGVO die einschlägigen Vorschriften des BDSG.

Auch juristische Personen des privaten Rechts können bereits dadurch unter die Verweisnorm fallen, dass sie in ihr § 2 Abs. 2 DSDG SN gesondert aufgeführt sind. Dadurch stellt sich einerseits die zur Rechtslage im Saarland problematisierte Frage, ob sie als öffentlich-rechtliche Unternehmen anzusehen sind, in Sachsen nicht. Andererseits ergibt sich daraus auch, dass ein Unternehmen jedenfalls vorliegend auch eine juristische Person des öffentlichen Rechts sein kann und eben nicht notwendigerweise eine juristische Person des privaten Rechts zu sein braucht.[270] Zumindest im Krankenhausbereich kommt dem Merkmal der Unternehmenseigenschaft kommt dabei keine weitere Bedeutung zu.[271]

Im Unterschied zu einigen anderen Ländern müssen die Wettbewerbsunternehmen vorliegend aber, ähnlich wie in Baden-Württemberg müssen Wettbewerbsunternehmen in Sachen – im Unterschied zu einigen anderen Ländern – eine eigene Rechtspersönlichkeit haben, um von der Verweisung auf das BDSG erfasst zu sein. Für Eigen- bzw. Regiebetriebe der öffentlichen Hand gilt dieser Verweis somit nicht. Liegt also keine juristische Person des privaten Rechts vor, so muss es sich um eine juristische Person des öffentlichen Rechts handeln, also um eine Anstalt, Stiftung oder Körperschaft des öffentlichen Rechts.

Der Verweis in § 2 Abs. 3 DSDG SN auf das BDSG gilt also für in einer der in dieser Norm genannten Formen organisierte Krankenhäuser. Denn am Wettbewerb nehmen grundsätzlich alle Krankenhäuser teil.[272] Somit gilt vorrangigen das LKHG SN, nachrangig das BDSG und außerhalb der Öffnungsklausen die DSGVO direkt.

Da von der Verweisung auf das BDSG in § 2 Abs. 3 DSDG SN die Aufsicht nicht ausgenommen wird, ist der Sächsische Datenschutzbeauftragte für öffentliche Krankenhäuser mit eigener Rechtspersönlichkeit nicht wie für sonstige öffentlichen Stellen gemäß § 14 Abs. 1 DSDG SN zuständig, sondern als Aufsichtsbehörde gemäß § 14 Abs. 2 DSDG SN in Verbindung mit § 40 BDSG. Für öffentliche Krankenhäuser ohne eigene Rechtspersönlichkeit würde, sofern solche in Sachsen noch existieren, allerdings neben der DSGVO und dem LKGH SN ausschließlich das DSDG SN einschließlich § 14 Abs. 1 DSDG SN gelten.

[270] Vgl. dazu die näheren Ausführungen zu Baden-Württemberg, s.o. S. 81 f.

[271] Vergleichbar der Rechtslage in Hamburg, s.o. S. 112 f., oder Baden-Württemberg, s.o. S. 80 f.

[272] Vgl. dazu näher die Ausführungen zu Baden-Württemberg, oben S. 80 ff.

Ergebnis: Für KHG-geförderte Krankenhäuser i. S. v. § 2 Nr. 1 KHG gilt das LKHG SN vorrangig, welches nachrangig auf die jeweils geltenden Datenschutzvorschriften verweist. Für als Eigen oder Regiebetrieb geführte, öffentliche Kliniken in mittelbarer oder unmittelbarer Landesträgerschaft gilt nachrangig das DSDG SN. Für die als juristische Personen des öffentlichen Rechts in Trägerschaft des Landes oder als juristische Personen des privaten Rechts, an denen die öffentliche Hand des Landes mittelbar oder unmittelbar mit absoluter Mehrheit beteiligt ist, geführten, öffentlichen Kliniken gelten nachrangig das BDSG und außerhalb der Öffnungsklauseln die DSGVO direkt.[273]

Krankenhäuser privater Träger

Gemäß § 2 Abs. 1 gilt das LKHG SN für KHG-geförderte Krankenhäuser i. S. v. § 2 Nr. 1 KHG. Die jeweils geltenden Datenschutzvorschriften sind gemäß § 33 Abs. 1 S. 1 LKHG SN anzuwenden, soweit das LKHG SN nichts anderes bestimmt.

Gilt subsidiär das LDSG oder das BDSG?

Kliniken in privater Trägerschaft sind keine öffentlichen Stellen i.S.v. § 2 Abs. 1 und Abs. 2 DSDG SB und fallen somit nicht unter das DSDG SN. Insbesondere § 2 Abs. 1 S. 2 DSDG SN, nach dem nicht-öffentliche Stellen unter das LDSG SN fallen, wenn sie hoheitliche Aufgaben wahrnehmen, ist auf sie nicht anwendbar. Ein Krankenhaus nimmt keine hoheitlichen Aufgaben wahr, wenn gleiches sein kann, dass es – jedenfalls bei öffentlicher Trägerschaft – Aufgaben der öffentlichen (Leistungs-)Verwaltung erfüllt. Auf private Kliniken sind daher nachrangig das BDSG und – außerhalb der Öffnungsklauseln – die DSGVO direkt anzuwenden.

Ergebnis: Für KHG-geförderte Krankenhäuser i. S. v. § 2 Nr. 1 KHG gilt das LKHG SN vorrangig, welches nachrangig auf die jeweils geltenden Datenschutzvorschriften verweist. Für Kliniken in privater Trägerschaft gelten nachrangig das BDSG und - außerhalb der Öffnungsklauseln - die DSGVO direkt.[274]

Öffnungsklausel für kirchliche Träger?

Es besteht eine Öffnungsklausel für kirchliche Krankenhäuser. Religionsgemeinschaften treffen gemäß § 2 Abs. 2 LKHG SN eigene Regelungen bezüglich des Vierten Abschnitts mit Ausnahme der §§ 21 Abs. 1, Abs. 4, 22, 23 LKHG SN. Im Übrigen gilt das LKHG SN auch für Religionsgemeinschaften.

Zusammenfassung

Für KHG-geförderte Krankenhäuser i. S. v. § 2 Nr. 1 KHG gilt das LKHG SN vorrangig und verweist nachrangig auf die jeweils geltenden Datenschutzvorschriften. Für als Eigenbetrieb geführte, öffentliche Kliniken in mittelbarer oder unmittelbarer Landesträgerschaft gilt nachrangig das DSDG SN. Werden Krankenhäuser öffentlicher Träger als juristische Personen des öffentlichen oder privaten Rechts geführt, gelten nachrangig das BDSG sowie – außerhalb der Öffnungsklauseln - die DSGVO direkt. Auch für Kliniken privater Träger gelten nachrangig das

[273] Europarechtskonforme Nutzung der in der DSGVO bestehenden Öffnungsklauseln vorausgesetzt.

[274] Europarechtskonforme Nutzung der in der DSGVO bestehenden Öffnungsklauseln vorausgesetzt.

BDSG und ferner – außerhalb der Öffnungsklauseln – die DSGVO direkt. Für kirchliche Krankenhäuser besteht eine Öffnungsklausel.

Vorschriften zur Auftragsverarbeitung[275]

§ 33 Abs. 8 S. 1 LKHG SN bestimmt, dass soweit sich das Krankenhaus bei der Verarbeitung von Patientendaten eines Auftragsverarbeiters bedient, insbesondere sicherzustellen ist, dass dieser die nach § 203 StGB entsprechende Schweigepflicht einhält. Die Auftragserteilung bedarf ferner der Zustimmung der zuständigen Behörde und der Auftragsverarbeiter hat einen Datenschutzbeauftragten zu benennen (§§ 33 Abs. 8 S. 2, S. 3 LKHG SN).

Subsidiär gilt für Krankenhäuser in Sachsen Art. 28 DSGVO. Das DSDG SN enthält genauso wenig wie das BDSG Regelungen zur Auftragsverarbeitung. § 7 LDSG SN enthält zwar solche Regelungen, die jedoch wie dieses Gesetz insgesamt nicht auf Krankenhäuser Anwendung finden.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

Das neue DSDG SN enthält keine Regelung zu technischen und organisatorischen Maßnahmen. Für die technischen und organisatorischen Maßnahmen bei der Verarbeitung von Patientendaten ist daher auf Art. 32 DSGVO allein abzustellen.

3.4.14 Sachsen-Anhalt

Auf Krankenhäuser anwendbare Datenschutzvorschriften[276]

Das LKHG ST enthält keine Regelung über den Anwendungsbereich dieses Gesetzes. Gemäß § 1 Abs. 1 LKHG ST ist es Aufgabe der Landkreise und kreisfreien Städte, die Krankenhausversorgung der Bevölkerung als Aufgabe des eigenen Wirkungskreises nach Maßgabe des Krankenhausplanes sicherzustellen. Die Vielfalt der Krankenhausträger ist dabei gemäß § 1 Abs. 1 S. 1 LKHG ST zu beachten, wobei insbesondere ist gemeinnützigen und privaten Krankenhausträgern ausreichend Raum zu geben ist.

Gilt das LDSG oder das BDSG?

Es kommt deshalb eine unmittelbare Anwendung des LDSG ST in Betracht. Soweit die DSGVO und andere Rechtsvorschriften auf personenbezogene Daten anzuwenden sind, gehen diese zwar dem LDSG ST vor (§§ 2 Abs. 3, Abs. 5 LDSG ST). § 16 LKHG ST enthält Regelungen zur Verarbeitung von Patientendaten. Diese gehen insoweit also dem LDSG ST vor. Für die Regelung des Datenschutzes in Krankenhäusern kommen nachrangig das LDSG ST, das BDSG und die DSGVO in Betracht.

Krankenhäuser öffentlicher Träger

Gemäß §§ 2 Abs. 1 S. 1, Abs. 2 gilt das LDSG ST u. a. für öffentlich-rechtlich organisierte Einrichtungen und Stellen des Landes, der Gemeinden, der Landkreise und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen, ungeachtet ihrer Rechtsform. Somit fällt ein Krankenhaus eines öffentlichen Trägers

[275] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 278 f.

[276] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 213 ff.

unter den Anwendungsbereich des LDSG ST, wenn es die in § 2 Abs. 2 LDSG ST genannten Voraussetzungen erfüllt.

Ein Krankenhaus nimmt keine hoheitlichen Aufgaben wahr, wenngleich es sein kann, dass es Aufgaben der öffentlichen Verwaltung erfüllt. Es fällt deshalb nicht schon aufgrund des § § 2 Abs. 2 S. 2 unter das LDSG ST.

Eine von einem der in § 2 Abs. 2 S. 1 LDSG ST genannten Träger als juristische Person des privaten Rechts geführte öffentliche Klinik fällt unter das LDSG ST, weil es sich um eine Vereinigung nach § 2 Abs. 2 S. 1 LDSG ST handelt. Nach dem Wortlaut kommt es dafür ausdrücklich nicht auf den Wortlaut an.

Soweit jedoch Stellen, die unter das LDSG ST fallen, als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten für sie und ihre Vereinigungen gemäß § 2 Abs. 7 Nr. 1 LDSG ST nur die Vorschriften zum Datenschutzbeauftragten (§§ 17 – 20), sowie § 23 (Aufgaben und Befugnisse), § 24 (Rechte und Pflichten) und § 26 (Ergänzende Regelungen im Beschäftigungskontext). Im Übrigen gelten die Vorschriften des BDSG, mit Ausnahme der §§ 5 bis 16 und § 38 BDSG und – außerhalb der Öffnungsklauseln – die DSGVO direkt.

Zumindest im Krankenhausbereich kommt dem Merkmal der Unternehmenseigenschaft dabei keine weitere Bedeutung zu. Es kann sich dabei insbesondere auch um Eigenbetriebe oder juristische Personen des öffentlichen Rechts handeln.[277]

Der in § 2 Abs. 7 Nr. 1 enthaltene Teilverweis auf das BDSG gilt für Krankenhäuser somit immer dann, wenn sie in einer von § 2 Abs. 1 S. 1 LDSG ST genannten Form organisiert sind. Es gelten die speziellen Regelungen des LKHG ST und nachrangig Teile des LDSG ST und im Übrigen Teile des BDSG und außerhalb der Öffnungsklauseln die DSGVO direkt[278].

Ergebnis: Das LKHG ST enthält spezielle Vorschriften zur Verarbeitung von Patientendaten. Für öffentliche Kliniken gelten daher das LKHG ST vorrangig und Teile des LDSG ST und im Übrigen außerhalb der Öffnungsklauseln die DSGVO direkt und sofern der Teilverweis greift Teile des BDSG und außerhalb der Öffnungsklauseln die DSGVO direkt.[279]

Krankenhäuser privater Träger

Das LKHG ST nimmt keine Unterscheidung zwischen den Typen von Krankenhäusern vor, sodass auch für Kliniken privater Trägerschaft die speziellen Regelungen zur Verarbeitung von Patientendaten gelten. Kliniken eines privaten Trägers sind keine Stellen, die unter das LDSG ST fallen. Es handelt sich Insbesondere nicht um eine Stelle nach § 2 Abs. 2 S. 2 LDSG ST, die hoheitliche Aufgaben der öffentlichen Verwaltung wahrnimmt. Auf Kliniken in privater Trägerschaft sind daher das BDSG und außerhalb der Öffnungsklauseln die DSGVO direkt anzuwenden.

[277] Vergleichbar der Rechtslage in Hamburg, s.o. S. 112 f., oder Baden-Württemberg, s.o. S. 80 f.

[278] Europarechtskonforme Nutzung der Öffnungsklauseln der DSGVO vorausgesetzt.

[279] Europarechtskonforme Nutzung der Öffnungsklauseln der DSGVO vorausgesetzt.

Ergebnis: Im LKHG ST bestehen spezielle Vorschriften über die Verarbeitung von Patientendaten in Krankenhäusern. Auf Kliniken privater Träger sind vorrangig das LKHG ST, nachrangig das BDSG und außerhalb der Öffnungsklauseln die DSGVO direktanzuwenden.

Öffnungsklausel für kirchliche Träger?

Es besteht keine Öffnungsklausel für kirchliche Krankenhäuser.

Zusammenfassung

Im LKHG ST bestehen spezielle Vorschriften über die Verarbeitung von Patientendaten in Krankenhäusern, die für alle Krankenhäuser gelten. Für öffentliche Kliniken gelten nachrangig das LDSG ST und bei Teilverweis Teile des BDSG sowie außerhalb der Öffnungsklauseln die DSGVO direkt. Auf Kliniken privater Träger sind nachrangig das BDSG und außerhalb der Öffnungsklauseln die DSGVO direkt anzuwenden.[280]

Vorschriften zur Auftragsverarbeitung[281]

Das LKHG ST enthält in § 16 LKHG ST eine Regelung zur Verarbeitung von Patientendaten. Nach § 16 Abs. 4 S. 1 LKHG ST kann sich das Krankenhaus zur Verarbeitung von Patientendaten im Wege der Datenverarbeitung im Auftrag anderer Personen oder Stellen bedienen, die an Tätigkeiten des Krankenhauses mitwirken und dafür Daten verarbeiten, soweit dies für die Inanspruchnahme der Tätigkeit anderer Personen oder Stellen erforderlich ist und soweit keine Anhaltspunkte besehen, dass durch die Auftragsverarbeitung schutzwürdige Belange des Patienten oder des Betroffenen beeinträchtigt werden. Jede bei der Auftragsverarbeitung nach Satz 1 beteiligte Person ist zur Geheimhaltung zu verpflichten, soweit sie nicht infolge ihrer sonstigen Tätigkeit bereits einer strafrechtlich sanktionierten Schweigepflicht unterliegt (§ 16 Abs. 4 S. 2 LKHG ST). Der Patient ist vorab über die Auftragsverarbeitung zu informieren und kann dieser Verarbeitung der ihn betreffenden Daten widersprechen (§ 16 Abs. 4 S. 3 LKHG ST).

Subsidiär gilt – sofern der Geltungsbereich eröffnet ist – das LDSG ST. Dieses enthält in § 15 LDSG ST Regelungen, die auch für die Auftragsverarbeitung zu Behandlungszwecken im Krankenhaus relevant werden können.

§ 15 Abs. 1 LDSG ST lässt die Einrichtung eines automatisierten Abrufverfahrens oder eines gemeinsamen automatisierten Dateisystems, in oder aus dem mehrere datenverarbeitende Stellen personenbezogene Daten verarbeiten zu, soweit dies unter Berücksichtigung der Rechte und Freiheiten der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist und durch technische und organisatorische Maßnahmen Risiken für die Rechte und Freiheiten der betroffenen Personen vermieden werden können. Hier ist die Auftragsverarbeitung zwar nicht erwähnt. Wenn aber Auftragsverarbeiter an der Verarbeitung im Rahmen eines solchen automatisierten Abrufverfahrens mitwirken, hätten auch diese die Vorgaben zu beachten. Dies kann z.B. der Fall sein, wenn ein Cloud-KIS-Modul der Leistungsabstimmung zwischen verschiedenen Krankenhäusern oder der Zuweiser-Kommunikation dient.

[280] Europarechtskonforme Nutzung der in der DSGVO bestehenden Öffnungsklauseln jeweils vorausgesetzt.

[281] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 279

Wenn personenbezogene Daten im Auftrag eines Verantwortlichen durch eine andere Stelle verarbeitet werden und auf diesen Auftragsverarbeiter die Vorschriften des LDSG ST nicht direkt anwendbar sind, verpflichtet § 15 Abs. 2 LDSG ST den Verantwortlichen, (vertraglich) sicherzustellen, dass der Auftragsverarbeiter die Bestimmungen des LDSG ST befolgt und sich der Kontrolle durch den Landesbeauftragten für den Datenschutz unterwirft.

Subsidiär ist auch hier Art. 28 DSGVO anzuwenden.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

Das LKHG ST enthält eine Regelung für spezifische Maßnahmen des Datenschutzes in § 18 LKHG ST. Nach § 18 S. 1 LKHG ST sind für die Wahrung der Rechte und der Interessen der Patienten und der Betroffenen angemessene und spezifische Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbunden Risiken für die Rechte der Patienten und der Betroffenen zu treffen.

Gemäß § 18 S. 2 LKHG ST sind Maßnahmen im Sinne des Satzes 1 insbesondere:

1. technische- und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt,
2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten verarbeitet worden sind,
3. Sensibilisierung und Schulung der an Verarbeitungsvorgängen Beteiligten,
4. Bestellung eines Datenschutzbeauftragten,
5. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
6. Pseudonymisierung personenbezogener Daten,
7. Verschlüsselung personenbezogener Daten,
8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
9. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen, oder
10. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der DSGVO sicherstellen.

Die Vorschrift ist nahezu identisch mit der Vorschrift von Baden-Württemberg oder Nordrhein-Westfalen. Besonders ist jedoch, dass anders als in den anderen Bundesländern sich diese Regelung im LKHG ST und nicht im LDSG ST befindet.

Das LDSG ST enthält ebenfalls eine Regelung zu technischen und organisatorischen Maßnahmen in § 14 LDSG ST.

§ 14 LDSG ST behandelt die Schutzmaßnahmen bei der Verarbeitung besonderer Kategorien personenbezogener Daten. Nach § 14 Abs. 1 LDSG ST sind von den Verantwortlichen und den

Auftragsverarbeitern zur Wahrung der Grundrechte und der Interessen der betroffenen Person Maßnahmen zu treffen, wenn im Rahmen der Datenverarbeitung nach den § 8 LDSG ST (Optische-elektronische Beobachtung),§ 26 LDSG ST (Vorschriften für die Datenverarbeitung im Beschäftigungskontext nach Art. 88 DSGVO), § 27 LDSG ST (Ausnahmen in Bezug auf die Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken nach Art. 89 DSGVO), § 28 LDSG ST (Öffentliche Auszeichnungen und Ehrungen) und § 29 LDSG ST (Begnadigungsverfahren) besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO verarbeitet werden.

Die Verarbeitung von Patientendaten fällt grundsätzlich unter keine der von § 14 LDSG ST genannten Vorschriften. Vor dem Hintergrund, dass sich eine entsprechende Regelung bereits in § 18 LKHG ST finden lässt.

Die Vorgaben an die technischen und organisatorischen Maßnahmen bei der Verarbeitung von Patientendaten ergeben sich somit aus § 18 LKHG ST und im Übrigen aus Art. 32 DSGVO.

3.4.15 Schleswig-Holstein

Auf Krankenhäuser anwendbare Datenschutzvorschriften[282]

Lange Zeit verfügte Schleswig-Holstein lediglich über ein knapp gehaltenes Ausführungsgesetz zum KHG, in dem keine Regelungen zum Datenschutz enthalten waren. Daher war auf die im Allgemeinen geltenden Datenschutzvorschriften zurückzugreifen.

Krankenhäuser öffentlicher Träger

Das LDSG SH gilt nach § 2 Abs. 1 LDSG SH für die Verarbeitung personenbezogener Daten bei öffentlichen Stellen des Landes Schleswig-Holstein. Öffentliche Stellen im Sinne dieses Gesetzes sind Behörden und sonstige öffentliche Stellen der im Landesverwaltungsgesetz genannten Träger der öffentlichen Verwaltung.

§ 2 Abs. 1 LVwG SH nennt das Land, die Gemeinden, die Kreise und die Ämter als Träger der öffentlichen Verwaltung. Ferner sind gemäß § 2 Abs. 2 LVwG SH die der Aufsicht des Landes unterstehenden Körperschaften des öffentlichen Rechts ohne Gebietshoheit und rechtsfähige Anstalten und Stiftungen des öffentlichen Rechts Träger einzelner Aufgaben der öffentlichen Verwaltung. Nach § 2 Abs. 3 LVwG SH können auch natürliche und juristische Personen des Privatrechts sowie nichtrechtsfähige Vereinigungen Träger der öffentlichen Verwaltung für die ihnen übertragenen Aufgaben sein, was allerdings eine Beleihung voraussetzt. Eine solche findet jedoch im Krankenhausbereich in aller Regel nicht statt.[283]

Somit fallen privatrechtliche Vereinigungen, an denen der öffentlichen Hand die Mehrheit der Anteile zusteht, im Gegensatz zum bis 26.01.2012 gültigen § 3 Abs. 1 S. 1 Nr. 2 LDSG SH a.F. nicht mehr schon dann in den Anwendungsbereich des LDSG, wenn sie Aufgaben der öffentlichen Verwaltung wahrnehmen. Die eben genannte Wahrnehmung öffentlicher Aufgaben ist dabei weiter gefasst als die Übertragung öffentlicher Aufgaben. Die Anknüpfung daran schuf nach Auffassung des Landesgesetzgebers Zuordnungsschwierigkeiten, gerade auch bei kommunalen Krankenhäusern, auf deren Geschäftsprozesse ohnehin das BDSG angesichts dessen

[282] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 217 ff.

[283] Mit Ausnahmen bei Unterbringungs- und Maßregelvollzugskliniken, die hier nicht weiter betrachtet werden.

jüngerer Reformen besser passen würde. Aus diesem Grund wurden privatrechtliche Vereinigungen, außer im Fall der Beleihung, mit der Anfang 2012 erfolgten Änderung des LDSG SH vollständig aus dem Anwendungsbereich dieses Gesetzes ausgenommen. Trotz dem Land zugeordneter öffentlicher Trägerschaft gelten für diese somit die Vorschriften des BDSG und außerhalb der Öffnungsklauseln die DSGVO direkt.

Gemäß § 2 Abs. 4 LDSG SH findet das LDSG SH keine Anwendung, soweit öffentliche Stellen nach Abs. 1 am Wettbewerb teilnehmen und personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten. Auch öffentliche Stellen des Landes, die als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten gemäß § 2 Abs. 5 LDSG SH als nicht-öffentliche Stellen. Somit findet in beiden Konstellationen teilweise das BDSG und - außerhalb der Öffnungsklauseln - die DSGVO direkt Anwendung.

Nach § 17 Abs. 1 LDSG SH ist der Landesbeauftragte für Datenschutz Aufsichtsbehörde für die Datenverarbeitung sowohl öffentlicher als – gemäß § 40 BDSG – nicht-öffentlicher Stellen.

Ergebnis: Krankenhausrechtliche Spezialregelungen für den Schutz personenbezogener Daten existieren in Schleswig-Holstein nicht. Somit gelten für in öffentlicher Rechtsform – also als Eigenbetriebe oder Anstalten des öffentlichen Rechts – betriebene Kliniken dem Land zugeordneter öffentlicher Träger (einschließlich der Kommunen) das LDSG SH, im Übrigen aber das BDSG und nachfolgend die DSGVO. Für Kliniken entsprechender öffentlicher Träger in privater Rechtsform (z.B. GmbH, AG) gelten ausschließlich das BDSG und ferner die DSGVO[284].

Krankenhäuser privater Träger

Kliniken in privater Trägerschaft sind keine Stellen, die unter den Anwendungsbereich des LDSG SH fallen. Auf sie sind daher das BDSG und nachfolgend die DSGVO anzuwenden.[285]

Öffnungsklausel für kirchliche Träger?

Es besteht keine Öffnungsklausel.

Zusammenfassung

Krankenhausrechtliche Spezialregelungen für den Schutz personenbezogener Daten existieren in Schleswig-Holstein nicht. Für in öffentlicher Rechtsform betriebene Kliniken dem Land zugeordneter öffentlicher Träger gelten Teile des LDSG SH und im Übrigen das BDSG und ferner die DSGVO. Auf öffentliche Kliniken in privater Rechtsform wie auch auf Kliniken privater Träger sind ausschließlich die Vorschriften des BDSG und ferner die DSGVO anzuwenden.

Das neue Landeskrankenhausgesetz

Zum 1. Januar 2021 ist das neue LKHG SH in Kraft getreten.[286]

[284] Bei beiden Konstellationen wird hier die europarechtskonforme Ausnutzung der in der DSGVO bestehenden Öffnungsklauseln vorausgesetzt.

[285] Europarechtskonforme Nutzung der Öffnungsklauseln vorausgesetzt.

[286] Krankenhausgesetz für das Land Schleswig-Holstein – Landeskrankenhausgesetz - (LKHG) vom 10. Dezember 2020, verkündet am 23. Dezember 2020, GBl. Nr. 22, S. 1004.

Nach § 2 Abs. 1 LKHG SH gilt dieses Gesetz, sofern nichts anderes bestimmt ist, für alle Krankenhäuser im Land Schleswig-Holstein, die der allgemeinen akutstationären oder teilstationären Versorgung dienen, soweit diese nach dem Krankenhausfinanzierungsgesetz förderfähig sind, und für das Universitätsklinikum Schleswig-Holstein sowie für die mit diesen notwendigerweise verbundenen Ausbildungsstätten. Somit gilt dieses neue Krankenhausgesetz vorrangig für Krankenhäuser sowohl öffentlicher als auch privater Träger, abgesehen von nicht förderfähigen reinen Privatkliniken. Im Übrigen bleibt es bei den obigen Ausführungen zu den nachrangigen Gesetzen.

Das neue Gesetz enthält zudem eine Öffnungsklausel für kirchliche Träger in § 2 Abs. 4 LKHG SH, wonach für Krankenhäuser im Sinne des § 2 Abs. 1 LKHG SH, die von Religionsgemeinschaften mit dem Status einer Körperschaft des öffentlichen Rechts oder von diesen zuzuordnenden Einrichtungen betrieben werden, die Vorschriften des Datenschutzes (7. Teil des Gesetzes) nur gelten, soweit die Religionsgemeinschaften keine gleichwertigen Regelungen getroffen haben.

Vorschriften zur Auftragsverarbeitung[287]

Derzeit kein Landeskrankenhausgesetz

In Schleswig-Holstein bestand lange Zeit kein Landeskrankenhausgesetz mit Regelungen zur Auftragsverarbeitung oder auch nur allgemein zum Patientendatenschutz, sondern lediglich ein recht knapp gehaltenes Ausführungsgesetz zum KHG. Vor diesem Hintergrund mussten neben den Anforderungen des Art. 28 DSGVO auch diejenigen des § 203 Abs. 3 StGB eingehalten werden, welcher nach seiner Reformierung im Jahr 2017 immerhin eine Auslagerung von Patientendaten unter Erforderlichkeitsvorbehalt erlaubt.

Geplantes Landeskrankenhausgesetz

Dies hat sich jedoch mit dem Inkrafttreten des neuen LKHG SH zum 1. Januar 2021 geändert. Das neue LKHG SH enthält eine Regelung zur Datenverarbeitung im Auftrag in § 37 LKHG SH. Nach § 37 Abs. 1 S. 1 LKHG SH sind grundsätzlich alle Patientendaten im Krankenhaus zu verarbeiten. Gemäß § 37 Abs. 1 S. 2 LKHG SH kann sich das Krankenhaus zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedienen. Nach § 37 Abs. 2 S. 1 LKHG SH dürfen dem Auftragsverarbeiter Patientendaten nur offenbart werden, soweit dies für die Auftragserfüllung erforderlich ist. Der Krankenhausträger hat gemäß § 37 Abs. 2 S. 2 Halbsatz 1 LKHG SH dem Auftragsverarbeiter, soweit dies für den Auftragszweck ausreichend ist, anonymisierte Daten zur Verfügung zu stellen. Ist eine Anonymisierung nicht möglich, so müssen die Patientendaten gemäß § 37 Abs. 2 Halbsatz 2 LKHG SH pseudonymisiert werden.

Ein früherer Entwurf der Landesregierung enthielt noch weitergehende Vorschriften. So war § 37 Abs. 1 S. 2 LKHG-E SH an weitere Bedingungen geknüpft (beispielsweise: "Störungen im Betriebsablauf können sonst nicht vermieden werden"). § 37 Abs. 3 LKHG-E SH enthielt zudem die Vorgaben, dass sich der Ort der physikalischen Speicherung innerhalb der Europäischen Union befinden muss und der Auftragsverarbeiter jederzeit Auskunft über den Ort zu geben kann. Die Landesregierung führte hierzu aus, dass § 37 Abs. 3 LKHG-E SH sicherstellen solle,

[287] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 279

dass Patientendaten nicht im Wege des sogenannten "Cloud-Computing" außer Kontrolle geraten würden.[288] Der spätere Gesetzesentwurf sowie die finale Fassung enthalten diese Bestimmungen hingegen nicht mehr.[289] Das Entfallen dieser Einschränkung führt jedoch nicht dazu, dass personenbezogene Daten an einen beliebigen Ort übertragen werden dürften. Es gelten weiterhin die Vorgaben der Art. 45 ff. DSGVO und die Vorgaben des "Schrems II"-Urteil des EuGH.

Auch ohne diese entfallenen Einschränkungen sind die Bestimmungen des § 37 LKHG SH vergleichsweise restriktiv. Die weite Erlaubnis des § 37 Abs. 1 S. 2 LKHG SH wird zwar nicht durch § 37 Abs. 1 S. 1 LKHG SH eingeschränkt, da diese Vorschrift angesichts der Systematik wohl nur symbolischen Charakter hat, allerdings gibt § 37 Abs. 2 LKHG SH recht weitreichende Einschränkungen vor, da die Auftragsverarbeitung für Krankenhäuser nur bei Anonymisierung oder zumindest Pseudonymisierung der Daten erlaubt ist. Diese Vorgaben speziell und die Vorschriften über den Patientendatenschutz allgemein wurden daher teilweise als unnötig und zu einschränkend kritisiert.[290]

Das LDSG SH beinhaltet Regelungen zur Auftragsverarbeitung in §§ 38 ff. LDSG SH. Diese sind jedoch auf Krankenhäuser nicht anwendbar, da sich diese Regelungen auf die Auftragsverarbeitung im Zusammenhang mit der Richtlinie (EU) 2016/680 zur Strafverfolgung und Kriminalprävention beziehen. Damit würde für Krankenhäuser auch künftig Art. 28 DSGVO greifen, allerdings nur soweit der LKHG-E SH keine Regelungen zur Auftragsverarbeitung beinhaltet.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

Das LDSG SH enthält in § 12 eine Vorschrift zur Verarbeitung besonderer Kategorien personenbezogener Daten mit einer Regelung zu technischen und organisatorischen Maßnahmen.

§ 12 Abs. 2 LDSG SH bestimmt, dass der Verantwortliche durch geeignete technische wie organisatorische Maßnahmen sicherzustellen hat, dass die Vorgaben der DSGVO eingehalten werden und Grundrechte sowie Interessen der betroffen Person gewahrt werden, wenn auf der Grundlage des Unterabschnitts 3 - § 13 LDSG SH (Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken), § 14 LDSG SH (Videoüberwachung öffentlich zugänglicher Räume), § 15 LDSG SH (Datenverarbeitung im Beschäftigungszusammenhang) und § 16 LDSG SH (Öffentliche Auszeichnungen) - oder einer sonstigen gesetzlichen Regelung im Landesrecht besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO verarbeitet werden.

Gemäß § 1 S. 2 KDSH SG trifft das Gesetz ergänzende Regelungen zur Durchführung der DSGVO. Sind keine ergänzenden Regelungen einschlägig, gilt die DSGVO.

---

[288] Schleswig-Holsteinischer Landtag, Drucksache 19/184: Unterrichtung der Landesregierung vom 10. Oktober 2019, Entwurf eines Landeskrankenhausgesetzes, S. 56.

[289] Schleswig-Holsteinischer Landtag, Drucksache 19/2042: Gesetzentwurf der Landesregierung: "Entwurf eines Krankenhausgesetzes für das Land Schleswig-Holstein - Landeskrankenhausgesetz- (LKHG)" vom 03. März 2020.

[290] Schleswig-Holsteinischer Landtag Umdruck 19/4054: Klinik-Verbund Schleswig-Holstein, "Stellungnahme zum Kabinettsentwurf des Landeskrankenhausgesetzes Schleswig-Holstein (LKHG) vom 03.03.20" vom 19. Mai 2020, S. 6; Schleswig-Holsteinischer Landtag Umdruck 19/4213: Krankenhausgesellschaft Schleswig-Holstein e.V., Stellungnahme zum Entwurf des LKHG, S. 8 f.; Schleswig-Holsteinischer Landtag Umdruck 19/4238: Landes-Arbeitsgemeinschaft der freien Wohlfahrtsverbände Schleswig-Holstein e.V. Stellungnahme zum Entwurf, S. 9.

Die Verarbeitung von Patientendaten fällt grundsätzlich nicht unter einen der in Unterabschnitt geregelten Fälle. Der LKHG-E SH enthält keine Regelungen zur Verarbeitung besonderer Kategorien personenbezogener Daten. Mangels ergänzender landesrechtlicher Regelungen ist daher die DSGVO und somit Art. 32 DSGVO anzuwenden.

Die Vorgaben an die technischen und organisatorischen Maßnahmen ergeben sich allein aus Art. 32 DSGVO

3.4.16 Thüringen

Auf Krankenhäuser anwendbare Datenschutzvorschriften[291]

Krankenhäuser öffentlicher Träger

Gemäß § 3 Abs. 1 S. 1 gilt das LKHG TH für Krankenhäuser, die von der weiten Definition des § 2 Nr. 1 KHG erfasst sind und somit letztlich für alle Krankenhäuser in Thüringen.[292] Die §§ 27, 27a und 27b zum Schutz personenbezogener Daten finden nach § 3 Abs. 5 LKHG TH auch auf Universitätskliniken i. S. d. § 5 Abs. 1 Nr. 1 KHG Anwendung. Für Krankenhäuser im Straf- oder Maßregelvollzug gelten sie hingegen gemäß § 3 Abs. 4 LKHG TH nicht. Die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten sind gemäß § 27 Abs. 2 S. 1 LKHG TH auf Patientendaten anzuwenden, soweit das LKHG TH nichts anderes bestimmt.

Gilt subsidiär das LDSG oder das BDSG?

Gemäß § 2 Abs. 1 gilt das LDSG TH u. a. für die Verarbeitung personenbezogener Daten durch die Behörden, Gerichte und sonstigen öffentlichen Stellen des Landes, der Gemeinden und Gemeindeverbände und die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts.

Nach § 2 Abs. 2 LDSG TH fallen auch juristische Personen und sonstige Vereinigungen des privaten Rechts unter das LDSG TH, wenn sie Aufgaben der öffentlichen Verwaltung wahrnehmen und eine oder mehrere der in § 2 Abs. 1 LDSG TH genannten juristischen Personen des öffentlichen Rechts an ihnen ist bzw. sind. Die Krankenhausversorgung kann, wie § 2 LKHG TH ausdrücklich bestätigt, auch als Aufgabe der öffentlichen Verwaltung wahrgenommen werden.[293] Die Aufgabe der Gewährleistung einer bedarfsgerechten Versorgung der Bevölkerung durch leistungsfähige Krankenhäuser wird dabei dem Land, den Landkreisen sowie den kreisfreien Städten zugewiesen. Somit fallen Kliniken öffentlicher Trägerunter das LDSG TH, wenn sie von einem der in § 2 Abs. 1 und Abs. 2 LDSG TH genannten Träger geführt werden.

Am Vorrang des LKHG TH wird auch insofern festgehalten, als besondere Rechtsvorschriften des Bundes oder des Landes, die den Datenschutz betreffen, dem LDSG TH gemäß § 2 Abs. 3 LDSG TH vorgehen.

Allerdings enthält auch das LDSG TH wie die entsprechenden Vorschriften vieler anderer Bundesländer Sonderregeln für öffentliche Stellen, soweit diese am Wettbewerb teilnehmen, was

[291] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 221 ff.

[292] Schmidt/Seiler/Maier/Vollmöller, LKHG TH, § 3 Erläuterung 1.

[293] Vgl. dazu nähere Ausführungen bei Baden-Württemberg, s.o. S. 80 f.

bei Krankenhäusern regelmäßig der Fall ist.[294] Dies wird jedoch systematisch an anderer Stelle, nämlich in § 26 LDSG TH, geregelt In diesen Fällen sind auf sie, auf ihre Zusammenschlüsse und Verbände von dem LDSG TH nur die Regeln zur Aufsicht anzuwenden (§§ 3 bis 12 LDSG TH). Im Übrigen gelten für sie die Bestimmungen des Teils 2 (§§ 22 bis 31) des BDSG.

Ergebnis: Für den Schutz von Patientendaten in Kliniken öffentlicher Träger gelten in Thüringen folgende Regelungen in absteigender Rangfolge: 1. LKHG TH, 2. LDSG TH oder bei Teilnahme am Wettbewerb Teile des LDSG TH (Regelungen über die Aufsicht) und Teile des BDSG und 3. die DSGVO.[295]

Krankenhäuser privater Träger

Die schon zu den öffentlichen Kliniken erfolgten Ausführungen zum Anwendungsbereich des LKHG TH sind auf Kliniken in privater Trägerschaft übertragbar. Demnach ist das LKHG TH auf solche Kliniken privater Träger anwendbar, bei denen es sich um Krankenhäuser i. S. v. § 2 Nr. 1 KHG und somit um Krankenhäuser im natürlichen Wortsinn handelt. Dass die Datenschutzbestimmungen der §§ 27, 27a und 27b auch auf nicht öffentlich geförderte Krankenhäuser Anwendung finden, wird dabei durch § 3 Abs. 3 LKHG TH klargestellt.[296]

Gilt subsidiär das LDSG oder das BDSG?

Eine Klinik in privater Trägerschaft ist keine Stelle die unter das LDSG TH fällt und insbesondere keine Stellen, die i.S.v. § 2 Abs. 2 S. 3 LDSG TH hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen. Auf sie sind daher nachrangig das BDSG sowie – außerhalb der Öffnungsklauseln - die DSGVO direkt anzuwenden.

Ergebnis: Das LKHG TH gilt für Krankenhäuser nach der weiten Definition des § 2 Nr. 1 KHG vorrangig. Auf Patientendaten sind die jeweils geltenden datenschutzrechtlichen Vorschriften anzuwenden, soweit das LKHG TH nichts anderes bestimmt. Auf Kliniken privater Träger sind nachrangig folglich das BDSG und – außerhalb der Öffnungsklauseln - die DSGVO direkt[297] anzuwenden.

---

[294] S. dazu die entspr. Ausführungen zu Baden-Württemberg, oben S. 80 ff.

[295] Europarechtskonforme Nutzung der in der DSGVO bestehenden Öffnungsklauseln vorausgesetzt.

[296] Die Regelung des § 3 Abs. 3 LKHG TH verwundert, da weder öffentliche Förderung noch (nicht einmal) Förderfähigkeit nach dem KHG überhaupt gemäß Abs. 1 Anwendungsvoraussetzung des LKHG TH ist, sondern insoweit lediglich auf die sehr weite Definition in § 2 Nr. 1 KHG verwiesen wird. Daher wird diese Regel vorliegend nur als „klarstellend" interpretiert. Diese „Verwirrung" liegt möglicherweise daran, dass ursprünglich im Regierungsentwurf zum ersten LKHG TH (Landtags-Drucksache 1/2359) der Anwendungsbereich in § 3 zusätzlich an die Förderung nach dem KGH angeknüpft wurde. Der Entwurf wurde dann jedoch durch mehrere Änderungsanträge abgewandelt, so dass sich in der letztlich angenommenen Beschlussempfehlung (LT-Drucks. 1/3069) einerseits in § 3 Abs. 1 lediglich die Anknüpfung an die weite Definition aus dem KHG (ohne Notwendigkeit der Förderung) findet, andererseits aber in Abs. 3 die nicht mehr dazu passende (sich wohl noch auf den Regierungsentwurf beziehende) „Ausnahme" (u.a. bzgl. des damals noch in § 25 geregelten Datenschutzes), nach der es nicht auf die öffentliche Förderung ankommen soll. Insofern ist auch die Kommentierung von Schmidt/Seiler/Maier/Vollmöller, LKHG TH, in den Erläuterungen 1 (zu Abs. 1) und 3 (zu Abs. 3) etwas widersprüchlich, denn in Erläuterung 1 wird klar festgehalten, dass es bei der Anknüpfung an den weiten § 2 Nr. 1 KHG nicht um die Frage der Förderung geht.

[297] Europarechtskonforme Nutzung der in der DSGVO bestehenden Öffnungsklauseln jeweils vorausgesetzt.

Öffnungsklausel für kirchliche Träger?

Eine Öffnungsklausel für Datenschutzregelungen in kirchlichen Krankenhäusern durch Religionsgesellschaften besteht in Thüringen nicht. Das lässt sich auch daraus schließen, dass § 3 Abs. 1 S. 2, 3 LKHG TH die nicht den Datenschutz betreffenden § 28 Abs. 2 und 3 sowie § 28a für kirchliche Krankenhäuser für nicht anwendbar erklärt. Im Umkehrschluss bedeutet dies, dass der übrige Teil des LKHG TH insbesondere die §§ 27, 27a und 27b über den Patientendatenschutz, für solche Krankenhäuser anwendbar bleibt.[298]

Zusammenfassung

Für alle Krankenhäuser in Thüringen, die unter die weite Definition des § 2 Nr. 1 KHG fallen, gilt das LKHG TH vorrangig. Auf Patientendaten sind die jeweils geltenden Datenschutzvorschriften anzuwenden, soweit das LKHG TH nichts anderes bestimmt. Für öffentliche Kliniken in mittelbarer oder unmittelbarer Landesträgerschaft, auch in privater Rechtsform, gelten nachrangig im Wesentlichen das LDSG TH, bei Teilnahme am Wettbewerb teilweise zusätzlich das BDSG und nachfolgend die DSGVO. Auf Kliniken privater Träger sind nachrangig ausschließlich das BDSG und – außerhalb der Öffnungsklauseln - die DSGVO direkt anzuwenden.[299] Es besteht keine Öffnungsklausel für Regelungen des Datenschutzes in kirchlichen Krankenhäusern durch Religionsgesellschaften.

Vorschriften zur Auftragsverarbeitung[300]

In Thüringen sind Patientendaten gemäß § 27b Abs. 1 S. 1 LKHG TH grundsätzlich im Krankenhaus zu verarbeiten. Eine Verarbeitung und Nutzung durch eine andere Stelle im Auftrag ist nach § 27b Abs. 1 S. 2 LKHG TH nur zulässig, wenn

1) sonst Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger vorgenommen werden können,
2) die Einhaltung der Datenschutzbestimmungen dieses Gesetzes sowie eine den Voraussetzungen des § 203 des Strafgesetzbuchs entsprechende Schweigepflicht beim Auftragnehmer sichergestellt ist und
3) der Auftraggeber der Aufsichtsbehörde nach § 32 Abs. 2 LKHG TH rechtzeitig vor Auftragserteilung Art, Umfang und die technischen und organisatorischen Maßnahmen der beabsichtigten Datenverarbeitung im Auftrag schriftlich angezeigt hat.

Nach § 27b Abs. 2 LKHG TH ist im Auftragsverarbeitungsvertrag sicherzustellen, dass der Auftragnehmer vom Auftraggeber oder von dessen Datenschutzkontrollbehörde veranlasste Kontrollen jederzeit zu ermöglichen hat.

Die Bedingung, dass sie dort erheblich kostengünstiger erbracht werden kann als im Krankenhaus selbst, dürfte ein Text-Mining in der Cloud vorliegend erfüllen. Durch eine entsprechende

[298] Schmidt/Seiler/Maier/Vollmöller, LKHG TH, § 3 Erläuterung 1.3.

[299] Europarechtskonforme Nutzung der Öffnungsklauseln der DSGVO jeweils vorausgesetzt.

[300] Vgl. hierzu mit Stand Mai 2014: Schneider, Sekundärnutzung klinischer Daten, S. 279 f.

vertragliche Gestaltung und die Anzeige bei der Aufsichtsbehörde könnten die übrigen Bedingungen erfüllt werden.

Subsidiär ist in seinem Geltungsbereich das LDSG TH einschlägig. Nach § 19 Abs. 1 LDSG TH ist der Verantwortliche verpflichtet, Auftragsverarbeiter, auf die das LDSG TH, die DSGVO oder das BDSG nicht anwendbar sind, vertraglich zur Einhaltung der DSGVO und des LDSG TH zu verpflichten.

Im Übrigen gilt Art. 28 DSGVO.

Vorschriften zu technischen und organisatorischen (Sicherheits-)Maßnahmen

Das LDSG TH enthält keine Regelung. Gemäß § 1 Abs. 1 LDSG TH trifft das Gesetz nur ergänzende Regelungen zur DSGVO. Sind keine abweichenden Regelungen vorhanden, soll die DSGVO direkt gelten. Art. 32 DSGVO findet Anwendung.

Die Vorgaben an die technischen und organisatorischen Maßnahmen ergeben sich allein aus Art. 32 DSGVO

3.4.17 Überblick: Auf Krankenhäuser anwendbares Datenschutzrecht

Die Komplexität der Bestimmung der jeweils anwendbaren Vorschriften unter Berücksichtigung des Landesrechts kann zusammenfassend der nachfolgenden Tabellenübersicht entnommen werden.

Dabei wird nach Trägerschaft und Art des Krankenhauses (in der Tabelle „Klinik" genannt) sowie nach dessen dem Bundesland differenziert, in dem es seinen Sitz hat. Maßgeblich ist nach den Regeln der Landeskrankenhausgesetze der Sitz, also die räumliche Lokalisierung des einzelnen Krankenhauses, nicht etwa der Hauptsitz einer Krankenhausgruppe.

Die dann für die jeweilige Kombination von Träger, Art des Krankenhauses und Sitz genannten gesetzlichen Grundlagen sind ihrer **Anwendungsreihenfolge** nach geordnet, die auch der speziellen Rangfolge entspricht, soweit zulässigerweise Öffnungsklauseln der DSGVO genutzt wurden, wovon hier grundsätzlich auszugehen ist. Die unter Nr. 1 angeführte Rechtsgrundlage, in der Regel das jeweilige Landeskrankenhausgesetz (LKHG), ist somit zuerst zu prüfen und prinzipiell vorrangig anzuwenden. Die danach als Nummern 2 und gegebenenfalls 3 gelisteten Rechtsgrundlagen sind in absteigender Reihenfolge anzuwenden, soweit die vorrangigen Vorschriften keine Regelungen zu einem Sachverhalt, wie zum Beispiel der Auftragsverarbeitung mit Patientendaten, enthalten.

Soweit für Krankenhäuser öffentlicher Träger an sich das jeweilige Landesdatenschutzgesetz (LDSG) subsidiär auf Stufe 2 anwendbar ist, dieses jedoch für öffentliche Stellen, die am Wettbewerb teilnehmen, auf die für nicht-öffentliche Stellen geltenden Vorschriften verweist, wird diese Verweisung wie folgt in der Tabelle dargestellt: „**LDSG → BDSG**". Dies ist vor dem Hintergrund zu sehen, dass zum einen Krankenhäuser jedenfalls im Behandlungsbereich nach praktisch einhelliger Meinung auch am wirtschaftlichen Wettbewerb teilnehmen. Zum anderen finden sich die allgemeinen datenschutzrechtlichen Vorschriften für nicht-öffentliche Stellen in Deutschland im BDSG, soweit überhaupt ein nationaler Spielraum besteht, also Öffnungsklauseln in der DSGVO europarechtskonform genutzt wurden. Letztlich findet auf Krankenhäuser aber immer auch, zumindest subsidiär, die DSGVO Anwendung.

Welche Vorschriften aus den genannten Rechtsgrundlagen unter welchen Voraussetzungen konkret Anwendung finden, ist den jeweiligen Textabschnitten in diesem Kapitel 3 zu entnehmen.

Ergänzend findet sich in der Tabelle auch die für die Datenschutzaufsicht über das jeweilige Krankenhaus zuständige Behörde, wobei „**BfDI**" für den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit steht, welcher für die wenigen dem Bund zugeordneten Krankenhäuser zuständig ist. „**LfD**" steht für den jeweiligen Landesbeauftragten für den Datenschutz, der im öffentlichen Bereich ausschließlich nach LDSG und DSGVO tätig wird, was durch den Zusatz „(LDSG)" gekennzeichnet ist (bzw. für Bremen durch das entsprechende DSGVO-Ausführungsgesetz – DSGVOAG). Bei nicht-öffentlichen oder diesen gegebenenfalls gleichgestellten (am Wettbewerb teilnehmenden) Krankenhäusern kann der LfD aber auch als Aufsichtsbehörde für den nicht-öffentlichen Bereich tätig werden, was durch den Zusatz „(BDSG)" gekennzeichnet wird. In Bayern ist für den nicht-öffentlichen Bereich das Bayerische Landesamt für Datenschutzaufsicht (**LDA**) zuständig.

Tabelle 3-1: Auf Krankenhäuser anwendbares Datenschutzrecht nach Bundesland und Trägerschaft

Trägerschaft und Art der Klinik / **Sitz der Klinik**	**Öffentliche Träger**		**Private Träger**		**Kirchliche Träger**
	Bund oder diesem zugeordnete Anstalten, Körperschaften, Stiftungen	Land oder diesem zugeordnete Anstalten, Körperschaften, Stiftungen	Plankrankenhaus (in den jeweiligen Krankenhausplan aufgenommen)	Reine Privatklinik (§ 5 Nr. 2 KHG: 40 %-Untergrenze bei der Abrechnung zu GKV-Sätzen nach § 67 AO nicht erreicht)	Öffnungsklausel vorhanden?
Baden-Württemberg	1. BDSG 2. DSGVO Aufsicht: BfDI	Mit eigener Rechtspersönlichkeit (unabhängig von Rechtsform): 1. LKHG 2. LDSG → BDSG 3. DSGVO Aufsicht: LfD (BDSG) Eigen-/Regiebetriebe (keine eigene Rechtspersönlichkeit): 1. LKHG 2. LDSG 3. DSGVO Aufsicht: LfD (LDSG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	Ja: § 43 LKHG BW
Bayern	1. BDSG 2. DSGVO Aufsicht: BfDI	1. LKHG 2. LDSG → BDSG 3. DSGVO Aufsicht: LfD (LDSG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LDA (BDSG)	1. BDSG 2. DSGVO Aufsicht: LDA (BDSG)	Nein
Berlin	1. BDSG 2. DSGVO Aufsicht: BfDI	1. LKHG 2. LDSG → BDSG 3. DSGVO Aufsicht: LfD (LDSG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	Nein
Brandenburg	1. BDSG 2. DSGVO Aufsicht: BfDI	1. KHEG 2. LDSG → BDSG 3. DSGVO Aufsicht: LfD (LDSG)	1. KHEG 2. LDSG 3. DSGVO Aufsicht: LfD (BDSG)	1. KHEG 2. LDSG 3. DSGVO Aufsicht: LfD (BDSG)	Ja: § 25 KHEG BB
Bremen	1. BDSG 2. DSGVO Aufsicht: BfDI	1. LKHG 2. DSGVOAG → BDSG 3. DSGVO Aufsicht: LfD (DSGVOAG)	1. LKHG 2. DSGVOAG 3. DSGVO Aufsicht: LfD (BDSG)	1. LKHG 2. DSGVOAG 3. DSGVO Aufsicht: LfD (BDSG)	Ja: § 1 Abs. 3 KHDSG HB

Trägerschaft und Art der Klinik / Sitz der Klinik	Öffentliche Träger		Private Träger		Kirchliche Träger
	Bund oder diesem zugeordnete Anstalten, Körperschaften, Stiftungen	Land oder diesem zugeordnete Anstalten, Körperschaften, Stiftungen	Plankrankenhaus (in den jeweiligen Krankenhausplan aufgenommen)	Reine Privatklinik (§ 5 Nr. 2 KHG: 40 %-Untergrenze bei der Abrechnung zu GKV-Sätzen nach § 67 AO nicht erreicht)	Öffnungsklausel vorhanden?
Hamburg	1. BDSG 2. DSGVO Aufsicht: BfDI	Private Rechtsform: 1. LKHG 2. LDSG → BDSG 3. DSGVO Aufsicht: LfD (BDSG) Öffentl. Rechtsform: 1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (LDSG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	1. BDSG 2. DSGVO Aufsicht: LfD (BDSG)	Ja: § 7 Abs. 4 LKHG HH
Hessen	1. BDSG 2. DSGVO Aufsicht: BfDI	1. LKHG 2. LDSG 3. DSGVO Aufsicht: LfD (LDSG)	1. LKHG 2. LDSG 3. DSGVO Aufsicht: LfD (LDSG)	1. BDSG 2. DSGVO Aufsicht: LfD (BDSG)	Ja: § 12 Abs. 5 LKHG HE
Mecklenburg-Vorpommern	1. BDSG 2. DSGVO Aufsicht: BfDI	1. LKHG 2. LDSG → BDSG 3. DSGVO Aufsicht: LfD (LDSG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	Soweit akut-stationär: 1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG) Im Übrigen: 1. BDSG 2. DSGVO Aufsicht: LfD (BDSG)	Nein
Niedersachsen	1. BDSG 2. DSGVO Aufsicht: BfDI	1. LDSG → BDSG 2. DSGVO Aufsicht: LfD (LDSG)	1. BDSG 2. DSGVO Aufsicht: LfD (BDSG)	1. BDSG 2. DSGVO Aufsicht: LfD (BDSG)	Nein
Nordrhein-Westfalen	1. BDSG 2. DSGVO Aufsicht: BfDI	1. GDSG 2. LDSG 3. DSGVO Aufsicht: LfD (LDSG)	1. GDSG 2. LDSG 3. DSGVO Aufsicht: LfD (BDSG)	1. BDSG 2. DSGVO Aufsicht: LfD (BDSG)	Ja: § 2 Abs. 3 GDSG NW

Trägerschaft und Art der Klinik / Sitz der Klinik	Öffentliche Träger		Private Träger		Kirchliche Träger
	Bund oder diesem zugeordnete Anstalten, Körperschaften, Stiftungen	Land oder diesem zugeordnete Anstalten, Körperschaften, Stiftungen	Plankrankenhaus (in den jeweiligen Krankenhausplan aufgenommen)	Reine Privatklinik (§ 5 Nr. 2 KHG: 40 %-Untergrenze bei der Abrechnung zu GKV-Sätzen nach § 67 AO nicht erreicht)	Öffnungsklausel vorhanden?
Rheinland-Pfalz	1. BDSG 2. DSGVO Aufsicht: BfDI	1. LKHG 2. LDSG → BDSG 3. DSGVO Aufsicht: LfD (LDSG)	1. LKHG 2. LDSG/BDSG 3. DSGVO Aufsicht: LfD (BDSG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	Ja: § 38 LKHG RP
Saarland	1. BDSG 2. DSGVO Aufsicht: BfDI	1. LKHG 2. LDSG → BDSG 3. DSGVO Aufsicht: LfD (LDSG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	1. LKHG 2. DSGVO Aufsicht: LfD (BDSG)	Ja: § 2 Abs. 2 LKHG SL
Sachsen	1. BDSG 2. DSGVO Aufsicht: BfDI	Mit eigener Rechtspersönlichkeit (unabhängig von Rechtsform): 1. LKHG 2. DSDG → BDSG 3. DSGVO Aufsicht: LfD (BDSG) Eigen-/Regiebetriebe (keine eigene Rechtspersönlichkeit): 1. LKHG 2. DSDG 3. DSGVO Aufsicht: LfD (DSDG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	1. BDSG 2. DSGVO Aufsicht: LfD (BDSG)	Nein
Sachsen-Anhalt	1. LKHG 2. DSGVO Aufsicht: BfDI	1. LKHG 2. LDSG → BDSG 3. DSGVO Aufsicht: LfD (LDSG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	Nein

Trägerschaft und Art der Klinik / Sitz der Klinik	Öffentliche Träger		Private Träger		Kirchliche Träger
	Bund oder diesem zugeordnete Anstalten, Körperschaften, Stiftungen	Land oder diesem zugeordnete Anstalten, Körperschaften, Stiftungen	Plankrankenhaus (in den jeweiligen Krankenhausplan aufgenommen)	Reine Privatklinik (§ 5 Nr. 2 KHG: 40 %-Untergrenze bei der Abrechnung zu GKV-Sätzen nach § 67 AO nicht erreicht)	Öffnungsklausel vorhanden?
Schleswig-Holstein	1. BDSG 2. DSGVO Aufsicht: BfDI	Öffentl. Rechtformen: 1. LKHG 2. LDSG → BDSG 3. DSGVO Aufsicht: LfD (BDSG) Private Rechtsformen: 1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	1. BDSG 2. DSGVO Aufsicht: LfD (BDSG)	Nein
Thüringen	1. BDSG 2. DSGVO Aufsicht: BfDI	1. LKHG 2. LDSG → BDSG 3. DSGVO Aufsicht: LfD (LDSG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	1. LKHG 2. BDSG 3. DSGVO Aufsicht: LfD (BDSG)	Nein

3.4.18 Überblick: Anforderungen an die Auftragsverarbeitung für Krankenhäuser

Im Hinblick auf die Vorgaben für die Auftragsverarbeitung kann vor dem Hintergrund der Regelung in den Landeskrankenhausgesetzen und durch die Schweigepflicht, soweit die Bundesländer keine eigenen Befugnisnormen zu deren Durchbrechung beinhalten, folgende Grobklassifikation vorgenommen werden.[301]

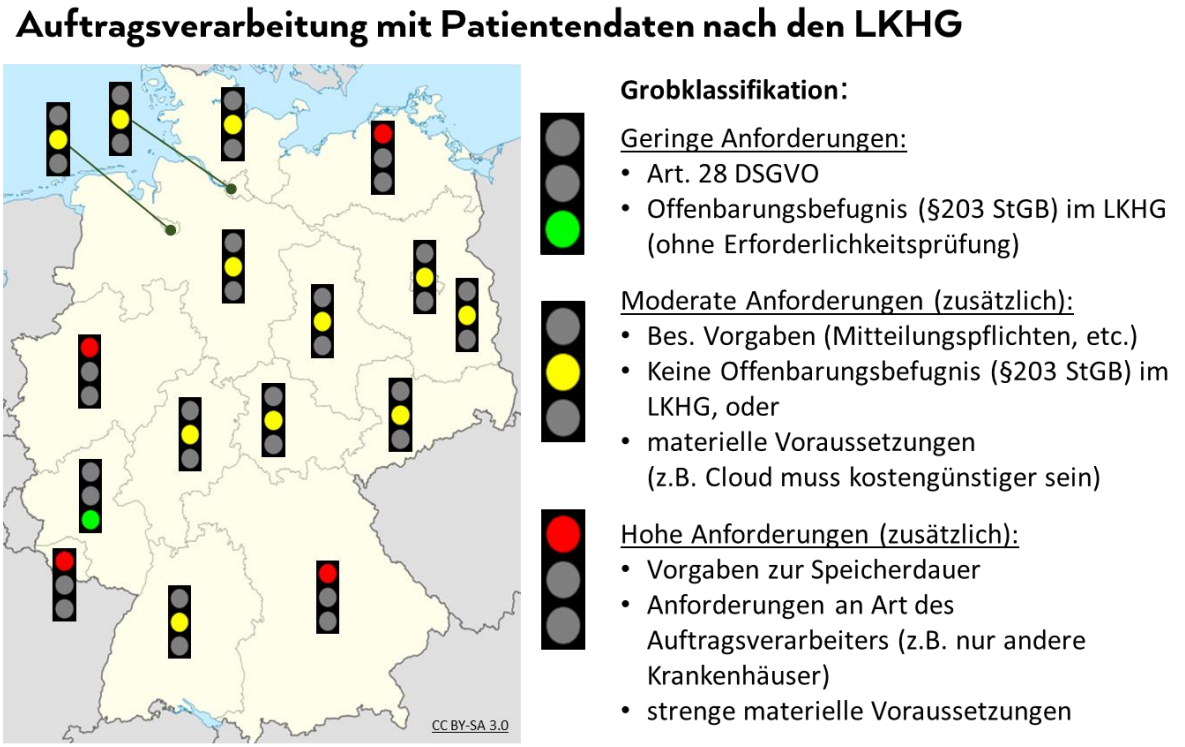

Abb. 3-2: Auftragsverarbeitung mit Patientendaten nach den LKHG[302]

In etwas feinerer Granularität lassen sich die Anforderungen an die Auftragsverarbeitung in den jeweiligen Landeskrankenhausgesetzen wie in nachfolgender Übersichtstabelle klassifizieren:

[301] Die bundeseinheitlichen Regelungen zur Übermittlung von Leistungsdaten nach §§ 294 ff. SGB V werden hier nicht berücksichtigt, können aber auch nur die Auslagerung von Abrechnungsmodulen eines KIS in die Cloud erschweren, nicht aber von rein medizinischen Modulen.

[302] Zu Berlin wird dabei die geltende Rechtslage zugrunde gelegt und nicht der schon verkündete, aber erst im Oktober 2022 in Kraft tretende § 24 Abs. 7 LKHG BE, der die Ampel dort auf Rot springen ließe. Quelle der Vorlage der Deutschlandkarte mit Bundeslandgrenzen: https://commons.wikimedia.org/wiki/Deutschland#/media/File:Germany_location_map.svg; Urheber: https://commons.wikimedia.org/wiki/User:NordNordWest; Lizenz: https://creativecommons.org/licenses/by-sa/3.0/. Ergänzung der Ampelsymbole: eigene Darstellung; Lizenz ebenfalls: https://creativecommons.org/licenses/by-sa/3.0/.

Tabelle 3-2: Anforderungen an die Auftragsverarbeitung nach den jeweiligen Landesvorschriften

Bundesland	Art des Auftragnehmers	Sitz des Auftragnehmers	Weitere Verpflichtungen des Auftragnehmers	Sonstige materielle Anforderungen	Obligate Einschaltung der Datenschutzaufsicht
Baden-Württemberg § 48 LKHG	Anderes Krankenhaus oder Rechenzentrum [LKHG]	Keine speziellen Anforderungen	- Schriftliche Festlegung der nach LDSG und BDSG erforderlichen Maßnahmen [LKHG] - Schweigepflicht (§ 203 StGB) [LKHG]	Keine speziellen Anforderungen	Pflicht des Auftraggebers zur Mitteilung des Auftrages an die Datenschutzaufsichtsbehörde [LKHG]
Bayern Art. 27 Abs. 4 LKHG	Grds. nur andere Krankenhäuser oder KIS im administrativen Bereich [LKHG]	Keine speziellen Anforderungen	Besondere Schutzmaßnahmen technischer und organisatorischer Art [LKHG]	Keine Beeinträchtigung von Belangen der Patienten [LKHG]	Keine speziellen Anforderungen
Berlin § 24 Abs. 1 LKHG § 26 Abs. 3 LDSG (bis September 2022)	Keine speziellen Anforderungen	Wartungsarbeiten mit der Möglichkeit der Kenntniserlangung personenbezogener Daten durch Stellen außerhalb des Geltungsbereichs der DSGVO sind nur zulässig, wenn sie erforderlich sind [LDSG]	Keine speziellen Anforderungen	Sicherstellung, dass nur auf die für die Wartung erforderlichen personenbezogenen Daten zugegriffen werden kann [LDSG]	Keine speziellen Anforderungen
Berlin § 24 Abs. 7 LKHG (ab Oktober 2022) § 26 Abs. 3 LDSG (wie bis September 2022)	Verarbeiter muss gleicher Unternehmensgruppe /Unternehmensgruppe eines anderen Krankenhauses angehören [LKHG]	Verarbeitung nur durch Personen, die Geheimhaltungspflicht nach Unionsrecht oder Recht eines Mitglieds der EU unterliegen [LKHG]	Keine speziellen Anforderungen	Wenn Verarbeiter weder Unternehmensgrupp Krankenhaus/anderes Krankenhaus angehört und nicht unter Geheimhaltungspflicht fällt, dann technische Maßnahmen, dass Verarbeiter keinen Zugriff auf Personenbezug hat [LKHG]	Keine speziellen Anforderungen
Brandenburg	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen

Bundesland	Art des Auftragnehmers	Sitz des Auftragnehmers	Weitere Verpflichtungen des Auftragnehmers	Sonstige materielle Anforderungen	Obligate Einschaltung der Datenschutzaufsicht
Bremen **§ 41 LKHG**	Keine speziellen Anforderungen	Keine speziellen Anforderungen	- Schweigepflicht (§ 203 StGN) [LKHG]	- Störungen im Betriebsablauf sonst nicht vermeidbar, oder - Verarbeitung erheblich kostengünstiger, oder - Datenverarbeitung vom Krankenhaus nicht oder nur mit einem großen Aufwand geleistet werden kann, oder - Patientenakten oder ähnliche Unterlagen in Papierform einzuscannen und zu digitalisieren sind.	Keine speziellen Anforderungen
Hamburg	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen
Hessen	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen
Mecklenburg-Vorpommern **§ 38 LKHG**	Keine speziellen Anforderungen	Wenn außerhalb des Anwendungsbereichs des Grundgesetzes: Einwilligung Patient / Geheimhaltungspflicht Verarbeiter aufgrund ausländischen Rechts [LKHG]	- Schweigepflicht (§ 203 StGB) [LKHG] - Pflicht zur Ermöglichung der Einsicht in Daten durch Patient für 10 Jahre (nur bei Übernahme nach Betriebsaufgabe) [LKHG] - Speicherung über drei Monate nur zulässig, wenn Daten auf getrennten Datenträgern gespeichert [LKHG]	- Störungen im Betriebsablauf sonst nicht vermeidbar [LKHG] oder - Verarbeitung erheblich kostengünstiger [LKHG] oder - Betriebsaufgabe [LKHG] UND - Erforderlichkeit [LKHG]	Keine speziellen Anforderungen
Niedersachsen	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen

Bundesland	Art des Auftragnehmers	Sitz des Auftragnehmers	Weitere Verpflichtungen des Auftragnehmers	Sonstige materielle Anforderungen	Obligate Einschaltung der Datenschutzaufsicht
Nordrhein-Westfalen § 7 GDSG	Keine speziellen Anforderungen	Keine speziellen Anforderungen	- Schweigepflicht (§ 203 StGB) [GDSG] - Aufbewahrung Daten in physisch getrennten Dateien (nur ärztlicher Bereich) [GDSG]	- Störungen im Betriebsablauf sonst nicht vermeidbar [GDSG] / - Verarbeitung erheblich kostengünstiger [GDSG]	Keine speziellen Anforderungen
Rheinland-Pfalz § 33 Abs. 9 LKHG	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen
Saarland § 13a LKHG	Keine speziellen Anforderungen	Wenn außerhalb des Anwendungsbereichs des LKHG: - Verpflichtung auf entsprechenden Datenschutz [LKHG] - Unterwerfung unter die Aufsicht des LfDI [LKHG]	- schriftliche Vereinbarung von Maßnahmen [LKHG] - Pflicht zur Ermöglichung der Einsicht in Daten durch Patient für 10 Jahre (bei Übernahme nach Betriebsaufgabe) [LKHG] - Speicherung über drei Monate nur zulässig, wenn Daten auf getrennten Datenträgern gespeichert [LKHG]	- Störungen im Betriebsablauf sonst nicht vermeidbar [LKHG] oder - Verarbeitung erheblich kostengünstiger [LKHG] oder - Betriebsaufgabe [LKHG] UND: - im Interesse der Patienten [LKHG] oder - pseudonymisierte Patientendaten [LKHG]	Pflicht zur Übersendung Dokumente an Behörden [LKHG]
Sachsen § 33 Abs. 8 LKHG	Keine speziellen Anforderungen	Keine speziellen Anforderungen	- Schweigepflicht (§ 203 StGB) [LKHG] - Benennung Datenschutzbeauftragter [LKHG]	Keine speziellen Anforderungen	Zustimmung Behörde erforderlich [LKHG]
Sachsen-Anhalt § 16 Abs. 4 LKHG	Keine speziellen Anforderungen	Verpflichtung Anwendbarkeit LDSG und Kontrolle LfDI [LKHG]	- Schweigepflicht (§ 203 StGB) [LKHG] - Angemessene Mittel zur Vermeidung von Risiken [LKHG]	- Erforderlichkeit [LKHG] - Keine Beeinträchtigung Belange von Patienten [LKHG] - Mitteilungspflicht an Patienten [LKHG]	Keine speziellen Anforderungen
Schleswig-Holstein § 37 LKHG	Keine speziellen Anforderungen	Keine speziellen Anforderungen	Keine speziellen Anforderungen	- Erforderlichkeit - Anonymisierung, soweit möglich/ausreichend - Pseudonymisierung im Übrigen	Keine speziellen Anforderungen

Bundesland	Art des Auftragnehmers	Sitz des Auftragnehmers	Weitere Verpflichtungen des Auftragnehmers	Sonstige materielle Anforderungen	Obligate Einschaltung der Datenschutzaufsicht
Thüringen **§ 27b LKHG**	Keine speziellen Anforderungen	Verpflichtung DSGVO und LDSG [LDSG]	- Schweigepflicht (§ 203 StGB) [LKHG] - Befugnis zur jederzeitigen Kontrolle durch Auftraggeber oder LfD [LKHG]	- Störungen im Betriebsablauf sonst nicht vermeidbar [LKHG] oder - Verarbeitung erheblich kostengünstiger [LKHG]	Mitteilung an Aufsichtsbehörde [LKHG]

3.4.19 Überblick: Technische und organisatorische Maßnahmen nach Landesrecht

Die Bundesländer regeln teilweise konkrete Maßnahmen als Vorgaben oder Vorschläge für die technischen und organisatorischen Maßnahmen bei der Verarbeitung von Patientendaten in ihren Landesdatenschutz- und Landeskrankenhausgesetzen. Folgende Tabelle enthält eine Übersicht dahingehend, ob Gesetze der Bundesländer solche Vorgaben und ob diese auf die Verarbeitung von Patientendaten Anwendung finden. Die Spalte „Eingeschränkter Anwendungsbereich der TOM" zeigt an, ob diese Maßgaben für jegliche Verarbeitung personenbezogener Daten im Anwendungsbereich der Landesgesetze gelten (dann mit „-" markiert) oder ob dies an zusätzliche Voraussetzungen geknüpft ist, wie zum Beispiel Auftragsverarbeitung oder Fernwartung in Berlin oder die Verarbeitung besonderer Kategorien personenbezogener Daten in Bremen (dann mit „+" gekennzeichnet).

Tabelle 3-3*: Vorgaben zu technischen und organisatorischen Maßnahmen (TOM) für Krankenhäuser im Landesrecht*

Bundesland	Regelung zu TOM im LDSG / LKHG	Eingeschränkter Anwendungsbereich der TOM	Anwendung auf die Verarbeitung von Patientendaten zu Behandlungszwecken
BW	+ (§ 3 LDSG BW)	-	+
BY	-	-	-
BE	+ (§ 26 LDSG BE)	+	+
BB	+ (§ 24 LDSG BB)	+	+
HB	+ (§ 11 DSGVOAG HB)	+	+
HH	-	-	-
HE	+ (§ 20 LDSG HE)	+	+
MV	+ (§ 8 LDSG MV)	+	-
NI	+ (§ 17 LDSG NI)	+	+
NW	+ (§ 15 LDSG NW)	-	+
RP	+ (19 LDSG RP)	+	+
SL	+ (§ 8 LDSG SL)	+	+
SN	-	-	-
ST	+ (§ 18 LKHG ST und § 14 LDSG ST)	-	+
SH	+ (§ 12 LDSG SH)	+	-
TH	-	-	-

3.5 Datenschutzrechtliche Anforderungen an Cloud-KIS in kirchlichen Krankenhäusern

3.5.1 Vorbemerkung zur Anwendbarkeit der kirchlichen Datenschutzregeln

Die Position der beiden großen Kirchen in Deutschland

Im Zuge der Einführung der DSGVO erließen sowohl die evangelische als auch die katholische Kirche eigene Datenschutzgesetze. Zuvor war es den Kirchen im Krankenhausdatenschutz nach verbreiteter Meinung nur bei Bestehen von Öffnungsklauseln erlaubt, eigene Regelungen zu erlassen.[303] Nach Ansicht der beiden Kirchen sollen diese neuen Datenschutzgesetze aber nun bundesweit gelten. Dies leiten die Kirchen aus Art. 91 DSGVO ab, der es ermögliche, bestehende (kirchliche) Datenschutzvorschriften weiter anzuwenden, wenn sie mit der EU-DSGVO in Einklang gebracht würden. Die DSGVO und das BDSG würden daher nicht für den Anwendungsbereich der kirchlichen Datenschutzgesetze gelten.[304]

Kritik an der kirchlichen Rechtssetzungskompetenz für Patientendaten

Diese Ansicht der Kirchen ist sehr zweifelhaft. Der Wortlaut des Art. 91 Abs. 1 DSGVO könnte zwar so interpretiert werden, dass er eine Öffnung der DSGVO nicht gegenüber den Mitgliedstaaten, sondern direkt gegenüber Kirchen oder religiösen Vereinigungen oder Gemeinschaften enthält, ohne dass ein Mitgliedstaat diese Öffnung für Kirchen bestätigen oder regulieren müssten. Dies gilt aber jedenfalls nur dann, wenn die Kirchen bei Inkrafttreten der DSGVO schon umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung angewendet haben, was jedenfalls aufgrund der bisherigen deutschen Regeln bezüglich dem Patientendatenschutz in einigen Bundesländern nicht gegeben war.

Zudem verweist der korrespondierende Erwägungsgrund 165 der DSGVO auf den Status, den Kirchen in den Mitgliedstaaten nach deren bestehenden verfassungsrechtlichen Vorschriften genießen. Lediglich dieser durch das nationale Verfassungsrecht bedingte Status wird durch die DSGVO im Einklang mit Art. 17 Abs. 1, 2 AEUV geachtet und nicht beeinträchtigt.

Vor diesem Hintergrund ist das kirchliche Selbstbestimmungsrecht nach Art. 137 Abs. 3 S. 1 der Weimarer Reichsverfassung, die nach Art. 140 GG insoweit fort gilt, aber auch die dort vorgenommene Eingrenzung dieser Selbstbestimmung auf die eigenen Angelegenheiten der Kirchen „innerhalb der Schranken des für alle geltenden Gesetzes" auch im Datenschutz nach wie vor zu beachten.

Der Patientendatenschutz in Krankenhäusern ist davon nach hier vertretener Auffassung, mit Ausnahme einer eventuellen Krankenhausseelsorge, jedoch nicht umfasst. Denn die medizinische Versorgung der Bevölkerung, gerade wenn sie aus Mitteln der GKV finanziert wird, gehört

[303] Schneider, Sekundärnutzung klinischer Daten, S. 80 f.

[304] So das FAQ der Bischofskonferenz zum KDG: https://www.dbk.de/themen/kirche-staat-und-recht/datenschutz-faq (Stand 15.12.2020). Der Sache nach vertritt auch die Evangelische Kirche in Deutschland diese Position.

nicht zu den eigenen oder gar inneren Angelegenheiten der Kirchen, für welche diese eigene Regelungen erlassen dürften – auch nicht nach Art. 91 DSGVO.[305]

Daher muss für eigenständige Regelungen der Kirchen auf dem Gebiet des Patientendatenschutzes im Krankenhaus weiterhin zumindest eine Öffnungsklausel im Landesrecht bestehen, die als Befugnis zum Erlass von kirchlichen Datenschutzbestimmungen dient. Verfassungsrechtlich geboten erscheint dies jedoch nach den bereits gemachten Ausführungen keineswegs, falls es überhaupt zulässig wäre.[306]

Im Folgenden sollen gleichwohl exemplarisch einzelne Regelungen der beiden großen deutschen Kirchen vorgestellt werden.

3.5.2 Evangelische Kirche

Auf Krankenhäuser anwendbare Datenschutzvorschriften

Bundeseinheitlich soll in der evangelischen Kirche das Datenschutzgesetz der evangelischen Kirche in Deutschland (DSG-EKD) gelten.

Zur Anwendbarkeit der kirchlichen Datenschutzregelungen auf kirchliche Krankenhäuser in Abgrenzung zum staatlichen Recht sei auf die eben gemachten Ausführungen verwiesen. Diese Anwendung kirchlicher Regeln auf Krankenhäuser ist damit letztlich nach hier vertretener Auffassung von einer Öffnungsklausel in den jeweiligen Landeskrankenhausgesetzen (LKHG) abhängig.

Dies könnte auch mit § 2 Abs. 6 DSG-EKD in Einklang gebracht werden, wonach andere Rechtsvorschriften, die kirchliche Stellen anzuwenden haben, dem Kirchengesetz vorgehen, soweit sie die Verarbeitung personenbezogener Daten regeln.

Nach § 2 Abs. 2 DSG-EKD gilt das Kirchengesetz für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Gemäß § 2 Abs. 3 DSG-EKD findet das Kirchengesetz Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit einer kirchlichen Stelle oder in deren Auftrag, unabhängig vom Ort der Verarbeitung.

Der Umgang mit Gesundheitsdaten auch für Behandlungszwecke ist in § 13 Abs. 1 DSK-EKD geregelt. Besondere Vorschriften zur Auftragsverarbeitung finden sich hier jedoch nicht.

---

[305] Im Ergebnis gleicher Meinung, jedenfalls für die bundeslandübergreifende Forschung unter Beteiligung von kirchlichen Krankenhäusern, in der Tendenz aber auch für die Behandlung, mit ausführlicherer Begründung und Darstellung des Streitstandes: Dierks, Lösungsvorschläge für ein neues Gesundheitsforschungsdatenschutzrecht in Bund und Ländern, S. 77 ff. m.w.N. Ebenso Kircher, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, 2016, S. 116; S. 249 dort Nr. 7.

[306] Man muss dabei auch bedenken, dass kirchlichen Gemeinschaften eine Rechtssetzungsbefugnis mit Wirkung für alle Patienten ihrer Krankenhäuser eingeräumt würde, ganz gleich, ob diese der entsprechenden Kirchen angehören und damit theoretisch – zumindest in der evangelischen Kirche – über Wahlen zum Kirchenparlament Einfluss auf diese Regelungen nehmen könnten. Wenn solche Krankenhäuser jedoch in einen Landeskrankenhausplan aufgenommen wurden, werden sie maßgeblich über GKV-Beiträge sowie Investitionszuschüsse des Staates finanziert und müssen allen Patienten offenstehen.

Grundsätzlich gilt somit für die Verarbeitung von Gesundheits- und Patientendaten für alle evangelischen Kirchen das DSG-EKD, soweit eine landesrechtliche Öffnungsklausel vorhanden ist. Nachrangig gelten gegebenenfalls landesrechtliche Bestimmungen oder das BDSG und im Übrigen die DSGVO.

Evangelische Landeskirche in Baden-Württemberg als exemplarisches Beispiel

Nach § 54 Abs. 1 DSG-EKD kann der Rat der Evangelischen Kirche in Deutschland durch Rechtsverordnung mit Zustimmung der Kirchenkonferenz Durchführungsbestimmungen zu diesem Kirchengesetz oder ergänzende Bestimmungen zum Datenschutz erlassen. Dies wurde mit der Verordnung zur Sicherheit der Informationstechnik (ITSVO) vorgenommen.[307] Nach § 6 Abs. 1 ITSVO-EKD können die Evangelische Kirche in Deutschland, die Gliedkirchen und die gliedkirchlichen Zusammenschlüsse jeweils für ihren Bereich Durchführungsbestimmungen zu dieser Verordnung und ergänzende Bestimmungen zur IT-Sicherheit erlassen, soweit sie dieser Verordnung nicht widersprechen.

Nach § 54 Abs. 2 DSG-EKD können die Gliedkirchen für ihren Bereich Durchführungsbestimmungen zu diesem Kirchengesetz und ergänzende Bestimmungen zum Datenschutz erlassen, soweit sie dem Recht der Evangelischen Kirche in Deutschland nicht widersprechen.

Dies wurde beispielsweise durch die Evangelische Landeskirche in Württemberg durch die 905. Kirchliche Verordnung zur Durchführung und Ergänzung des EKD-Datenschutzrechts (DSDEVO)[308] vorgenommen, die auf § 25 Abs. 4 Kirchenverfassungsgesetz, § 54 Abs. 2 DSG-EKD und § 6 Abs. 1 ITSVO beruht. Das LKHG BW enthält eine Öffnungsklausel, sodass auch nach hier vertretener Auffassung eine eigene Regelung der evangelischen Kirche vertretbar ist.

Die Evangelische Landeskirche in Württemberg hat beispielsweise gemäß §§ 2 Abs. 1 Satz 1, 8 DSDEVO, § 1 ff. Datenschutzkirchenbezirksfestlegungsverordnung (DKBFVO)[309] für die Bestellung eines örtlich Beauftragten für Datenschutz neben dem Kirchenkreis Stuttgart jeweils die Kirchenbezirke im Zuständigkeitsbereich einer Kirchlichen Verwaltungsstelle zusammengefasst.

Für die Evangelische Landeskirche in Württemberg sind somit die Bestimmungen der DSDEVO, der ITSVO-EKD und des DSG-EKD und im Übrigen gegebenenfalls weitere landesrechtliche Bestimmungen, sowie außerhalb der Nutzung von Öffnungsklauseln die DSGVO maßgebend.

Zusammenfassung

Für Krankenhäuser der evangelischen Kirche gelten – sofern eine Öffnungsklausel im Landesrecht vorliegt - das DSG-EKD und die ITSVO-EKD. Die einzelnen Landeskirchen können wiederum eigene Regelungen in Verordnungen festlegen, was beispielsweise durch die Evangelische

[307] Verordnung zur Sicherheit der Informationstechnik (IT-Sicherheitsverordnung – ITSVO-EKD) vom 29. Mai 2015 (ABl. EKD s. 146); Ermächtigung noch nach § 9 Abs. 2 Satz 2 DSG-EKD a.F.

[308] 905. Kirchliche Verordnung zur Durchführung und Ergänzung des EKD-Datenschutzrechts (Datenschutzdurchführungs- und -ergänzungsverordnung – DSDEVO) vom 14 Mai 2018 (Abl. 68 S. 56).

[309] 906. Verordnung des Oberkirchenrats über die Festlegung von Kirchenbezirken bezüglich der Bestellung von örtlichen Beauftragten für den Datenschutz und für IT-Sicherheit (Datenschutzkirchenbezirksfestlegungsverordnung – DKBFVO) vom 21. Mai 2019

Landeskirche in Württemberg mit der DSDEVO vorgenommen wurde. Im Übrigen gelten landesrechtliche Regelungen und außerhalb der Nutzung von Öffnungsklauseln die DSGVO direkt.

Vorschriften zur Auftragsverarbeitung

Das DSG-EKD enthält Regelungen zur Auftragsverarbeitung.

Auftragsverarbeiter im Sinne des DSG-EKD ist gemäß § 4 Nr. 10 DSG-EKD eine natürliche oder juristische Person, kirchliche oder sonstige Stelle, die personenbezogene Daten im Auftrag der verantwortlichen Stelle verarbeitet.

Kapitel 4 des DSG-EKD behandelt die Pflichten der verantwortlichen Stellen und Auftragsverarbeiter.

Nach § 26 DSG-EKD ist es den bei der Datenverarbeitung tätigen Personen untersagt, personenbezogene Daten unbefugt zu verarbeiten. Diese sind bei der Aufnahme ihrer Tätigkeit auf dieses Datengeheimnis schriftlich zu verpflichten, soweit sie nicht aufgrund anderer kirchlicher Bestimmungen zur Verschwiegenheit verpflichtet wurden. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

Nach § 30 Abs. 1 DSG-EKD bleibt die auftraggebende kirchliche Stelle für die Einhaltung der Vorschriften des DSG-EKD und anderer Vorschriften über den Datenschutz verantwortlich, wenn personenbezogene Daten im Auftrag durch andere Stellen oder Personen verarbeitet werden. Die Rechte der betroffenen Person nach Kapitel 3 des DSG-EKD sind ihr gegenüber geltend zu machen und zuständig für die Aufsicht ist die Aufsichtsbehörde der beauftragenden kirchlichen Stelle.

Gemäß § 30 Abs. 2 DSG-EKD gilt für eine Auftragsverarbeitung in Drittländer § 10 DSG-EKD (Datenübermittlung an und in Drittländer oder an internationale Organisationen).

§ 30 Abs. 3 Satz 1 DSG-EKD bestimmt, dass der Auftragsverarbeiter unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist gemäß § 30 Abs. 3 Satz 2 DSK-EKD schriftlich zu erteilen, wobei insbesondere

1. der Gegenstand und die Dauer des Auftrags, 2.
2. der Umfang, die Art und der Zweck der vorgesehenen Verarbeitung, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 27 DSG-EKD zu treffenden technischen und organisatorischen Maßnahmen sowie ihre Kontrolle durch den Auftragsverarbeiter,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die Verpflichtung der Beschäftigten des Auftragsverarbeiters auf das Datengeheimnis,
6. gegebenenfalls die Berechtigung zur Begründung sowie die Bedingungen von Unterauftragsverhältnissen,
7. die Kontrollrechte der beauftragenden kirchlichen Stelle und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragsverarbeiters,

8. mitzuteilende Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnis, die sich die beauftragende kirchliche Stelle gegenüber dem Auftragsverarbeiter vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragsverarbeiter gespeicherter Daten nach Beendigung des Auftrags.

Nach §§ 30 Abs. 3 Satz 3, Satz 4 DSG-EKD hat sich die beauftragende Stelle vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen und das Ergebnis schriftlich festzuhalten.

Gemäß § 30 Abs. 4 DSG-EKD darf der Auftragsverarbeiter die Daten nur im Rahmen der Weisungen der kirchlichen Stellen verarbeiten und er hat die kirchliche Stelle unverzüglich darauf hinzuweisen, wenn er der Ansicht ist, dass eine Weisung der kirchlichen Stelle gegen dieses Kirchengesetz oder andere Vorschriften über den Datenschutz verstößt.

Nach § 30 Abs. 5 Satz 1 DSK-EKD ist die kirchliche Stelle verpflichtet sicherzustellen, dass der Auftragsverarbeiter diese oder gleichwertige Bestimmungen beachtet, sofern die kirchlichen Datenschutzbestimmungen auf den Auftragsverarbeiter keine Anwendung finden. In diesem Fall dürfen sich gemäß § 30 Abs. 5 Satz 2 DSG-EKD die Vertragsinhalte abweichend von Absatz 3 an Art. 28 DSGVO orientieren. Der Auftragsverarbeiter muss sich aber der kirchlichen Datenschutzaufsicht unterwerfen (§ 30 Abs. 5 Satz 3 DSG-EKD).

Gemäß § 30 Abs. 6 DSK-EKD gelten die Absätze 1 bis 5 entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werde kann.

§ 30 Abs. 7 DSK-EKD erklärt, dass das Recht der Evangelischen Kirche in Deutschland, der Gliedkirchen und der gliedkirchlichen Zusammenschlüsse bestimmen kann, dass vor der Beauftragung die Genehmigung einer kirchlichen Stelle einzuholen ist oder Mustervereinbarungen zu verwenden sind, wobei bei der Beauftragung anderer kirchlicher Stellen in den Rechtsvorschriften von §§ 30 Abs. 3 Satz 2 Nr. 3, Nr. 5, Nr. 7 und Nr. 9 DSK-EKD abgesehen werden kann.

Nach § 30 Abs. 8 DSG-EKD kann können die Einhaltung von genehmigten Verfahrensregeln und die Verwendung zertifizierter und kirchlich geprüfter Informationstechnik herangezogen werden, um die Erfüllung der datenschutzrechtlichen Anforderungen durch den Auftragsverarbeiter nachzuweisen.

Nach § 31 Abs. 2 DSG-EKD hat jeder Auftragsverarbeiter ein Verzeichnis zu allen Kategorien von im Auftrag einer verantwortlichen Stelle durchgeführten Tätigkeiten der Verarbeitung zu führen. Das Verzeichnis ist gemäß § 31 Abs. 3 DSG-EKD schriftlich oder elektronisch zu führen und der Auftragsverarbeiter hat die Verzeichnisse auf Antrag der Aufsichtsbehörde gemäß § 31 Abs. 4 DSG-EKD zur Verfügung zu stellen.

Die in § 31 Abs. 2 DSG-EKD genannten Pflichten gelten gemäß § 31 Abs. 5 DSG-EKD nicht für verantwortliche Stellen, die weniger als 250 Beschäftigte haben; diese erstellen Verzeichnisse nach Absatz 2 nur hinsichtlich der Verfahren, die die Verarbeitung besonderer Kategorien personenbezogener Daten einschließen, also in jedem Fall bezüglich der Patientendaten im Krankenhaus.

Nach § 31 Abs. 6 DSG-EKD kann das Recht der Evangelischen Kirche in Deutschland, der Gliedkirchen und der gliedkirchlichen Zusammenschlüsse vorsehen, dass für einheitliche Verfahren das Verzeichnis zentral geführt wird.

Verletzt ein Auftragsverarbeiter oder ein Verantwortlicher eine im DSG-EKD vorgeschrieben Pflicht, kann eine Geldbuße nach § 45 DSG-EKD die Folge sein. Verantwortliche Stellen sind von Geldbußen ausgenommen, soweit sich nicht als Unternehmen im Sinne des § 4 Nr. 1 DSG-EKD am Wettbewerb teilnehmen. Die Geldbuße kann zudem gemäß § 45 Abs. 5 DSG-EKD maximal 500.000 Euro betragen und kann gemäß § 45 Abs. 6 DSG-EKD zusätzlich oder anstelle von Maßnahmen nach § 44 Abs. 3 DSG-EKD (Maßnahmen zur Wiederherstellung eines rechtmäßigen Zustands) verhängt werden.

Evangelische Landeskirche in Württemberg als exemplarisches Beispiel

Die Evangelische Landeskirche in Württemberg hat nach obigen Ausführungen eine eigene Verordnung erlassen, die auch eigene Regelungen zur Auftragsverarbeitung enthält.

Gemäß § 3 DSDEVO legt der Oberkirchenrat den Wortlaut der Verpflichtung nach § 30 Abs. 3 Satz 2 Nr. 5 DSG-EKD fest. Das Original der Verpflichtung ist zu den Personalakten zu nehmen und bei ehrenamtlichen Mitarbeiterinnen und Mitarbeitern sind die Originale gesammelt aufzubewahren.

Nach § 4 Abs. 1 DSDEVO ist die vom Oberkirchenrat festgelegte Mustervereinbarung zu verwenden, wenn personenbezogene Daten im Auftrag verarbeitet werden. Im Einzelfall kann auf schriftlichen Antrag der auftraggebenden kirchlichen Stelle mit Genehmigung des Oberkirchenrats von der Mustervereinbarung abgesehen werden. Gemäß § 4 Abs. 2 DSDEVO wird bei der Beauftragung anderer kirchlicher Stellen von §§ 30 Abs. 3 Satz 2 Nr. 3, Nr. 5, Nr. 7 und Nr. 9 und Satz 4 DSG-EKD abgesehen.

Das Verzeichnis nach § 31 Abs. 6 DSG-EKD führt der Oberkirchenrat für einheitliche Verfahren gemäß § 5 DSDEVO zentral.

Im Übrigen gilt aber auch hier das DSG-EKD und ferner außerhalb der Nutzung von Öffnungsklauseln der DSGVO der Art. 28 DSGVO.

Vorschriften zu technischen und organisatorischen Maßnahmen

Das DSG-EKD enthält eine Regelung zu technischen und organisatorischen Maßnahmen in § 27 DSG-EKD.

Nach § 27 Abs. 1 Satz 1 DSG-EKD haben die verantwortliche Stelle und der kirchliche Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschied-

lichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und einen Nachweis hierüber führen zu können. Gemäß § 27 Abs. 1 Satz 2 DSG-EKD schließen diese Maßnahmen unter anderem ein:

1. die Pseudonymisierung, die Anonymisierung und die Verschlüsselung personenbezogener Daten,
2. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,
3. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall unverzüglich wiederherzustellen,
4. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Gemäß § 27 Abs. 2 DSG-EKD sind bei der Beurteilung des angemessenen Schutzniveaus insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Nach § 27 Abs. 3 DSG-EKD sind Maßnahmen nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die Einhaltung eines nach dem EU-Recht zertifizierten Verfahrens kann gemäß § 27 Abs. 4 DSG-EKD als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten der verantwortlichen Stelle gemäß Absatz 1 nachzuweisen.

Die verantwortliche Stelle und der kirchliche Auftragsverarbeiter haben nach § 27 Abs. 5 DSG-EKD sicherzustellen, dass natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf ihre Weisung verarbeiten.

Zudem sind verantwortliche Stellen und Auftragsverarbeiter gemäß § 27 Abs. 6 DSG-EKD verpflichtet, IT-Sicherheit zu gewährleisten, wobei das Nähere durch die ITSVO-EKD geregelt wurde.

Nach § 1 Abs. 1 ITSVO-EKD sind die mit der Informationstechnik erhobenen oder verarbeiteten Daten insbesondere vor unberechtigtem Zugriff, vor unerlaubten Änderungen und vor der Gefahr des Verlustes zu schützen (IT-Sicherheit), um deren Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten. Nach § 1 Abs. 2 ITSVO-EKD ist ein Sicherheitskonzept zu erstellen und kontinuierlich fortzuschreiben. Gemäß § 1 Abs. 3 ITSVO-EKD orientiert sich der für die Umsetzung des IT-Sicherheitskonzeptes erforderliche Sicherheitsstandard an den Empfehlungen des BSI[310] zur Informationssicherheit und zum IT-Grundschutz, wobei vergleichbare Sicherheitsstandards ebenfalls zu Grunde gelegt werden können. Dieses IT-Sicherheitskonzept muss den

[310] Bundesamt für Sicherheit und Informationstechnik.

Schutzbedarf der Daten, die Art der eingesetzten IT und die örtlichen Gegebenheiten der jeweiligen kirchlichen Stelle berücksichtigen. Die Evangelische Kirche in Deutschland stellt nach Maßgabe des Absatzes 3 Muster-IT-Sicherheitskonzepte zur Verfügung gemäß § 1 Abs. 4 ITSVO-EKD.

Nach § 5 ITSVO-EKD ist zudem ein IT-Sicherheitsbeauftragter zu bestimmen. Zudem ist gemäß § 6 ITSVO-EKD es den einzelnen Kirchenteilen für ihren Bereich Durchführungsbestimmungen und ergänzende Bestimmungen zu erlassen.

Evangelische Kirche in Württemberg als exemplarisches Beispiel

Die evangelische Kirche in Württemberg hat hierzu ebenfalls Regelungen in der DSDEVO erlassen. Nach § 6 Abs. 1 DSDEVO sind den IT-Sicherheitskonzepten die Muster-IT-Sicherheitskonzepte der Evangelischen Kirche zugrunde zu legen und es dürfen nur die vom Oberkirchenrat geprüften und freigegebenen Verfahren und Programme eingesetzt werden.

Nach § 7 Abs. 1 DSDEVO bestellt der Oberkirchenrat den oder die IT-Sicherheitsbeauftragten, wobei nach § 7 Abs. 2 DSDEVO durch Verordnung auch ein Beauftragter für mehre Kirchenbezirke festgelegt werden kann.

Im Übrigen gilt aber auch hier das DSG-EKD, sowie außerhalb der Nutzung von Öffnungsklauseln der DSGVO der Art. 32 DSGVO.

3.5.3 Katholische Kirche

Auf Krankenhäuser anwendbare Datenschutzvorschriften

Die katholische Kirche regelt ihr Datenschutzrecht umfassend im Gesetz über den kirchlichen Datenschutz (KDG). Zur Anwendbarkeit der kirchlichen Datenschutzregelungen in Abgrenzung zum staatlichen Recht sei auf die obigen Ausführungen verwiesen. Diese Anwendung kirchlicher Regeln zum Patientendatenschutz in Krankenhäusern ist damit zumindest von einer Öffnungsklausel in den jeweiligen Landeskrankenhausgesetzen (LKHG) abhängig.

Dies sich auch in Einklang mit § 2 Abs. 2 KDG befinden, wonach soweit besondere kirchliche oder besondere staatliche Rechtsvorschriften auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, sie den Vorschriften dieses Gesetzes vorgehen, sofern sie das Datenschutzniveau des Gesetzes nicht unterschreiten.

Nach § 2 Abs. 1 KDG gilt dieses Gesetz für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Gemäß § 2 Abs. 3 KDG blieben zudem die Verpflichtung zur Wahrung des Beicht- und Seelsorgegeheimnisses, anderer gesetzlicher Geheimhaltungspflichten oder anderer Berufs- oder besonderer Amtsgeheimnisse, die nicht auf gesetzlichen Vorschriften beruhen, unberührt.

Das KDG gilt gemäß § 3 Abs. 1 lit c) KDG für die Verarbeitung personenbezogener Daten durch die kirchlichen Körperschaften, Stiftungen, Anstalten, Werke, Einrichtungen und die sonstigen kirchlichen Rechtsträger ohne Rücksicht auf ihre Rechtsform. Nach § 3 Abs. 2 KDG findet das KDG Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten eines Verantwortlichen oder eines Auftragsverarbeiters erfolgt, unabhängig davon,

wo die Verarbeitung stattfindet, wenn diese im Rahmen oder im Auftrag einer kirchlichen Stelle erfolgt.

Wie bereits bei der evangelischen Kirche finden sich auch hier Regelungen zum Schutz von Gesundheitsdaten, auch zu Behandlungszwecken, nämlich in § 11 KDG. Dieser enthält jedoch keine Sondervorschriften zum Cloud-Computing, insbesondere auch nicht zur Auftragsverarbeitung, sondern regelt „nur" die grundsätzliche Zulässigkeit der Verarbeitung besonderer Datenkategorien aus katholischer Sicht.

Erzdiözese Freiburg als exemplarisches Beispiel

Gemäß § 56 KDG trifft die zur Durchführung des Gesetzes erforderlichen Regelungen der Generalvikar gemäß § 56 KDG. Ein Generalvikar ist der ständige Vertreter des Bischofs einer Diözese für den Bereich der Verwaltung in der katholischen Kirche.

Als exemplarisches Beispiel dient hier die Erzdiözese Freiburg. Das LKHG BW enthält eine kirchliche Öffnungsklausel, sodass auch nach hier vertretener Ansicht eine Regelung durch die Kirchen möglich ist. Der Generalvikar der Erzdiözese Freiburg erließ am 18. Januar 2019 aufgrund von § 56 KDG die KDG-DVO.[311] Diese KDG-DVO wurde jedoch durch einstimmigen Beschluss der Vollversammlung des Verbandes der Diözesen Deutschlands vom 19. November 2018 vorgefertigt. Sie ist somit deutschlandweit identisch, wenngleich sie von den Generalvikaren der einzelnen Diözesen erlassen wurde.[312]

Fraglich erscheint vor diesem Hintergrund, ob alte Verordnungen der Diözesen zum Datenschutz noch anwendbar sind. Dies wurde teilweise ohne weitere Begründung angenommen.[313] Bei der Annahme wurde jedoch nicht bedacht, dass die Rechtsverordnungen wie beispielsweise der Diözese Osnabrück[314] oder der Erzdiözese Freiburg[315] zum Patientendatenschutz veraltet sind und im Zuge der Einführung der DSGVO und des KDG nicht angepasst wurden. Diese beziehen sich noch auf die veraltete Anordnung über den kirchlichen Datenschutz (KDO),[316] die durch das KDG abgelöst wurde. Gegen eine solche Annahme spricht auch, dass auf Grundlage des § 49 KDG eine eigene kirchliche Datenschutzgerichtsordnung (KDSGO) eingeführt wurde. Den Betroffenen soll nun durch das KDG ein eigener Rechtsweg offenstehen, was nur durch eine Vereinheitlichung wirklich sinnvoll geschehen kann. Das bundeseinheitliche Gebrauchen der Ermächtigungskompetenz in § 56 KDG durch Einführung der KDG-DVO, die Einführung der KDSGO und der Verweis auf die alte KDO in den Verordnungen lassen somit vielmehr den

[311] Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) in der Fassung des einstimmigen Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 19. November 2018.

[312] So Erzdiözese Freiburg: Veröffentlichung im Amtsblatt vom 23. März 2018 (Abl. Nr. 7, S. 185 ff.) und Erzdiözese München und Freising: Erlass am 18. Januar 2019 durch den Generalvikar Beer.

[313] Dierks, Lösungsvorschläge für ein neues Gesundheitsforschungsdatenschutzrecht in Bund und Ländern, S. 80.

[314] Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Osnabrück, Kirchliches Amtsblatt für die Diözese Osnabrück, Band 48, Nr. 7, Seite 41 ff, Art. 50. Diese ist aus dem Jahr 1990 und wurde zuletzt im Band 50 angepasst. Die Rechtverordnung verweist noch auf § 203 StGB a. F.

[315] Krankenhaus-Datenschutzordnung – Datenschutz in kirchlichen Krankenhäusern, Amtsblatt der Erzdiözese Freiburg, Nr. 32, S. 442 vom 28. November 2014.

[316] „Anordnung über den kirchlichen Datenschutz (KDO) für die Dienststellen und Einrichtungen des Verbandes der Diözesen Deutschlands" in der Fassung der Vollversammlung des Verbandes der Diözesen Deutschlands vom 20.06.2016.

Schluss zu, dass diese eigenständigen Regelungen der Diözesen nicht mehr maßgeblich sein sollen.

Somit ist für die Erzdiözese Freiburg als exemplarisches Beispiel das KDG, ergänzend die KDG-DVO und außerhalb der kirchlichen Öffnungsklausel landesrechtliche Regelungen, sowie außerhalb der Nutzung von Öffnungsklauseln die DSGVO anwendbar.

Zusammenfassung

Auf Krankenhäuser der katholischen Kirche ist – nach hier vertretener Auffassung soweit das Landesrecht eine Öffnungsklausel vorsieht – das KDG anwendbar. Die Generalvikare der jeweiligen Diözesen haben die bundesweit einheitlich vorformulierte KDG-DVO erlassen, die ergänzende Anwendung findet. Ferner gelten landesrechtliche Bestimmungen und im Übrigen außerhalb der Nutzung von Öffnungsklauseln die DSGVO.

Vorschriften zur Auftragsverarbeitung

Das KDG enthält mehrere Regelungen zur Auftragsverarbeitung.

Gemäß § 3 Abs. 2 KDG findet das Gesetz Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten eines Verantwortlichen oder eines Auftragsverarbeiters erfolgt, unabhängig davon, wo die Verarbeitung stattfindet, wenn diese im Rahmen oder im Auftrag einer kirchlichen Stelle erfolgt.

Auftragsverarbeiter im Sinne des KDG ist gemäß § 4 Nr. 10 KDG eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Die Auftragsverarbeitung selbst wird in Kapitel 4 „Verantwortlicher und Auftragsverarbeiter" geregelt.

§ 29 KDG behandelt die Verarbeitung personenbezogener Daten im Auftrag. Nach § 29 Abs. 1 KDG darf der Verantwortliche bei einer Verarbeitung im Auftrag nur mit Auftragsverarbeitern arbeiten, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieses Gesetzes erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Gemäß § 29 Abs. 2 KDG nimmt der Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen keinen weiteren Auftragsverarbeiter in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung hat der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter zu informieren, wodurch der Verantwortliche die Möglichkeit erhalten soll, gegen derartige Änderung Einspruch zu erheben.

Nach § 29 Abs. 3 KDG erfolgt die Verarbeitung entsprechend Art. 28 Abs. 3 DSGVO durch einen Auftragsverarbeiter auf der Grundlage eines Vertrages oder eines anderen Rechtsinstruments nach dem kirchlichen Recht, dem Recht der Europäischen Union oder dem Recht ihrer Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet.

§ 29 Abs. 4 KDG führt besondere Anforderungen an diesen Vertrag bzw. dieses Rechtsinstrument auf.

§ 29 Abs. 5 KDG bestimmt, dass wenn der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch nimmt, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem kirchlichen Recht oder dem Recht der Union oder dem Recht des betreffenden Mitgliedstaats der Europäischen Union dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß den Absätzen 3 und 4 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieses Gesetzes erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

Gemäß § 29 Abs. 6 KDG kann die Einhaltung nach europäischem Recht genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 5 nachzuweisen.

§ 29 Abs. 7 KDG erklärt, dass unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3, 4 und 5 ganz oder teilweise auf den in den Absatz 8 genannten Standardvertragsklauseln beruhen kann, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter erteilten Zertifizierung sind.

Die Datenschutzaufsicht kann nach § 29 Abs. 8 KDG Standardvertragsklauseln zur Regelung der in den Absätzen 3 bis 5 genannten Fragen festlegen.

Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 bis 5 ist nach § 29 Abs. 9 KDG schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann. Maßgebend sind die Formvorschriften der §§ 126 ff. BGB.

Ein Auftragsverarbeiter, der unter Verstoß gegen dieses Gesetz die Zwecke und Mittel der Verarbeitung bestimmt, gilt in Bezug auf diese Verarbeitung gemäß § 29 Abs. 10 KDG als Verantwortlicher.

Nach § 29 Abs. 11 Satz 1 KDG darf der Auftragsverarbeiter die Daten nur innerhalb der Mitgliedstaaten der Europäischen Union oder des Europäischen Wirtschaftsraums verarbeiten. Abweichend von Satz 1 ist die Verarbeitung in Drittstaaten zulässig, wenn ein Angemessenheitsbeschluss der Europäischen Kommission gemäß § 40 Absatz 1 vorliegt oder wenn die Datenschutzaufsicht selbst oder eine andere Datenschutzaufsicht festgestellt hat, dass dort ein angemessenes Datenschutzniveau besteht.

Die Absätze 1 bis 11 gelten gemäß § 29 Abs. 12 KDG entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen

im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 30 KDG bestimmt zudem, dass der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten dürfen, es sei denn, dass sie nach kirchlichem Recht, dem Recht der Europäischen Union oder dem Recht ihrer Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Nach § 31 Abs. 2 KDG ist jeder Auftragsverarbeiter vertraglich zu verpflichten, ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung zu führen. Nach § 31 Abs. 3 KDG ist dieses Verzeichnis schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann. Dieses ist gemäß § 31 Abs. 4 KDG dem betrieblichen Datenschutzbeauftragten und auf Anfrage der Datenschutzaufsicht zur Verfügung zu stellen.

Gemäß § 31 Abs. 5 KDG gelten die in den Absätzen 1 und 2 genannten Pflichten für Unternehmen oder Einrichtungen, die 250 oder mehr Beschäftigte haben. Sie gilt darüber hinaus für Unternehmen oder Einrichtungen mit weniger als 250 Beschäftigten, wenn durch die Verarbeitung die Rechte und Freiheiten der betroffenen Personen gefährdet werden, die Verarbeitung nicht nur gelegentlich erfolgt oder die Verarbeitung besondere Datenkategorien gemäß § 11 KDG bzw. personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des § 12 KDG beinhaltet.

Der Auftragsverarbeiter hat einen betrieblichen Datenschutzbeauftragen nach den §§ 36 ff. KDG zu benennen.

Zudem besteht ein gerichtlicher Rechtsbehelf einer betroffenen Person in einem eigenständigen Verfahren gegen den Auftragsverarbeiter nach § 49 KDG, §§ 2 Abs. 1, Abs. 2 7 Abs. 1 KDSGO. Es besteht ferner ein eigenständiger Schadensersatzanspruch des Betroffenen gegen den Auftragsverarbeiter nach § 50 KDG und wie bei den evangelischen Kirchen eine Vorschrift für Geldbußen gegen den Auftragsverarbeiter nach § 51 KDG. Erzdiözese Freiburg als exemplarisches Beispiel

Im Bereich der Erzdiözese Freiburg ist zudem die KDG-DVO gemäß § 56 KDG anwendbar. Diese enthält eine Regelung zu externen Zugriffen und Auftragsverarbeitung in § 21 KDG-DVO mit weitergehenden Vorgaben.

In § 21 Abs. 1 KDG-DVO wird ausgeführt, dass der Zugriff aus und von anderen IT-Systemen durch Externe besondere Gefahren hinsichtlich der Ausspähung von Daten schafft. Derartige Zugriffe dürfen nur aufgrund vertraglicher Vereinbarung erfolgen und insbesondere mit Auftragsverarbeiter, die nicht den Regelungen des KDG unterfallen ist grundsätzlich neben der Anwendung der DSGVO die Anwendung des KDG zu vereinbaren.

Nach § 21 Abs. 2 KDG-DVO ist bei Zugriffen durch Externe mit besonderer Sorgfalt darauf zu achten und nicht nur vertraglich, sondern nach Möglichkeit auch technische sicherzustellen, dass keine Kopien der personenbezogenen Datenbestände gefertigt werden können.

Gemäß § 21 Abs. 3 KDG-DVO ist, wenn dem Externen bei Vornahme der Arbeiten ein Systemzugang eröffnet werden muss, dieser Zugang entweder zu befristen oder unverzüglich nach Beendigung der Arbeiten zu deaktivieren. Im Zuge dieser Arbeiten vergeben Passwörter sind nach Beendigung der Arbeiten unverzüglich zu ändern.

Bei einer dauerhaften Inanspruchnahme von externen IT-Dienstleistern sind gemäß § 21 Abs. 4 KDG-DVO geeignete vergleichbare Regelungen zu treffen.

Nach § 21 Abs. 5 KDG-DVO darf eine Fernwartung von IT-Systemen darüber hinaus nur erfolgen, wenn der Beginn aktiv seitens des Auftraggebers eingeleitet wurde und die Fernwartung systemseitig protokolliert wird.

Gemäß § 21 Abs. 6 KDG-DVO darf die Verbringung von IT-Systemen mit Daten der Datenschutzklasse III (Besondere Kategorien personenbezogener Daten) zur Durchführung von Wartungsarbeiten in den Räumen eines Externen nur erfolgen, wenn die Durchführung der Wartungsarbeiten in eigenen Räumen nicht möglich ist und sie unter den Bedingungen einer Auftragsverarbeitung erfolgt.

Im Übrigen gilt nachrangig und außerhalb der Nutzung von Öffnungsklauseln die Vorschrift über die Auftragsverarbeitung nach Art. 28 DSGVO

Vorschriften zu technischen und organisatorischen Maßnahmen

Das KDG enthält Regelungen zu technischen und organisatorischen Maßnahmen.

§ 26 KDG behandelt die technischen und organisatorischen Maßnahmen.

Nach § 26 Abs. 1 KDG haben der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung unter anderem des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und einen Nachweis hierüber führen zu können. Diese Maßnahmen schließen unter anderem ein:

a) die Pseudonymisierung, die Anonymisierung und die Verschlüsselung personenbezogener Daten,
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Gemäß § 26 Abs. 2 KDG sind bei der Beurteilung des angemessenen Schutzniveaus insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Nach § 26 Abs. 3 KDG sind Maßnahmen nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 26 Abs. 4 KDG bestimmt, dass die Einhaltung eines nach dem EU-Recht zertifizierten Verfahrens als Faktor herangezogen werden kann, um die Erfüllung der Pflichten des Verantwortlichen gemäß Absatz 1 nachzuweisen.

Gemäß § 26 Abs. 5 KDG unternehmen der Verantwortliche und der Auftragsverarbeiter Schritte um sicherzustellen, dass ihnen unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach kirchlichem oder staatlichem Recht zur Verarbeitung verpflichtet

§ 27 KDG behandelt die Technikgestaltung und Voreinstellungen.

Nach § 27 Abs. 1 KDG sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung technische und organisatorische Maßnahmen durch den Verantwortlichen zu treffen, die geeignet sind, die Datenschutzgrundsätze wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieses Gesetzes zu genügen und die Rechte der betroffenen Personen zu schützen.

Gemäß § 27 Abs. 2 KDG trifft der Verantwortliche technische und organisatorische Maßnahmen, die geeignet sind, durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, zu verarbeiten. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere geeignet sein, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Im Übrigen gilt nachrangig und außerhalb der Nutzung von Öffnungsklauseln die Vorschrift über die Sichere Verarbeitung nach Art. 32 DSGVO.

Erzdiözese Freiburg als exemplarisches Beispiel

Gemäß § 56 KDG trifft die zur Durchführung des Gesetzes erforderlichen Regelungen der Generalvikar, der nach lit. b) insbesondere die technischen und organisatorischen Maßnahmen gemäß § 26 KDG festlegt. Die vom Generalvikar der Erzdiözese Freiburg erlassene bundesweit aber einheitliche KDG-DVO enthält mehrere Vorschriften zu technischen und organisatorischen Maßnahmen in Kapitel 3. Diese sind auch auf den Auftragsverarbeiter anwendbar, was sich aus § 5 KDG-DVO ergibt, wonach die Verarbeitung personenbezogener Daten auf IT-Systemen erst erfolgen darf, wenn der Verantwortliche und der Auftragsverarbeiter die nach dem KDG und dieser Verordnung erforderlichen technischen und organisatorischen Maßnahmen zum Schutz dieser Daten getroffen haben.

Gemäß § 6 Abs. 1 KDG-DVO sind je nach der Art der zu schützenden personenbezogenen Daten unter Berücksichtigung von §§ 26 und 27 KDG angemessene technische und organisatorische Maßnahmen zu treffen, die geeignet sind,

a) zu verhindern, dass unberechtigt Rückschlüsse auf eine bestimmte Person gezogen werden können (z.B. durch Pseudonymisierung oder Anonymisierung personenbezogener Daten),
b) einen wirksamen Schutz gegen eine unberechtigte Verarbeitung personenbezogener Daten insbesondere während ihres Übertragungsvorgangs herzustellen (z. B. durch Verschlüsselung mit geeigneten Verschlüsselungsverfahren),
c) die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste zum Schutz vor unberechtigter Verarbeitung auf Dauer zu gewährleisten und dadurch Verletzungen des Schutzes personenbezogener Daten in angemessenem Umfang vorzubeugen,
d) im Fall eines physischen oder technischen Zwischenfalls die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen rasch wiederherzustellen (Wiederherstellung).

Nach § 6 Abs. 1 KDG-DVO sind im Einzelnen für die Verarbeitung personenbezogener Daten in elektronischer Form insbesondere folgende Maßnahmen zu treffen:

a) Unbefugten ist der Zutritt zu IT-Systemen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zutrittskontrolle).
b) Es ist zu verhindern, dass IT-Systeme von Unbefugten genutzt werden können (Zugangskontrolle).
c) Die zur Benutzung eines IT-Systems Berechtigten dürfen ausschließlich auf die ihrer Zuständigkeit unterliegenden personenbezogenen Daten zugreifen können; personenbezogene Daten dürfen nicht unbefugt gelesen, kopiert, verändert oder entfernt werden (Zugriffskontrolle).
d) Personenbezogene Daten sind auch während ihrer elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern gegen unbefugtes Auslesen, Kopieren, Verändern oder Entfernen durch geeignete Maßnahmen zu schützen.
e) Es muss überprüft und festgestellt werden können, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung erfolgt (Weitergabekontrolle). Werden personenbezogene Daten außerhalb der vorgesehenen Datenübertragung weitergegeben, ist dies zu protokollieren.
f) Es ist grundsätzlich sicher zu stellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in IT-Systemen verarbeitet worden sind (Eingabekontrolle). Die Eingabekontrolle umfasst unbeschadet der gesetzlichen Aufbewahrungsfristen mindestens einen Zeitraum von sechs Monaten.
g) Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden (Auftragskontrolle).
h) Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).

i) Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden (Trennungsgebot).
j) Im Netzwerk- und im Einzelplatzbetrieb ist eine abgestufte Rechteverwaltung erforderlich. Anwender- und Administrationsrechte sind zu trennen.

Gemäß § 6 Abs. 3 KDG-DVO gilt Absatz 2 entsprechend für die Verarbeitung personenbezogener Daten in nicht automatisierter Form sowie für die Verarbeitung personenbezogener Daten außerhalb der dienstlichen Räumlichkeiten, insbesondere bei Telearbeit.

3.5.4 Zusammenfassende Bewertung

Die Regelungen der evangelischen Kirche und der katholischen Kirche zum Datenschutz sind im Vergleich zu den Regelungen der Länder umfassend und detailreich. Sie verfolgen den Ansatz, aus sich heraus ohne Rückgriff auf die DSGVO lesbar zu sein.

Positiv hervorzuheben ist, dass beide Kirchen im Wesentlichen bundesweit einheitliche Regelungen anstreben, die regional nur eingeschränkt ergänzt werden können. Dies führt praktisch zu Erleichterungen, da eine vormals komplizierte Prüfung der Rechtslage in einzelnen Bistümern und Diözesen erleichtert wird.

Es wäre zu begrüßen, wenn die Bundesländer sich diesen Grundgedanken der Einheitlichkeit bei einer Anpassung der Landeskrankenhausgesetze zum Vorbild nehmen würden.

Allerdings sind beide Gesetze nach hier vertretener Auffassung unter dem Vorbehalt der landesrechtlichen Öffnungsklauseln zu sehen. Eine bundesweite Geltung ist somit nicht gegeben, sodass es faktisch bei einer regionalen Zersplitterung der Gesetze in den einzelnen Bundesländern verbleibt.

Auch mit Öffnungsklauseln in allen Bundesländern zu Gunsten eines kirchlichen Patientendatenschutzes wäre dies jedoch nicht anders. Dies könnte zwar weitgehend einheitliche Vorgaben für kirchliche Krankenhäuser in verschiedenen Bundesländern gewährleisten, aber keine Angleichung gegenüber den Häusern öffentlicher und privater Träger.

Letztlich sollten nach hier vertretener Auffassung die Bundesländer ihre Vorschriften zum Patientendatenschutz in Krankenhäusern harmonisieren und deren Verbindlichkeit – ggf. mit Ausnahme der für die Patienten freiwilligen Krankenhausseelsorge – auch für kirchliche Krankenhäuser klarstellen, also jedenfalls eventuelle Öffnungsklauseln streichen.

4 Technische Anforderungen

Vorbemerkung: In diesem Kapitel werden vorwiegend Cloud-spezifische Aspekte und gegebenenfalls notwendige grundsätzliche Hintergrundinformationen betrachtet, nicht aber gängige Technologien und Standards, die bei jedem Betrieb von IT-Lösungen und KIS heute Stand der Technik sind.

4.1 Befunde auf einen Blick

(1) Unter Cloud-Computing versteht man die Nutzung von beliebig skalierbaren Ressourcen bei einem Cloud-Dienstleister, der Infrastruktur oder Plattform oder beides inklusiv der darauf laufenden Anwendungen zur Verfügung stellt und zumeist nutzungs- bzw. wertschöpfungsorientierte Kostenmodelle anbietet.

(2) Im weitesten Sinne ist der Betrieb von Legacy-KIS des alten Stils auf skalierbaren Infrastrukturen oder Plattformen auch schon Cloud-Computing.

(3) Legacy-KIS sind in der Regel keine Webanwendungen, sondern klassische Client-Server-Anwendungen. Bei RZ-Betrieb erfolgt die Verarbeitung der „fetten Clients“ auch im Rechenzentrum und die Benutzung wird mittels Terminalserver bzw. virtualisiertem Desktop auf die Arbeitsrechner gebracht.

(4) Legacy-Anwendungen können die skalierenden Infrastruktur- und Plattform-Potenziale des Cloud-Computing nur in eingeschränktem Maße ausschöpfen.

(5) Die IT-Betriebslast eines Krankenhauses ist bei gegebener Anwendungslandschaft in ihrem Tagesprofil keinen großen Schwankungen unterworfen, sodass eine dynamische Skalierung bzw. hohe Elastizität der Umgebung und damit einhergehende nutzungsorientierte Kosten weniger ein Problem von KIS ist, da die Last-Tagesprofile deterministisch angegeben werden können und damit auch eine feste Nutzungspauschale vereinbart werden kann.

(6) Probleme von Legacy-Systemen sind vielfältig und werden durch die technologischen Veränderungen zunehmen. Softwaretechnisch sind diese KIS riesige verwinkelte Gebäude, die immer schlechter wart- und deploybar werden. Auch innovative Weiterentwicklung und Offenheit sind nur beschränkt oder mit großem Aufwand möglich. Diese Nachteile schlagen direkt auch auf die Kunden wie z.B. die Krankenhäuser zurück, sei es funktional oder bei den Lizenzkosten für neue Module und Funktionalitäten und bei den Pflegekosten.

(7) Aufgrund des technologischen Wandels und der Nichtmehrverfügbarkeit alter Technologien werden Legacy-KIS zunehmend verrotten, dieser Prozess hat bereits begonnen.

(8) Cloud Native Anwendungslösungen basieren auf einer modularen am Ansatz des „Domain Driven Design“ orientierten Softwarearchitektur und können in dieser Form auch modular als SaaS-Lösung funktional orchestrier- und choreografierbar am Markt angeboten werden.

(9) Die Motivation für Cloud-KIS besteht weniger in der Ausnutzung von Elastizität, sondern in den vielfältigen Vorteilen von Cloud Native Anwendungen wie z.B. Nachhaltigkeit, Offenheit, funktionaler Orchestrierbarkeit, ubiquitäre Nutzbarkeit auf allen festen und mo-

bilen Geräten und Mehrfachnutzbarkeit von modularen Komponenten, aber auch in kürzeren Entwicklungszyklen für die (Cloud-)Software, einfacherer Erweiterbarkeit, erhöhter Stabilität der Software und Vereinfachung des Software Development Lifecycle.

(10) Eine weitere Motivation besteht darin, dass sich durch Cloud-KIS das lokal hinsichtlich Anzahl und Know-How-Breite begrenzte IT-Personal wieder stärker auf gestaltende und Governance-Aufgaben konzentrieren kann, um den digitalen Wandel im Krankenhaus optimal orientiert an den lokalen Bedürfnissen planen, umzusetzen und begleiten zu können.

(11) Die Zielprojektion für ein Cloud-KIS muss es sein, dass für Krankenhäuser bzw. stationäre Einrichtungen jeglicher Art ein skalierbares Set an domänenspezifischen Software-Funktionalitäten zur Verfügung steht und die Funktionalitäten je nach Einrichtung und Bedarf bezogen und genutzt werden können.

(12) Ein modulares Cloud-KIS (mCloud-KIS) ist eine nutzer- und nutzenzentrierte webbasierte **Softwarelandschaft** bestehend aus domänenspezifischen voneinander unabhängigen fachlichen und systemtechnischen Microservice-Modulen, die von verschiedensten Softwareherstellern stammen können und mittels semantischer Interoperabilität auf Basis geeigneter Mechanismen zusammenarbeiten. („modular multivendor meaningful Cloud-HIS" = m^3cloud-HIS).

(13) Cloud-KIS bedeutet eine radikale Abkehr von heterogenen aus abgeschlossenen minimal-interoperablen proprietären Informationssystemen nicht skalier- und orchestrierbaren KIS, wie sie heute allerorten betrieben werden.

(14) Mit Legacy-KIS werden keine regionale digitalen Ökosysteme ähnlich wie in anderen Branchen entstehen können, auch wird zunehmend die Innovation stocken, mobile Nutzung ist nur eingeschränkt möglich oder es müssen aufwändig Zusatz-Apps entwickelt und von den Krankenhäusern bezahlt werden.

(15) Die softwaretechnische „Cloudifizierung" von Legacy-Systemen kommt einer Neuentwicklung gleich, da Code nicht übernommen werden kann und auch eine Überführung in eine moderne funktionsorientierte Modularisierung im Sinne eines „Domain Driven Design" nicht ohne Refactoring und Neuimplementierung möglich ist.

(16) Modulare Cloudifizierung von Legacy-KIS ist gut möglich, da alle medizinischen Handlungen und die zugehörigen IT-Funktionalitäten modular sind.

(17) Eine schrittweise Migration von Legacy-KIS hin zu Cloud Native Anwendungen ist gut möglich. So können neue Funktionalitäten als Cloud Native Anwendungen entwickelt werden und interoperabel mit dem Legacy-KIS betrieben werden. Der Einbau entsprechender Aufrufschnittstellen in die Legacy-Systeme ist einfach zu bewerkstelligen.

(18) Das KHZG bietet eine große Chance, dass für die in §19 benannten Fördergegenstände die Legacy-KIS um Cloud Native Module dafür erweitert werden.

(19) Legacy-KIS-Anbieter werden auf absehbare Zeit eher nicht aus eigenem Antrieb zu Cloud-Nativ Anwendungen migrieren, hierzu bedarf es eines externen Bedarfes und Drucks durch Kunden und Politik.

(20) Bei Förderprogrammen zur Digitalisierung im Krankenhaus sollten zukünftig Förderkriterien die Pflicht zur Implementierung als Cloud-fähige Lösung beinhalten, Krankenhäuser sollten bei Ausschreibungen auf die Perspektiven des Herstellers bezüglich der Cloudifizierung des Legacy-Systems achten.

(21) Ein großes Potenzial für eine „Cloudifizierung" von digitalen Lösungen bzw. der Realisierung von Cloud Native Anwendungen liegt im Krankenhaus- bzw. Gesundheitswesen in den über viele Jahrzehnte entwickelten Interoperabilitäts- und Semantikstandards – hier vor allem den Standards von HL7 und IHE und SNOMED. So Kann FHIR direkt auch für die Interoperabilität von Microservices eingesetzt werden, CDA-Dokumente als justitiable Persistenzobjekte können als strukturierte und formalisierte Dokumente für die justitiable Dokumentenspeicherung und den Austausch genutzt werden.

(22) Alle Systeme/Module eines Cloud-KIS müssen in der Lage sein, auf Basis einer krankenhausindividuellen Policy Daten bzw. Dokumente in einem offenen Format in ein Langzeitarchiv zu speichern.

(23) Cloud-KIS können in optimaler Weise Cloud-Repositories nutzen. Der Betrieb und die Inhaltspflege von Cloud-Repositories für verschiedenste Objekttypen wie Organisationen, Medikamente, Semantikkataloge, Materialien, Bettenangebote u.v.a.m. auf regionaler oder nationaler Ebene hat sowohl bezogen auf die Integrität von Daten in einem verteilten System also auch ökonomisch durch Einmalpflege erhebliche positive Effekte auf die zukünftige Entwicklung eines digitalen Gesundheitswesens.

(24) Für Cloud-KIS wird mehr als bisher ein Compliance-Management System notwendig und der konsequente Einsatz vorhandener Compliance-Mechanismen. Hierzu zählt auch eine konsequente Nutzeridentifikation und -authentifikation jedes Benutzers unabhängig von der beruflichen Rolle im Krankenhaus. Cloud-KIS bieten die Chance, heute allen Bürgern vertraute Authentifikationsmechanismen auch für den KIS-Zugang zu nutzen.

(25) Ein Single Point of Failure ist die Infrastrukturanbindung zwischen Krankenhaus und Cloud-Provider. Daher ist hierfür eine Mehrfachauslegung über getrennte Zugangsknoten vorzusehen.

(26) Die Kenntnisnahme der hoch schutzwürdigen medizinischen Daten durch den Provider ist soweit wie möglich zu verhindern bzw. zu erschweren und gleichzeitig hierzu auch vertragliche Regelungen zu schaffen und deren Umsetzung regelmäßig zu überprüfen. Kryptographische Verfahren, verteilte Geheimnisse und Trennung der Verwaltung von identifizierenden und medizinischen Daten in verschiedene Anbieter-Plattformen sind mögliche Ansätze. Hier besteht weiterer Forschungsbedarf.

(27) Cloud-Provider können heute ein für die Krankenhäuser wichtiges und notwendiges hohes Maß an Verfügbarkeit und Performance bieten, oft weit über das hinaus, was beim Vor-Ort-Betrieb möglich ist.

(28) Cloud-KIS können in optimaler Weise mit anderen Cloud-Lösungen und gesundheitstelematischen Anwendungen der TI interoperieren, da sie selbst konsequent serviceorientiert sind.

(29) Für viele Problem- und Fragestellungen z.B. von der Authentifikation über kryptographische Verfahren, der Datenhaltung bis hin zu generischen Lösungen für Interoperabilität und Oberflächengenerierung gibt es heute frei verfügbar Programm-Bibliotheken bzw. Frameworks, die eine Entwicklung von Cloud-KIS effektiv bewerkstelligen lassen.

(30) Die Zukunft wird geprägt sein von lokalen digitalen Gesundheits-Ökosystemen, in denen viele Gesundheitseinrichtungen aber auch Patienten und ihre Angehörige kooperativ digital zusammenarbeiten und sich einerseits digitale Ressourcen teilen, aber auch durch

digitale Verfahren direkt gemeinsam Patientenbehandlungen planen, durchführen, dokumentieren und überwachen. Hierzu werden gemeinsame Repositories für vielfältige Aspekte eingesetzt werden, so auch für medizinisches Wissen und klinische Pfade.

(31) Wissensgewinnung und Wissensentwicklung können in der Medizin nur noch gemeinsam und multizentrisch erfolgen. Cloud-KIS bieten die Chance, Community-Plattformen aufzubauen, die verzahnt mit KIS einen solchen gemeinsamen Wissensprozess und ein gemeinsames Wissensmanagement ermöglichen bei gleichzeitiger direkter kontextsensitiver Aufrufbarkeit und Integration des Wissens in die KIS-Funktionalitäten.

4.2 Einführung und Überblick

„Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud."[317]

"Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand. Note: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment."[318]

Ergänzt man die Definition zu einem KIS aus Kapitel 2.1, kann ein Cloud-basiertes Krankenhausinformationssystem (Cloud-KIS) definiert werden als: **„Ein Cloud-KIS ist die Summe aller über eine Cloud beziehbaren Plattform- und Software-Ressourcen zur Verarbeitung aller notwendigen Daten zur Unterstützung aller administrativen, logistischen und medizinischen Vorgänge bis hin zum Controlling und dem Qualitätsmanagement und für das strategische Management von Krankenhäusern."**

Aber: Die Verschiebung von Legacy-Systemen in die Cloud führt nicht zu wirklichen Cloud-Systemen. „But for now, know that a system that was architected and optimized to run in a traditional data center cannot take advantage of all the benefits of the cloud, such as elasticity. Thus we need a modern architecture to reap the benefits of the cloud."[319]

Cloud Lösungen meist in Form von Webanwendungen werden heute von großen Technologieunternehmen für ihre Plattformen, für elektronische Markplätze und als Branchenlösungen (vertikale SaaS) für vielfältige Branchensegmente oder in Form von für viele Unternehmen allgemeinverwendbaren Lösungen (horizontale SaaS) eingesetzt. Letztgenannte reichen z.B. von Office-Lösungen, über Kollaborations-Werkzeuge und WIKIs, Organisations- und Workflow-Lösungen bis hin zu Autorensystemen und eLearning-Plattformen oder Softwareentwicklungs-Repositories. Damit einher geht eine Entwicklung, bei der Softwarelösungen sowohl als lokal installierbare Lizenzlösungen als auch als im Jahresabonnement hybrid angeboten werden

[317] Armbrust et al, Above the Clouds: A Berkeley View of Cloud Computing. 2009. S. 1.

[318] International Standards Organisation: ISO/IEC 1778: Information technology - Cloud computing — Overview and vocabulary. 2014. S. 2.

[319] Gilbert, Cloud Native Development Patterns and Best Practices: Practical Architectural Patterns for Building Modern, Distributed Cloud-native Systems. 2018. S. 9.

bzw. wurden, da einige Hersteller beginnen, ihre Lösungen nur noch als cloud-basierte Jahresabonnements anzubieten – sei es in ihrer Public Cloud oder aber in einer ebenfalls von ihnen gehosteten Privat Cloud. Problematisch ist bei letztgenanntem Trend, dass ein On-Premises-Betrieb damit faktisch ausgeschlossen wird, also Kunden ihre technisch-/softwaretechnische Souveränität verlieren. Daneben gibt es inzwischen auch vielfältige Open Source Cloud-Lösungen ebenfalls für viele Branchenbereiche und Anwendungszwecke.

Für Cloud-Lösungen können als Basis heute vielfältige Technologien und Plattformen eingesetzt werden und es existieren eine Reihe von Anforderungen und Zertifikaten, in Deutschland insbesondere der vom BSI entwickelte B5-Kriterienkatalog (C5 = Cloud Computing Compliance Controls Catalogue), der u.a. auf diversen anderen Zertifikatskatalogen basiert.[320]

Die Hauptmotivation von Cloud-Software und SaaS besteht im flexiblen, also skalierbaren Angebot, Bezug und der Abrechnung von Software und deren Nutzung – auch unabhängig von Raum und Zeit – für die Kunden des Zielmarktes via Internet-Technologie. Eine weitere Motivation ist aber auch die modulare und eventuell verteilte Weiterentwicklung und der Ausbau um neue Funktionalitäten, also die Agilität der Entwicklung und der Software. Dies sind alles Aspekte, die schon immer im Kern der Bemühungen um gute betriebliche Informationssysteme standen: **Gut modularisiert und verstehbar, wiederverwendbar und erweiterbar**.[321]

Während in einem Sercive-RZ betriebene **Monolithen** alter Prägung („Legacy-Systeme"), die im Prinzip als Client-Server-Systeme in einem Backend-System – oftmals betrieben durch Nutzung der Client Software ebenfalls auf dem Server mittels Thin Clients vor Ort– eigentlich nur einen Shift vom lokalem Betrieb auf entfernten Betrieb darstellen, hat in den vergangenen 20 Jahren auch vor dem Hintergrund zunehmender Realisierung und Betrieb „großer" Weblösungen ein Entwicklungs- und Erkenntnisprozess stattgefunden zum Thema, wie „große" Softwaresysteme sinnvoll zu zerlegen und zu entwickeln sind. Weitere Motivationen waren und sind die Problematik der immer schlechteren Wart- und Weiterentwicklungsmöglichkeiten der monolithischen Großsysteme[322] sowie das komplexe langdauernde Deployment. Das Paradigma der Zukunft heißt nun: **Modulare Microservice- und API-basierte Anwendungslösungen**, wobei sich der Zuschnitt solcher Microservices an den fachlichen Notwendigkeiten entlang der Bearbeitungsvorgänge orientiert und die Prinzipien Kohäsion und lose Kopplung im Mittelpunkt stehen. Cloud-nativ-Anwendungen bzw. Anwendungssysteme stellen zwar softwaretechnisch mit Blick auf die Zerlegung großer Systeme in kleinere Einheiten kein neues Paradigma dar, Art und Weise des Zuschnitts und konsequente Servicebasierung und die Organisation der Softwareentwicklung aber schon.

Dementsprechend existierten für Cloud-Softwaresysteme verschiedene aber sich ähnelnde Architekturansätze, wie z.B. publiziert im ISO-Standard[323], vom National Institute of Standards and

[320] Bundesamt für die Sicherheit in der Informationstechnik, Kriterienkatalog Cloud Computing C5:2020.

[321] Parnas, On the criteria to be used in decomposing systems into modules. Commun. ACM, Band 15, Nr. 12, S. 1053–1058, 1972.

[322] Vernon spricht in diesem Zusammenhang von einem „Big Ball of Mud" (Vernon, Domain-Driven Design kompakt. 2017. S 57. Teilweise wird von Softwareverrottung gesprochen, also dem langsamen Zerfall.

[323] International Standards Organisation, ISO/IEC 17789: Information technology -Cloud computing - Reference architecture. 2014.

Technology US Department of Commerce (NIST)[324] und von kommerziellen Unternehmen, die Frameworks ermöglichen und fördern für die Implementierung von Cloud-Softwaresystemen oder anderen Unternehmen die Integration eigener Erweiterungen in ihre Cloud-Lösung. Cloud-Native Architekturen sollen auch Elastizität und Resilienz fördern.

Die Erwartungen der Unternehmen an Cloud-Nativ-Systeme sind im Wesentlichen[325]

- Kürzere Entwicklungszyklen für die (Cloud-)Software
- Erhöhte Stabilität der Software
- Vereinfachung des Software Development Lifecycle

Dieser mehr entwicklungstechnisch orientierten Liste können aber einige weitere auch ökonomisch relevante positive Aspekte hinzugefügt werden, so z.B. der passgenaue und im Zeitverlauf leicht änderbare Zuschnitt der Softwarelandschaft für ein diese nutzendes Unternehmen, die Beförderung von Innovation und Wettbewerb bei der Entwicklung von in bestehende Lösungen integrierbaren Cloud-Modulen, die leichte Austauschbarkeit von Modulen und die Ermöglichung auch von branchenbezogenen Ökosystemen z.B. im Rahmen von Community Clouds oder Mischformen aus Privat- und Community Clouds. Letztendlich kann auch ein einfacher „Roll-out" von Lösungen in der Fläche angeführt werden, da für eine Nutzung keine aufwändigen lokalen Installationen mehr notwendig sind, lediglich in der Regel eine initiale Orchestrierung und Parametrierung auf die spezifischen Bedürfnisse hin. Das macht Cloud-Lösungen nicht nur für die Kunden werthaltig, sondern auch für Hersteller von Standard-Software interessant.

Herausforderungen für das Cloud-Computing sind neben der paradigma-gerechten Softwarearchitektur und Implementierung u.a. in den folgend genannten Bereichen angesiedelt:[326]

- Cloud Computing Architectural Framework
- Governance and Enterprise Risk Management
- Legal Issues: Contracts and Electronic Discovery
- Compliance and Audit
- Information Management and Data Security
- Portability and Operability
- Traditional Security, Business Continuity and Disaster Recovery
- Data Center Operatns
- Incident Response, Notification and Remediation
- Application Security
- Encryption and Key Management
- Identity, entitlement and Access Management
- Virtualization
- Security as a Service

[324] Liu et al, NIST Cloud Computing Reference Architecture. Recommendations of the National Institute of Standards dann Technology. 2011.

[325] IDG Research Services, Studie Cloud Native 2020. S. 7.

[326] Kalloniatis et al, Towards the design of secure and privacy-oriented Information Systems in the Cloud: Identifying the major concepts. Research Paper 2014.

Im ISO-Standard 17789[327] werden als (Querschnitts)Aspekte aufgeführt:

- auditability
- availability
- governance
- interoperability
- maintenance and versioning
- performance
- portability
- protection of personally identifiable information
- regulatory
- resiliency
- reversibility
- security
- service levels and service level agreement.

Eine Taxonomie der Sicherheitsaspekte von Cloud-Computing Systemen findet sich in der Studie des Fraunhofer AISEC[328], die deutlich macht, dass auf allen Ebenen – Infrastruktur, Anwendung und Plattform, Verwaltung und Compliance – vielfältige Aspekte zu berücksichtigen sind.

Die Chancen von Cloud-Systemen und deren Nutzung für den Aufbau branchenspezifischer digitaler Ökosysteme haben zu der europäischen Großinitiative GAIA-X geführt mit dem Ziel, für Europa, seine Staaten, seine Unternehmen und seine Bürgerinnen und Bürger die nächste Generation einer Dateninfrastruktur zu schaffen, die höchsten Ansprüchen an digitale Souveränität genügt und Innovationen fördert. Diese Infrastruktur wird als Wiege eines Ökosystems verstanden, in dem Daten und Dienste verfügbar gemacht, zusammengeführt und vertrauensvoll geteilt werden können.[329] Ein Ansatz, der auch für das Ökosystem „Gesundheitsversorgung" gelten kann, so z.B. für regionale sektorübergreifende Versorgungsverbünde. Cloud-KIS sind daher nicht nur eine andere Form von KIS, sondern ein völlig neuer Lösungsansatz und können eingepasst in regionale digitale Ökosysteme z.B. auf Basis einer Community Cloud Teil einer neuen innovativen digitalen Infrastruktur für die koordinierte transparente und den Patienten einbeziehende Gesundheitsversorgung sein. Cloud-KIS und das Verständnis um Cloud-native Anwendungen werden wesentliche Treiber für die Digitalisierung im Gesundheitswesen werden.

Die Zielprojektion für ein Cloud-KIS muss es daher sein, dass für Krankenhäuser bzw. stationäre Einrichtungen jeglicher Art ein skalierbares Set an domänenspezifischen Software-Funktionalitäten – genauer gesagt **containerbasierte interoperable Anwendungssystembausteine** (im Folgenden auch als Cloud-Microservice-Module (CMSM) bezeichnet) – zur Verfügung steht, die je nach Einrichtung und Bedarf bezogen und genutzt werden können. Dies bedeutet eine radikale Abkehr von heterogenen aus abgeschlossenen minimal-interoperablen proprietären

[327] International Standards Organisation, ISO/IEC 17789 Information technology – Cloud computing – Reference architecture. 2014. S. 8 f.

[328] Streitberger, Ruppel: Cloud Computing. Schutzziele. Taxonomie. Markübersicht. 2009. S. 42.

[329] Siehe unter https://www.bmwi.de/Redaktion/DE/FAQ/Dateninfrastruktur/faq-projekt-gaia-x.html.

Informationssystemen nicht skalier- und orchestrierbaren KIS, wie sie heute allerorten betrieben werden.

4.3 Architektonische Aspekte

Mit Blick auf die Definition von Armbrust et. al. stellt sich die Frage, ob für Software-as-a-service (SaaS) andere Softwarearchitekturen notwendig werden bzw. sinnvoll sind, als für proprietäre Legacy-Systeme, die auch noch heute dem „Vor-Ort Client-Server-Paradigma" folgen.

Der hierzu geführte Diskussions- und Erkenntnisprozess kann in drei Phasen eingeteilt werden:

1. Schon 1996 wurde erstmalig der Begriff **„Serviceorientierte Architektur" (SOA)** geprägt, die Idee wurde dann ab dem Jahr 2004 vermehrt aufgegriffen, was sich durch die Vielzahl von Lehrbüchern zum Thema ab diesem Jahr verdeutlichte. Es zeigte sich aber in der Folge, dass der Service-Bus einen Single Point of Failure darstellt und weitere Nachteile mit der SOA einhergehen. 1999 wurde die OSGi Allianz[330] gegründet, die zum Ziel hatte, einen offenen Standard für offene modulare Serviceplattformen auf Basis von JAVA zu spezifizieren. Zentrale Komponente ist hier das Modul und die OSGi-µServices.
2. Im Jahr 2012 wurde motiviert durch die UNIX-Konzepte der weitegehenden Isolation von sinnvoll kapselbaren Funktionalitäten („Do One Thing and Do It Well") das Konzept der **Micro-Services** geprägt, vom Chefentwickler von Netflix als „Fine grained SOA" bezeichnet.
3. Ab dem Jahr 2017 setzt sich zunehmend die Auffassung durch, dass eine extensive Zerlegung und Granularisierung von großen Softwaresystemen in kleinste „MicroServices" ebenso vielfältige erhebliche Probleme mit sich bringt und daher Microservices eher als an der fachlichen Sicht orientierte isolierte **Fach-Module** gesehen werden sollten, die vor dem Hintergrund eines „Bounded Context" eine fachlich sinnvoll geclusterte Funktionalität inklusive der dazu notwendigen Daten kapseln und über APIs zur Verfügung stellen. In manchen Ansätzen haben diese Microservice-Module auch eigene Oberflächen.

In diesem Zusammenhang spricht man heute bezüglich solcher modularisierter Gesamtsysteme auch vom „modularen Monolithen", was aber Vision und Ziel auch nicht trifft, denn es sollen ja genau keine Monolithen mehr hergestellt werden, sondern offene ergänzbare modulare Web- bzw. -Cloud-Lösungen.

Architekturunabhängig, aber methodisch begleitend, beeinflusste die Erstpublikation der Idee eines **Domain Driven Designs (DDD)** im Jahr 2004[331] zunehmend auch die Art und Weise der Betrachtung und der Methoden, wie große Softwaresysteme entworfen und zerlegt werden sollten.

Vor diesem Hintergrund ist und bleibt die Diskussion um **Granularität von Software** und der damit einhergehende Zuschnitt auf allgemeine systemtechnische und spezifische fachlogische

[330] Siehe https://www.osgi.org/.

[331] Evans, Domain-driven design – Tackling complexity in the heart of software. 2004.

Services/Module ein wichtiges informatisches Thema, das auch mit Blick auf die damit verfolgten fachlichen Ziele und den Projekt-/Softwarekontext gesehen werden muss. Haesen et. al.[332] unterteilen bezüglich der Service-Granularität zwischen der Daten-, Geschäftsmehrwert- und Funktionsgranularität. In diesem Sinne führt eine thematische Verschneidung von DDD und Microservices zu den Kriterien **maximaler Kohäsion und maximal loser Kopplung** der einzelnen Softwarebausteine.

Bei Microservices geht es nicht nur darum, große Softwaresysteme in unabhängig deploy- und betreibbare kleinere Einheiten aufzuteilen, sondern auch darum, die Entwicklung auf voneinander unabhängige und eigenständig arbeitende Entwicklungsteams aufzuteilen. Dies kann auch den Vorteil haben, dass diese Teams nicht einmal aus einem Unternehmen stammen müssen und daher große Systeme durch das Zusammenwirken von Softwaremodulen entstehen, die von kleinen innovativen Firmen entwickelt wurden und die Experten in einer kleinen abgeschlossenen Domäne sind. Es geht also nicht (nur) um Technik, sondern um Menschen, Organisationen und offene Geschäftsmodelle für die Softwarebranche und um Innovation und Agilität. Und so ist in den großen Anwendungssoftware-Unternehmen nicht nur bezogen auf die Software ein „Big Ball of Mud" entstanden, sondern oft auch hinsichtlich des Personals und dessen fachlichen Zuordnungen und Kompetenzen.

Wie bereits vorangehend eingeführt, geht es um modulare Architekturen, deren Module nach dem Prinzip der funktionalen Kohäsion so klein wie möglich sein sollen und deren Zusammenarbeit nach dem Prinzip der losen Kopplung funktioniert. „Our objective is to use asynchronous, message-driven, inter-component communication to build resilient components that are responsive and elastic."[333]

Für die Umsetzung und den Betrieb können sieben Prinzipien angegeben werden bzw. müssen in geeigneter Wiese implementiert werden (konsequente Nutzung von Cloud Services für die Infrastrukturbereitstellung, konsequente Microservice-Modularisierung, Containerisierung der Microservices für den Betrieb, Scheduling und Orchestrierung der Container, Clustering, Service-Mesh als Infrastrukturschicht und kontinuierliche Integration und Deployment der Microservices)[334].

Dabei können bezüglich der Modularisierung sowohl fachlogische als auch allgemeine zumeist systemlogische Funktionalitäten unterschieden werden, für Letztgenannte spricht der ISO-Standard von „Multi-layer-functions". Auch horizontale Funktionalitäten z.B. für das Berechtigungsmanagement, die Modulkommunikation, die Administration usw. sind im Prinzip gegenüber monolithischer Legacy-Systemen nicht neu, aber dort sind diese horizontalen Funktionalitäten zumeist mit den Fachanwendungen weitegehend „verbacken". Viele der „Multi-layer-functions" sind heute bereits in den kommerziellen Cloud-Anwendungsplattformen enthalten, sodass für eine Implementierung nur eine Konzentration auf die fachlogischen Microservices erfolgen muss bei Berücksichtigung derer Interoperabilität mit den vorhandenen systemtechnischen Plattformfunktionalitäten.

---

[332] Haesen et al, On the Definition of Service Granularity and its Architectural Impact. Research Gate 2008. S. 6.

[333] Gilbert, Cloud Native Development Patterns and Best Practices: Practical Architectural Patterns for Building Modern, Distributed Cloud-native Systems. 2018. S. 28.

[334] Schäfer, Der Weg zu einer Cloud-nativen Architektur. 2017.

In der ISO-CCRA werden drei Hauptklassen von Funktionalitäten („cloud capability types") unterschieden: "Cloud capabilities type: Classification of the functionality provided by a cloud service (3.2.8) to the cloud service customer (3.2.11), based on resources used. NOTE – The cloud capabilities types are application capabilities type (3.2.1), infrastructure capabilities type (3.2.25) and platform capabilities type (3.2.31)."[335]

Im ISO-Standard wird die Grundidee der allgemeinen Architektur (Cloud Computing Reference Architecture CCRA)[336] entlang der Betrachtung von betrieblichen Rollen, ihren Aufgaben und den damit verbundenen unterstützenden Anwendungssystemfunktionen hergeleitet. Konsequenterweise werden vier „viewpoints" angegeben: User view, Functional view, Implementation view und Deployment view, wobei implementierungstechnische Aspekte sukzessive in der angegebenen Reihenfolge abgeleitet werden. Der Standard selbst behandelt aber nur die zwei erstgenannten Viewpoints, macht also keine Vorgaben oder Annahmen zu Implementierungen und Deployment. Es handelt sich also um eine logische Architektur.

Dabei werden in der ISO-CCRA – aber auch in anderen Architekturen – als kleinste Einheit Anwendungsfunktionen angegeben (functional components[337]), die in ihrer Gesamtsumme den Leistungsumfang einer Cloud-Anwendung ausmachen. Diese werden verschiedenen Schichten (Layer) zugeordnet. Layer klassifizieren die Funktionalitäten und es werden einerseits Layer unterschieden, deren Funktionen spezialisierter vertikale Art sind (graphisch sind die Layer aber horizontal dargestellt) und Layer, deren Funktionen systemweit verfügbar sind und von vielen anderen Funktionen konsumiert werden oder für die Gesamtkoordination und das Funktionieren des Cloud-Systems evident sind (graphisch sind die Layer aber vertikal dargestellt).

Die **Benutzerschicht („User Layer")** umfasst die zur Unterstützung der betrieblichen Aktivitäten notwendigen Funktionalitäten und wird weiter unterteilt in Funktionen für die Benutzer, die Administratoren der Anwendung und generelle Geschäftsfunktionen.

Die **Zugriffsschicht („Access Layer")** enthält Komponenten für die Kooperation und Zugriffskontrolle von Komponenten untereinander bzw. der verschiedenen Schichten.

Die Funktionen der **Service Schicht („Service Layer")** dienen der Verwaltung und Orchestrierung der Cloud-Services selbst.

In der **Ressourcen-Schicht („Resource Layer")** sind dann Funktionen für die Abbildung der physischen Umgebung bzw. der Nutzung physischer Ressourcen enthalten.

Bezogen auf einen stationären Versorgungsprozess stellt sich die Grundidee vereinfacht wie folgt gezeigt dar.

[335] International Standards Organisation, ISO/IEC 17788 Information technology - Cloud Computing - Overview and vocabulary. 2014. S. 2.

[336] International Standards Organisation, ISO/IEC 17789 Information technology -Cloud computing - Reference architecture. S. 5.

[337] „A functional component is a functional building block needed to engage in an activity, backed by an implementation. The capabilities of a cloud computing system are fully defined by the set of implemented functional components." Fn 20 , S. 7.

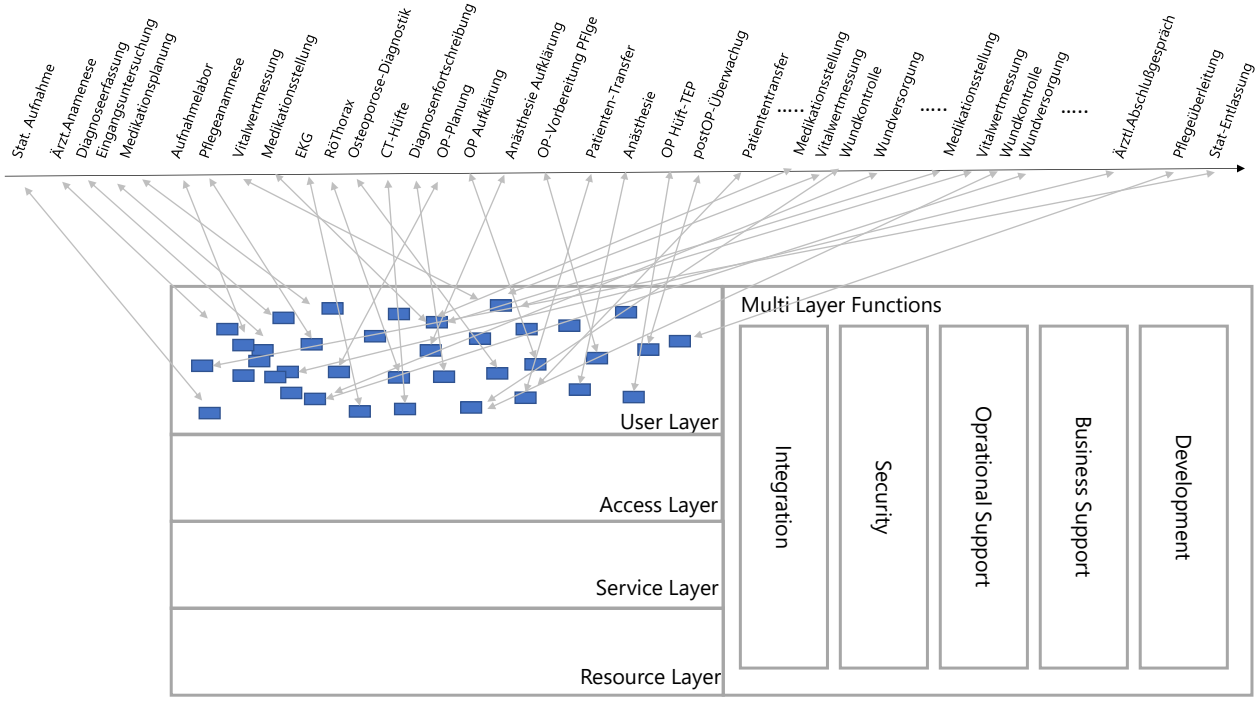

Abbildung 4-1*: Behandlungsprozess, Userfunktionen und ISO-CCRA*

Während viele der allgemein notwendigen Funktionalitäten in kommerziellen Frameworks und Plattformen schon vorhanden sind, bleibt es für jede spezielle branchenspezifische Cloud-Anwendungssoftware spezifische Aufgabe, die Benutzerfunktionalitäten also die Funktionen im User-Layer festzulegen und die Microservices dazu sinnvoll zu schneiden, zu kapseln und zu realisieren. Bei bestimmten betrieblichen Aufgaben kann es auch vorkommen, dass Benutzer direkt Funktionalitäten z.B. aus den Multi-Layer Funktionen benutzen, so wird z.B. ein Anwendungsadministrator Produktkataloge und Semantikeinträge oder Berechtigungen mit Funktionen mit Funktionen in den entsprechenden Schichten pflegen.

Ein Framework für die die Architekturentwicklung und Implementierung von Gesundheitsinformationssystemen wie z.B. KIS hat 2019 in einer ersten Version HL7 International vorgelegt, das im Kern auf die fachlogische Architektur und Interoperabilität der in vorangehender Abbildung gezeigten Module im User-Layer abzielt, aber nicht nur darauf limitiert ist. „The Service-Aware Interoperability Framework (SAIF) provides consistency between all artifacts, enables a standardized approach to Enterprise Architecture development and implementation, and a way to measure the consistency. SAIF is the framework that is required to rationalize interoperability of standards. SAIF is an architecture for achieving interoperability, but it is not a whole-solution design for Enterprise architecture management. This document describes a canonical form of Service-Aware Interoperability Framework (SAIF) which can be adapted to an organization's implementation requirements through the production of a SAIF implementation Guide.“[338] Die Grundidee: Mit einer Services-Aware Interoperability Framework Canonical Definition (SAIF-CD) können sogenannte Interoperabilitätsspezifiaktions-Matrizen (ISM) definiert werden, die als Grundlage für Compliance-Kriterien für spezielle Profile, die „Interoperability Specification

[338] HL7 International, Enterprise Consistency and Conformity Framework (ECCF). 2019. Siehe http://www.hl7.org/implement/standards/product_brief.cfm?product_id=3.

Templates (IST)", dienen, welche selbst abgeleitet sind aus organisationsspezifischen SAIF-Implementierungsleitfäden (SAIF-IGs). Die IST werden dann genutzt als Compliance-Rahmen für spezielle Spezifikationsinstanzen („Interoperability Specification Instances (ISI)"), welche Grundlage für die Implementierung konformer lauffähiger Instanzen sind.

4.4 Cloud-KIS

4.4.1 SaaS-Cloud-KIS und Ausgangssituation

Ein modulares Cloud-KIS, welches die Möglichkeiten einer Cloud-Infrastruktur z.B. der Skalierbarkeit und Hochverfügbarkeit - ausnutzen kann, ist eine nutzer- und nutzenzentrierte webbasierte **Softwarelandschaft** bestehend aus domänenspezifischen voneinander unabhängigen fachlichen und systemtechnischen Microservice-Modulen, die von verschiedensten Softwareherstellern stammen können und mittels semantischer Interoperabilität auf Basis geeigneter Mechanismen zusammenarbeiten. („modular multivendor meaningful Cloud-HIS" = m^3cloud-HIS).

Im Idealfall gibt es zu einem fachlichen Microservice-Modul (entsprechend einer „Fachfunktion") mehrere alternative Angebote, aus denen der Kunde das im genehmste auswählen kann. **Eine „Fachfunktion" stellt sowohl aus technischer als auch fachlogischer Sicht die Funktionalität für eine bestimmte betriebliche Aufgabe mit definiertem begrenztem Kontext zur Verfügung.** Eine Menge von Modulen ergeben sodann ein Anwendungssystem für einen betrieblichen Gegenstandsbereich und die Menge aller Systeme ergeben das gesamtbetriebliche Cloud-Informationssystem (Cloud Enterprise Information System EIS). In einer entsprechenden Cloud-Softwarelandschaft definieren sich konsequenterweise Systeme nicht mehr durch ihre Herkunft von einem Hersteller oder durch die gleich technische Basis, sondern sind bedarfsgerecht durch den Cloud-SaaS-Kunden zusammengestellte Sets von (Fach-)Modulen für einen definierten betrieblichen Gegenstandsbereich oder das gesamte Krankenhaus, wobei die Mehrfachverwendbarkeit von Modulen für viele Gegenstandsbereiche implizit ist.

Mit einem solchen cloud-orientierten Architekturansatz lassen sich dann durch Cloud-SaaS-Anbieter Multi-Vendor Saas-Angebote auf den Markt bringen, analog zu Multi-Vendor-Websites in Form von elektronischen Marktplatzplattformen. Denkbar sind aber auch „Master-Saas-Angebote", die wie eine Bibliothek von lauffähigen Modulen anzusehen sind und aus denen sich dann der Kunde maßgeschneidert sein EIS z.B. in seine Privat Cloud oder eine mit anderen Kunden betriebene Community Cloud oder sogar in sein On-Premises-System übernehmen kann. Damit ist eine einfache dynamische und flexible Orchestrierung der eigenen Softwarelandschaft möglich. Moderne Container-Lösungen und Deployment-Möglichkeiten von Containern minimalisieren dabei den Aufwand. Auch hierfür können entsprechende nutzungsbasierte Abrechnungsmodelle eingesetzt werden.

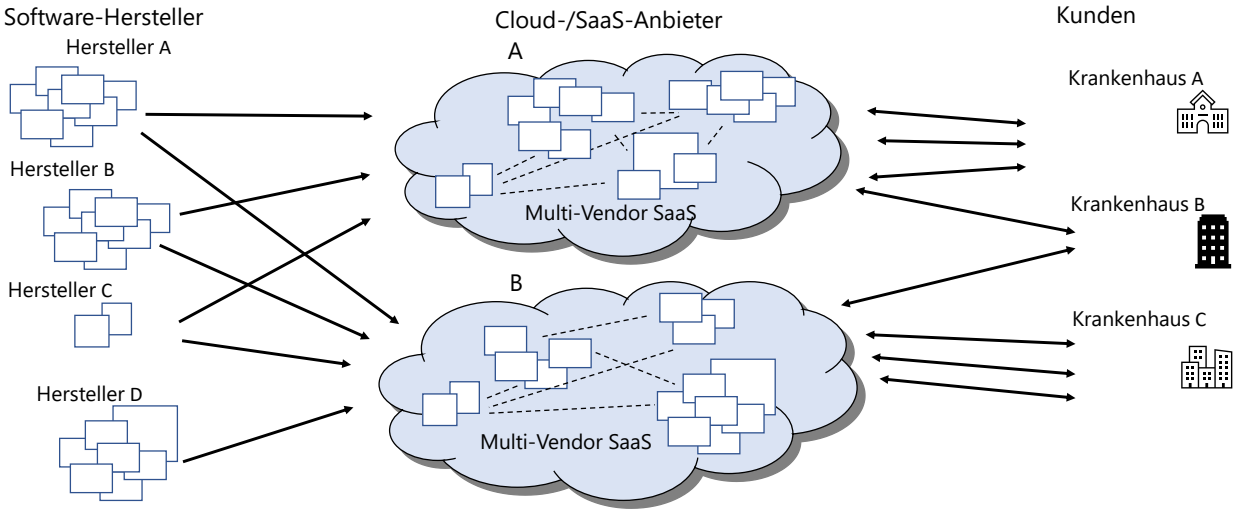

Abbildung 4-2: Cloud-KIS – Hersteller, Cloud-Anbieter und Kunden

Im Unterschied zu den herkömmlichen heterogenen KIS,

> bei denen alle Subsysteme die in der Regel von verschiedenen Herstellern stammen, viele Daten und Funktionalitäten beinhalten müssen, die auch (fast) alle anderen Systeme haben (Beispiel Patientendaten- und Falldatenverwaltung, Benutzerverwaltung und -authentifikation, Systemstammdatenverwaltung für Kostenträger, Semantikkataloge u.v.a.m.),

können sich bei einer wie zuvor beschriebenen Softwarelandschaft einzelne Systeme gemeinsam gleicher fachlogischer Komponenten bedienen bzw. selbst ausschließlich aus entsprechenden Komponenten zusammengesetzt sein, was nicht nur zur funktionalen und datentechnischen Integrität beiträgt, sondern auch zu einer beschleunigten Innovation und Agilität, da sich kleine Spezialanbieter auf ihre fachlogische Kompetenz und Innovation konzentrieren können, und nicht zusätzlich allgemein notwendige Kontextfunktionalität und Kontextdaten (Beispielswiese immer wieder eine Patientendaten- und Fallverwaltung, immer wieder eine Benutzerverwaltung usw.) zusätzlich in Ihrem Modul implementieren bzw. verwalten können müssen.

Im Gegensatz dazu stellt sich die heutige Situation eines KIS in einem Krankenhaus wie folgt gezeigt dar: Monolithische Anwendungssysteme verschiedener Hersteller werden entweder in einem Dienstleistungs-RZ oder vor Ort oder hybrid (Teile im RZ und Teile vor Ort) betrieben. Die einzelnen Systeme sind in der Regel via Messaging mittels eines Kommunikationsserver lose gekoppelt.

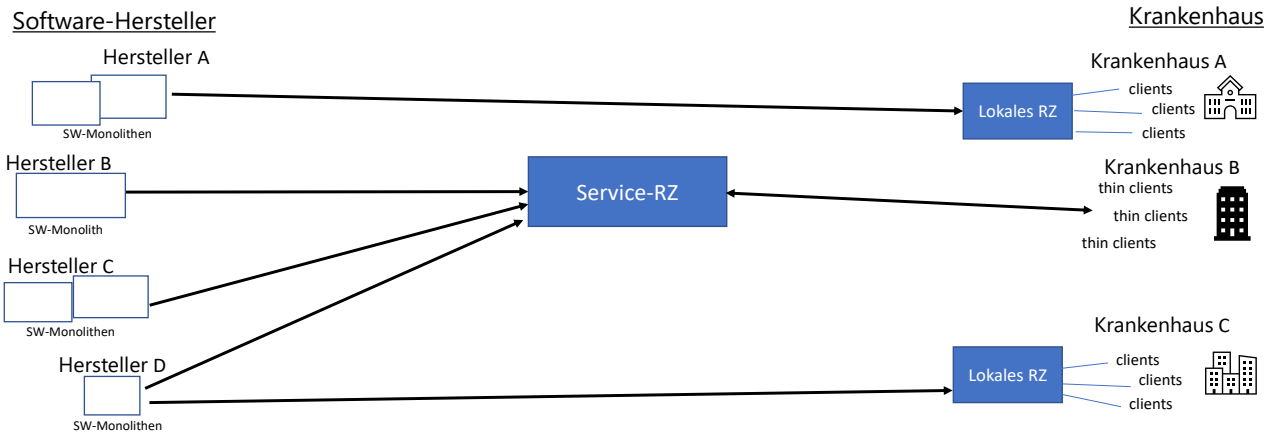

Abbildung 4-3*: Aktuelle Ausgangssituation*

Für das Aufzeigen eines Entwicklungsweges von der Ausgangssituation in Abbildung 4-3 hin zu einem SaaS-Cloud-KIS wie in Abbildung 4-1 gezeigt, stellen sich folgende zentrale Fragen:

- Welche fachlogischen Module mit definiertem „Bounded Context" können für ein KIS angegeben werden und wie **maximal feingranular** kann ein Cloud-KIS sein?
- Welche gekapselten Subsysteme können insgesamt als Cloud-Lösung ausgelagert werden und wie **maximal grobgranular** kann ein Cloud-KIS sein?
- Wie kann eine **Migrationsstrategie** sowohl auf System- als auch Modulebene aussehen?
- Welche Systeme/Module sind aufgrund loser Kopplung **primäre Migrationskandidaten?**
- Welche Systeme/Module sind aufgrund vielfacher Verwendbarkeit/Notwendigkeit **primäre Migrationskandidaten?**
- Wie können softwaretechnische **fachlogische Kopplung und Offenheit** realisiert werden, welche Rolle können dabei die **internationalen Health-IT-Standards** spielen?
- Wie können ein effektives Bridging bzw. eine Interoperabilität zwischen Cloud-KIS-Saas und proprietärem Legacy-System realisiert werden.
- Welche **übergreifenden Funktionalitäten** sollten in modularer Form in einem Cloud-KIS verfügbar sein?
- Welche Anforderungen ergeben sich an die **Orchestrierung und Parametrierung**?
- Welche Effekte haben modulare SaaS-KIS-Architekturen auf Markt und Wettbewerb?

Zur näheren Betrachtung und Klärung dieser Fragen ist es notwendig, dass die in einem KIS notwendigen Funktionalitäten bzw. die funktionale Modularisierung eines KIS exemplarisch genauer betrachtet werden.

4.4.2 Funktionale Modularisierung von KIS

Modularisierung ist ein zentraler Begriff der Informatik und spielt auch eine entscheidende Rolle für die Realisierung nutzerorientierter betrieblicher Softwaresysteme. Dabei kann zwischen der technischen und der fachlogischen Modularisierung unterschieden werden[339]. Während Erstgenannte vor allen Dingen die **technische Software-Zerlegung** betrifft und allgemeine technische Basis- und Querschnittsdienste im Blick hat, handelt es sich bei der zweiten Sichtweise um eine **nutzerorientierte funktionale Betrachtung** vor der Grundfrage: Welche Funktionalitäten eines betrieblichen Informationssystems können im Rahmen einer spezifischen Aufgabenerfüllung der einzelnen betrieblichen Akteure diese optimal bei ihren Arbeitsvorgängen unterstützen? (siehe auch Abb. Abbildung 4-1)

Im Rahmen neuerer Entwicklungen des Domain Driven Design (DDD) sowie der Architektur von betrieblichen Informationssystemen auf Basis von grobgranularen Micro-Services finden diese beiden Sichten zunehmend zusammen, sodass für Entwurf und Realisierung von betrieblichen Informationssystemen die Identifikation von anwendungslogischen Modulen[340] mit ihren Funktionalitäten wieder in den Mittelpunkt rückt. Wobei der Begriff Modul hier von einem Fachmodul mit mehreren (User-)Funktionalitäten reicht bis hin zu einzelnen User-Funktionen zur Bearbeitung bestimmter Vorgänge. Modul ist also ein sehr allgemeiner Begriff und die Größe eines Moduls hängt von der Strategie und dem Leitbild der Entwickler ab, wie sie Microservices „schneiden". So kann schon die Erfassung einer Diagnose als Modul angesehen werden, aber eben auch das gesamte Medikationsmanagement, wenngleich letztgenanntes Beispiel schon weniger die Architekturidee der Cloud-nativen Anwendung erfüllt.

Die Diskussion um Software-Architekturen und die damit verbundenen Konzepte wurden in den vergangenen Jahren auch durch die Entwicklung hin zu Cloud-basierten Anwendungssystemen bzw. SaaS-Angeboten befördert. Lose auf Basis von vereinbarten Standards gekoppelte Module spielen hier nicht nur im Sinne der Softwarearchitektur eine große Rolle, sondern auch aus geschäftsstrategischen Gründen der Cloud Anbieter, denn Module können nicht nur aus Gründen der Softwarepflege und Weiterentwicklung leicht und ohne Nebeneffekte ausgetauscht werden, sondern es können Module verschiedenster Software-Lieferanten - gegebenenfalls auch als Alternativen – zum Einsatz kommen.

Aber nicht nur für die **Neuentwicklung** von Software spielt dieser Ansatz eine große Rolle, sondern auch für die **Migration** bestehender großer Software-Systeme hin zu skalierbarer bzw. orchestrier- bzw. choreografierbarer Cloud-Software, denn es wird ein an diesem Paradigma orientiertes **Refactoring** der „Altsoftware" notwendig, bei dem maximale **Kohäsion** und maximale **lose Kopplung** im Vordergrund stehen mit der Frage, welche Funktionalitäten können sukzessive aus dem Legacy-System herausgelöst und „cloudisiert" werden.

---

[339] Winter unterscheidet in seinem 3LGM²-Modell drei Layer, die es zu unterscheiden gilt, wobei die nutzerorientierte Funktionalitätsbetrachtung auf der logischen Ebene stattfindet. (Winter, The 3LGM2-tool to support information management in health care. 2011).

[340] „Die Möglichkeit, semantisch zusammenhängende Software-Einheiten syntaktisch in einem Modul zu kapseln, wird als Merkmalkohäsion (engl. feature cohesion) bezeichnet. Die Zusammenstellung kann im Folgenden als einzelne, semantisch vollständige Einheit betrachtet werden." Kuhlemann, Moderne Modularisierungstechniken und ihre Bedeutung für qualitativ hochwertige Software. 2006. S. 7.

Mit Blick auf die zuvor dargestellte Multi-Vendor-Cloud wird es geradezu eine Notwendigkeit, Softwaresysteme entsprechend zu zerlegen und standardisiert interoperabel zu machen um somit für die Kunden **skalierbare KIS-Softwarelandschaften als SaaS-Angebot** zur Verfügung stellen zu können.

Wie bereits in Kapitel 2 dargestellt, kann ein KIS und die verschiedenen Systeme, aus denen das KIS besteht, aus sehr verschiedenen Sichten betrachtet werden, ebenso können verschiedene Systemtypen unterschieden werden. Wesentliche Betrachtungsdimensionen sind:

- Mengenorientierte operative vs. werteorientierte vs. berichts- und kontrollorientierte vs. analyse- und planungsorientierte Systeme (siehe auch Abbildung 2-1)
- Vertikale vs. horizontale vs. teilhorizontale Systeme
- Arbeitsplatz- vs. Bereichs- vs. Abteilungs- vs. Unternehmenssysteme (siehe auch Abbildung 2-3)
- Kernsysteme und Subsysteme, die selbst wieder verschiedenen Klassen zugeordnet werden können – hier vor allem die Fachabteilungssysteme vs. Funktionsstellensysteme vs. Pflegeinformationssystem (siehe auch Abbildung 2-2)

Aus technischer Gesamtsicht sind alle einzelnen Anwendungssysteme als „Subsysteme" zu betrachten – also Teil des Gesamtsystems. Die Software jedes monolithischen Anwendungssystems ist dann selbst wieder aus entsprechenden technischen und fachlogischen Teilen aufgebaut und hat gegebenenfalls spezielle ergänzende eigene „Subsysteme" wie z.B. angeschlossene Medizintechniksysteme oder spezielle Peripheriegeräte. Auch ist es denkbar, dass ein Anwendungssystem entsprechend mit einem anderen spezialisierten Anwendungssystem zusammenarbeitet. Vertikale Systeme – wie sie auch in der Informationssystempyramide in Abb. 2-1 gezeigt vor allem in den unteren beiden Schichten vorkommen – lassen sich besonders gut isoliert in die Cloud separieren und migrieren. Dabei sollte zu Beginn auch schon ein Gesamtkonzept für die Nutzung der für alle Systeme notwendigen Grunddaten (auch Stammdaten oder Systemdaten genannt)[341] entwickelt werden, denn deren ubiquitäre Verwaltung kann z.B. selbst als Cloud-Module schon isoliert als Teil eines Cloud-fähigen KIS prioritär implementiert werden.

Auch innerhalb der Software der vorhandenen Legacy-Anwendungssysteme gibt es dann wieder vertikale und horizontale Funktionalitäten, d.h. solche die nur für einzelne Arbeiten bzw. Arbeitsbereiche gebraucht werden (vertikale Softwarebausteine wie Befundschreibung, Bild-Befundungssoftware, Anamnesedokumentation etc.) und solche, die von allen oder vielen Mitarbeitern genutzt werden (Arbeitslisten, Terminplaner usw.).

In der Regel gibt es jedoch in den Krankenhäusern ein „führendes" medizinisches monolithisches Kernsystem und ein „führendes" administratives monolithisches Kernsystem. Während das administrative Kernsystem im Wesentlichen aus einer Menge von vertikalen Anwendungen mit sehr speziellen Funktionalitäten für die einzelnen administrativen Fachabteilungen besteht, hat das medizinische Kernsystem auch viele (teil-)horizontale Anwendungen, so z.B. das Order

[341] „Grunddaten (auch Stammdaten) sind das datenäquivalente Abbild der betrieblichen Ressourcen, die über lange Zeiträume abgebildet werden. Dies sind Objekte (z.B. Produkte) oder Subjekte (z.B. Mitarbeiter). Die Grunddaten steuern alle betrieblichen Vorgänge, die als Daten aufgezeichnet werden." Spitta/Bick, Informationswirtschaft. 2008. S. 73.

Entry-/Result-Reporting-Modul (ORM), das im Grunde von fast allen medizinischen Abteilung genutzt wird oder ein Formulargenerator zur Erstellung von Laufzeit-Formularen für alle Fachbereiche oder Terminmanagement-Funktionen oder eine Befundschreibefunktion.

Damit ergibt sich das folgende Bild einer logischen KIS-Topologie. Durch die gestrichelten Pfeile soll verdeutlicht werden, dass je nach Ausgestaltung eines konkreten KIS manche „Subsysteme" bereits in den Kernsystemen enthalten sind oder aber als eigenständige außerhalb des Kernsystems implementierte Subsysteme eines anderen Herstellers betrieben werden. Breite und Tiefe der Funktionalität in spezialisierten Subsystemen übersteigen meist jene der im Kernsystem angebotenen entsprechenden Module für den betreffenden betrieblichen Gegenstandsbereich.[342] Während administrative Systeme als verbindende Datenbasis alle betriebswirtschaftlichen Daten und Bestandsdaten zu Geräten, Mitarbeitern, Materialien etc. umfasst, ist die verbindende Grundlage der Medizinischen Systeme die institutionelle Elektronische Patientenakte (iEPA).

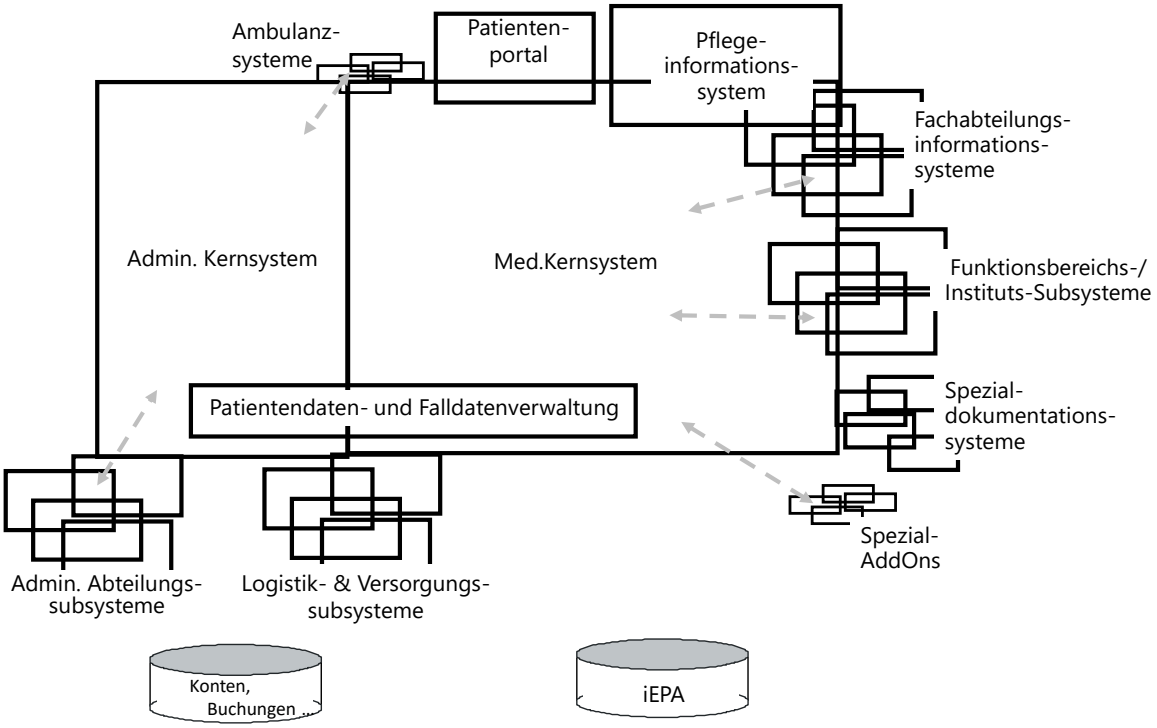

Abbildung 4-4: Funktionale Zergliederung eines KIS auf oberster Ebene

Hinsichtlich einer weiteren **funktionalen Modularisierung** können dann in einem Anwendungssystem weitere abgrenzbare Teile angegeben werden, die oftmals als Modul[343], dann Submodul und auf unterster Ebene als Anwendungsfunktion bezeichnet werden. Anwendungsfunktionen können noch gewisse Anwendungs-Subfunktion haben. Insgesamt ergibt sich also eine Hierarchie aus EIS -> (Sub)System -> Modul -> Submodul -> Anwendungsfunktion ->

[342] In diesem Zusammenhang wurde bereits Mitte der 90er Jahre die Ansätze Monolith vs. „Best of Breed" diskutiert. Siehe hierzu auch Koch, Best-of-Breed 3.0 oder: quo vadis, ganzheitliches KIS? 2011. S. 14-15.

[343] Der Begriff „Modul" in diesem Kontext bezeichnet eine andere Aggregation von Funktionalitäten als dies ein Modul im Sinne eines Softwarebausteines für eine MicroService-Architektur ist.

Subfunktion. Beliebig tiefergehende Gliederungen sind denkbar, zumeist aber wenig praktikabel für die Benutzer, da so dann auch eine tiefe und unübersichtliche Benutzungsnavigation entsteht. Software-technisch können Subfunktionen auch generische Funktionen sein (z.B. eine komplexe Auswahlliste zur Suche in großen Domainwert-/Bezugsobjekt-Mengen zu Befüllung eines Feldes in der Hauptmaske, Datumsauswahlmasken, Körper-Topografie zur Lokalisationsauswahl), die z.B. in Software-Bibliotheken zusammengefasst sind und von vielen Anwendungsfunktionen genutzt werden.

Die vorangehend aufgeführten Aspekte sind in der nachfolgenden Abbildung beispielhaft für ein Radiologieinformationssystem (RIS) gezeigt, welches so selbst schon ein kleines Ökosystem darstellt. Analog gilt dies jedoch für viele andere Anwendungssysteme wie dedizierte Laborinformationssysteme, Pflegeinformationssysteme, Anästhesieinformationssysteme usw..

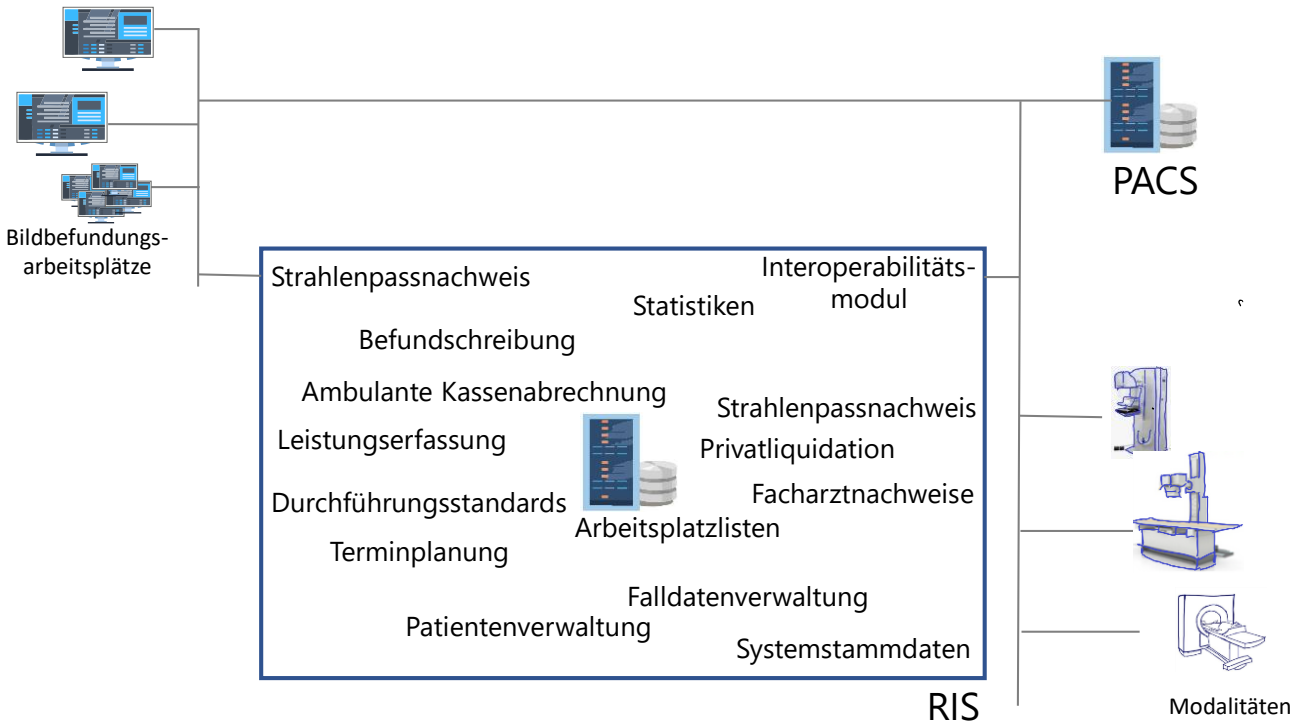

Abbildung 4-5: Radiologie-IT als Ökosystem

Bezüglich der beiden großen Kernsysteme eines KIS gibt es einen wesentlichen Unterschied: Während es sich beim administrativen Kernsystem zum Großteil um eine Aggregation von vertikalen Systemtypen handelt, besteht das medizinische Kernsystem sowohl aus vertikalen als auch horizontalen oder teilhorizontalen Systemen bzw. Funktionalitäten.

Im administrativen Kernsystem finden sich in der Regel die in Abbildung 2 gezeigten administrativen Systeme; minimal jedoch jene für die Patientendatenverwaltung und -abrechnung, alle Systeme bzw. Module für das Rechnungswesen und Controlling-Software. Andere administrative und logistische Systeme können ebenfalls im Kernsystem enthalten sein, werden teilweise aber auch als dedizierte eigenständige Subsysteme beschafft und betrieben. Der Grad der Heterogenität und Anzahl der spezialisierten Subsysteme korreliert stark mit der Größe und organisatorischen Differenzierung eines Krankenhauses, je größer desto mehr verschiedene Subsysteme kommen zum Einsatz.

Hinsichtlich der Funktionalitäten eines EHR-Systems – in diesem Kontext der klinische Teil eines KIS, also das klinische Kernsystem – gibt HL7 über **230 verschiedene Funktionalitäten** bzw. Leitungsmerkmale in 4 Kategorien an, die für verschiedene Zwecke profiliert werden können[344]. Solche Profile können bei modularer Implementierung der Funktionalitäten dann „Modul-Bundles" in der Softwareumgebung angesehen werden. Im HL7-Functional Model wird eine hierarchische Funktions-Gliederung mit bis zu vier Ebenen angegeben. Aggregiert werden diese jeweils auf oberster Ebene in sechs generelle Funktionsklassen. Nachfolgende Abbildung zeigt einen kleinen Ausschnitt aus der Hierarchie des HL7-EHR-Functional Models.

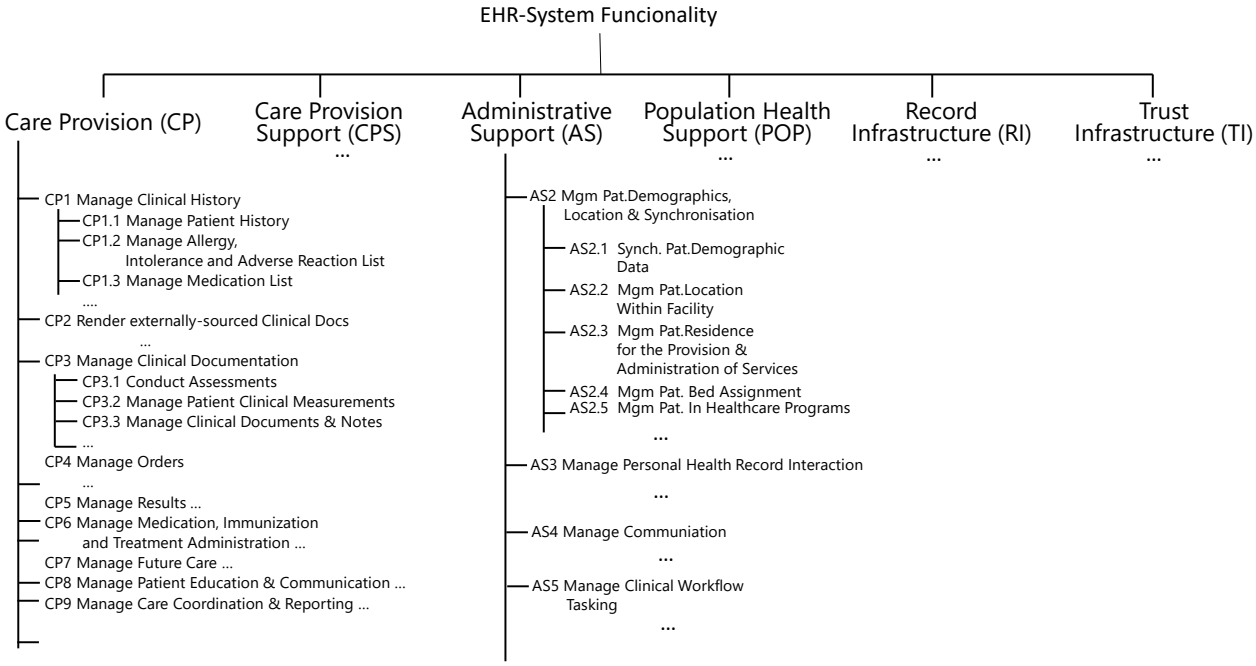

Abbildung 4-6*: Gliederungsauszug HL7 EHR Functional Model*

Ausführlich werden die wesentlichen Module und inhärenten Funktionalitäten eines Medizinisches Informationssystems in Form eines Schichtenmodelles detailliert bei Haas[345] beschrieben. Dabei werden die Module Stammdatenverwaltung, Patientenverwaltung, Fallverwaltung, Medizinische Dokumentation mit zahlreichen Submodulen, Organisation, Kommunikation und Materialverwaltung, Entscheidungsunterstützung sowie Statistik und Datenschutzmechanismen unterschieden.

[344] HL7 International, HL7 EHR-System Functional Model Release 2. 2014.

[345] Haas, Medizinische Informationssysteme und Elektronische Krankenakten. 2005. S. 278, 510.

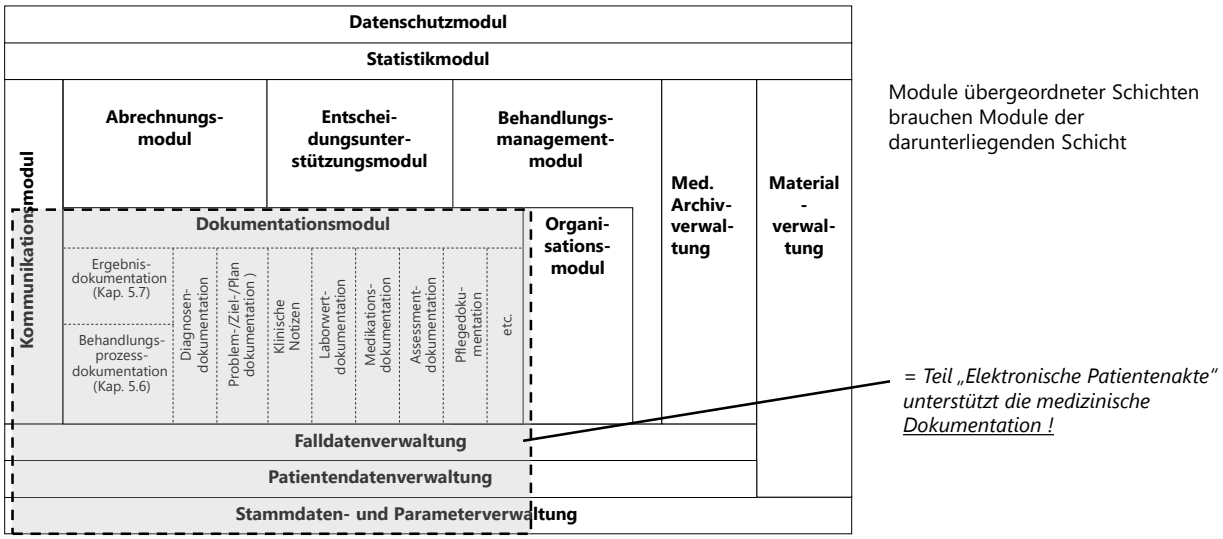

Abbildung 4-7: Schichtenmodell eines Medizinischen Informationssystems

Auch für die Reifegradbestimmung des KIS-Einsatzes bedarf es einer Angabe von Systemen, Modulen und Funktionalitäten, was die beiden führenden Modelle wie HIMSS-MRAM und der CHIME-Foundation in unterschiedlicher Weise berücksichtigen und bei den Einstufungen entsprechende Begrifflichkeiten auftauchen, die Systemen oder Modulen oder Anwendungsfunktionen entsprechen:

- Die HIMSS EMRAM-Kriterien mit 7 Stufen, es werden verschiedene Subsysteme und Funktionalitäten benannt (siehe auch Kapitel 2, Tabelle 2-2)
- Das Reifegradmodell der CHIME Foundation, in welchem 10 Stufen definiert sind, denen jeweils ebenfalls bestimmte Module und Funktionalitäten zugeordnet sind.

Die seit über 15 Jahren regelmäßigen Erhebungen zum IT-Einsatz in Krankenhäusern – zum Teil mit Fokussierung auf bestimmte Schwerpunkte wie Pflege, klinische Prozesse, Technologie usw. – durch die Forschungsgruppe Informatik im Gesundheitswesen der Fachhochschule Osnabrück[346] gibt ebenfalls ausführliche Informationen zu Modulen und Funktionalitäten von KIS. So wurde in 2018 ebenfalls der IT-Reifegrad erhoben[347].

Die nachfolgende Tabelle zeigt ausschnittsweise einige der wesentlichen (logischen) Systeme bzw. Module des klinischen Teiles des KIS, ggf. Submodule und einige beispielhaften Funktionalitäten. Bewusst wird an einigen Stellen beispielhaft auf Funktionalitätsebene detailliert, um im Folgenden darauf Bezug nehmen zu können.

Tabelle 4-1: Liste von KIS-Modulen und -Funktionen (Auszug)

Patientendatenverwaltungs- und Abrechnungssystem
Patientenverwaltung
Patientenstammdaten
Bezugspersonen
behandelnde Ärzte
Fallverwaltung

[346] siehe https://www.hs-osnabrueck.de/forschungsgruppe-informatik-im-gesundheitswesen/.

[347] Hübner et al, IT-Report Gesundheitswesen - Schwerpunkt Wie reif ist die IT in deutschen Krankenhäusern? 2018.

- Stationäre Fallverwaltung
  - Fallanlage stationärer Fall
  - Einweiserangaben
  - Versicherungsangaben
  - Wahlleistungserfassung
  - ....
  - DRG-Dokumentation
- Ambulante Fallverwaltung
  - Ambulante Fallanlage
  - Versicherungsangaben
  - ...
- Notfallaufnahme
- Stationäre Abrechnung
- Ambulante Abrechnung
  - Kassenabrechnung
  - Privatabrechnung
  - Sonderabrechnungen
- Klinische Dokumentationsmodule/-funktionen
  - Klinische Eingangsuntersuchung
  - Anamnese
  - Zwischenanamnese
  - Diagnosedokumentation
  - Symptomdokumentation
  - Verordnungsdokumentation/Medikationsmanagement
    - Medikationsübersicht
    - Medikation/Medikament anordnen und Anordnung prüfen
    - Medikament für Patienten bestellen
    - Medikamentenausgabe dokumentieren
    - Medikamenteneinnahme/-verabreichung dokumentieren
    - Unverträglichkeit dokumentieren
    - Medikationsabsetzung dokumentieren
    - Medikationswiederaufnahme dokumentieren
  - Visitendokumentation
  - Aufklärungsdokumentation
  - OP-Dokumentation
  - Anästhesiedokumentation
  - Wunddokumentation
  - Schmerzdokumentation
- Anforderungs- und Befundrückmeldungsmanagement
  - Leistungsanforderung
  - Terminierung
  - Leistungsdokumentation
  - Befund-/Ergebnisdokumentation (siehe auch nachfolgender Punkt)
- Spezielle Therapiedokumentation
  - Physiotherapiedokumentation
  - Logopädiedokumentation
  - Chemotherpiedokumentation
  - Strahlentherpiedokumentation
  - ...
  - Psychotherapiedokumentation
  - ...
- Pflegedokumentation
  - Pflegeanamnese
  - Pflegezielplanung
  - Pflegeplanung
  - Pflegemaßnahmendokumentation

Vitalwertdokumentation
Medikamentenverabreichungsdokumentation
Wunddokumentation
Schmerzdokumentation
Medikamentenverabreichungsdokumentation
…

Dabei kann vor allem die Dokumentation der Ergebnisse von diagnostischen und therapeutischen Maßnahmen - die ja sehr vielfältig sein können – hinsichtlich der Menge der einzelnen isolierten Dokumentationsfunktionen sehr umfangreich werden und in die Tausende gehen.

Eine Detaillierung einzelner Bereiche wurde z.B. in den Förderkriterien zum Krankenhauszukunftsgesetz vorgenommen, z.B. für Funktionalitäten eines Medikationsmanagements, der Pflegedokumentation oder eines Aufnahme- und Entlassmanagements.

Mit Blick auf großen Umfang an Funktionalitäten in einem KIS und der weitreichenden Granularität von oft unabhängig voneinander verwendeten Funktionalitäten stellt sich prinzipiell die Frage, wie eine Migration bzw. die Granularität eines SaaS-Cloud-KIS sein kann. Einem modularen Cloud-Ansatz kommt dabei zugute, dass die Nutzung der meisten Funktionalitäten sehr speziell in einem bestimmten Behandlungskontext erfolgen und gut abgrenzbar sind.

4.4.3 Cloud-Migration von KIS

Die Software für die Kernsysteme und Subsysteme in Krankenhäusern ist über viele Jahre bis Jahrzehnte entstanden und basiert auch heute zum Teil noch auf Software-Technologien aus diesen Jahren. Solche Systeme werden auch als „**Legacy-System**“ bezeichnet, dementsprechend wir im Folgenden vom „Legacy-KIS“ gesprochen. Diese Systeme lassen eine echte Migration hin zu Cloud-fähigen webbasierten Systemen zumeist nicht ohne Neuimplementierung zu, da ihr Code für diese Zwecke nicht wiederverwendbar ist.

Damit wird deutlich, dass es für Legacy-KIS einer schrittweisen Migration oder einer Neuimplementierung bedarf. Für ein migratives Vorgehen stellen sich einige der vorangehend aufgeführten Fragen:

- Welche fachlogischen Module mit definiertem „Bounded Context“ können für ein KIS angegeben werden?
- Wie **maximal feingranular** kann/sollte ein Cloud-KIS sein?
- Welche gekapselten Subsysteme können insgesamt als Cloud-Lösung ausgelagert werden?
- Welche Systeme/Module sind aufgrund loser Kopplung **primäre Migrationskandidaten?**
- Welche Systeme/Module sind aufgrund vielfacher Verwendbarkeit/Notwendigkeit **primäre Migrationskandidaten?**

Grobgranulares Cloud-KIS

Mit Blick auf die heute in den Krankenhäusern vorherrschenden heterogenen KIS erscheint es in einem ersten Schritt auf den ersten Blick als einfachster Lösungsansatz, dass einzelne lose gekoppelte Subsysteme – die ja heute auch schon nur über Nachrichtenaustausch z.B. via Kom-

munikationsserver und HL7-Nachrichten an das Kernsystem angebunden sind – als Cloudlösung migriert werden. Diese sind gegebenenfalls dann als granulare Monolithen („Modulithen“[348]) in der Cloud.

Mit Blick auf Abbildung 2-1 und Abbildung 4-4 sind hierfür ideale Kandidaten die Subsysteme mit vertikalem Charakter wie z.B. RIS, PACS, LIS, Pflegeinformationssystem, Materialwirtschaftssystem, Apothekensystem u.v.a.m. Die geschäftspolitische Entscheidung zur Migration für ein gesamtes Produkt muss aber jeder Subsysteme Hersteller für sich selbst treffen, also inwieweit er sein Produkt zu einer cloudfähigen Webanwendung umbaut bzw. migriert. Prinzipiell können so dann schon bestimmte Systemlandschaften als SaaS angeboten werden oder Krankenhäuser z.B. in einer Region sich in einer Community-Cloud entsprechender Lösungen und Leistungen – gegebenenfalls gemeinsam – bedienen. Denkbar heute schon z.B. für PACS.

Im Sinne von Zukunftsfähigkeit, Nachhaltigkeit und Weiterentwicklung sollten Krankenhäuser bei der Auswahl zu Neubeschaffungen von IT-Systemen bei den entsprechenden Kosten Nutzen Betrachtung zukünftig auch Kriterien für die teilweise oder gesamtheitliche Web-/Cloud-Fähigkeit dieser Systeme mit einbeziehen.

Bei einem solchen grobgranularen Ansatz würden so über eine sehr lange Übergangszeit von ca. 10-15 Jahren „Hybridlandschaften“ aus Cloud-Lösungen und klassischen Client-Server-Legacy-Lösungen am Ende zu **grobgranularen Cloud-KIS** führen, bei denen zwar alle Kern- und Subsysteme Cloud-Software sind, die aber dennoch nicht die Anforderungen und Erwartungen an ein skalierbares Cloud-KIS erfüllen, da es sich immer noch um ein loses Ensemble von „Cloud-Monolithen“ oder „Cloud-Modolithen“ handelt.

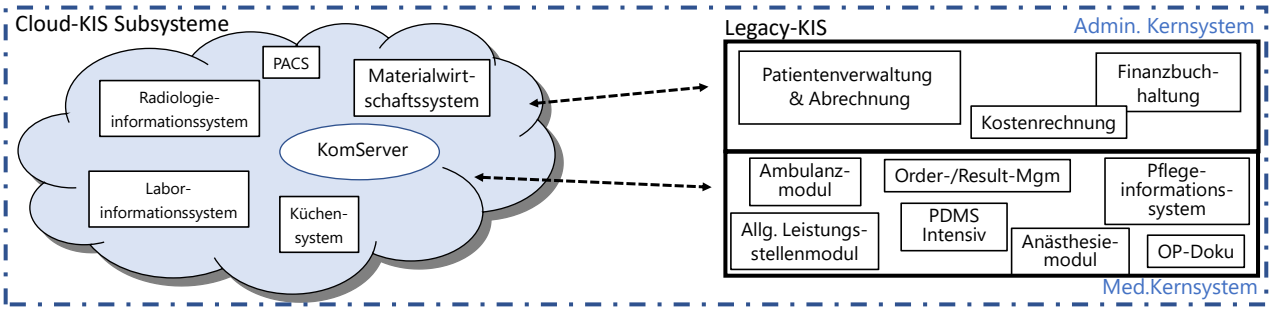

Abbildung 4-8: Beispiel grobgranulares Cloud-KIS als Hybrid aus Cloud-Mono-/Modulithen und Legacy-Kernsystem in der Übergangsphase

Eine Integration an der Oberfläche der einzelnen Systeme ist nur selten notwendig – wie auch heute schon bei heterogenen KIS, bei denen sich ein Benutzer selten in mehreren Subsystemen bewegen muss – und wenn, dann ist dies bezüglich der Cloud-Mono- oder Modulithen über geeignete Webaufrufe aus der proprietären Anwendung heraus leicht zu bewerkstelligen.

[348] Der Begriff Modulith bezeichnet ein modulares aber immer noch nur insgesamt deploybares System. Siehe u. A: https://www.informatik-aktuell.de/entwicklung/methoden/modulith-first-der-angemessene-weg-zu-microservices.html. Diese können zwar Cloud-fähig sein, sind aber nur modular für den Hersteller und trotzdem von außen nur wenig offen, also monolithisch. Als Geschäftspolitik schützen Sie vor Mitbewerbern und modularen Mitanbietern.

Cloud-Mono-/Modulithen können über die bereits vorhandenen Integrationstechnologien – in der Regel Kommunikationsserver zum Management des Messagings – ebenso uni- oder bidirektional in die Systemlandschaft eingebunden werden, zumal die gängigen Kommunikationsserver alle dazu notwendigen technischen Protokolle bereits beherrschen.

Das grobgranular Cloud-KIS selbst kann jedem der in Kapitel 2 genannten Modelle folgen, vermutlich wird man aber für solche Systeme, die Patientendaten enthalten, eher eine Community oder Privat Cloud wählen, ggf. auch On-Premises.

Feingranulares Cloud-KIS

Im Gegensatz zum grobgranularen Cloud-KIS besteht ein feingranulares modulares Cloud-Softwaresystem aus Web- und Cloud-fähigen Modulen, die im Sinne des Domain Driven Design je eine (Geschäfts)Funktionalität für jeden bestimmten administrativen und/oder klinischen Anwendungskontext zur Verfügung stellen (siehe auch Abbildung 4-1). Diese Module sind nicht mehr nach einzelnen Systemen bzw. Systemgrenzen im klassischen Sinne ausgerichtet, sondern nach der für einen Benutzer in einer bestimmten Situation notwendigen Funktionalität („funktionaler Schnitt") mit abgrenzbarem Kontext („Bounded Context"). Dabei kann sich dieser „Bounded Context" einerseits um die sich in einer bestimmten Situation notwendige Funktionalität und zugehörigen Informationsobjekttypen beziehen (Design-Aspekt), andererseits dann aber auch bezogen auf die Datenausprägungen, die dieser Funktionalität zur Laufzeit zugrunde liegt. In diesem Sinne kann es dann mehrere Instanzen von Modulen geben, die sich nur im „Bounded Data Context" (Laufzeitaspekt) unterscheiden.

Solche modularen Cloud-Lösungen werden auch als **Native Cloud Applications (NCAV)** oder Cloud Native Anwendungen bezeichnet, da sie die Möglichkeiten und Vorteile der technischen Cloud-Infrastrukturen und softwaretechnischen Architektur konsequent nutzen bzw. zur Laufzeit alle Vorteiler skalierbarer Infrastrukturen ausschöpfen können. Die Anwendungssystemmodule können maximal flexibel und ortsunabhängig auf beliebigen Servern, gegebenenfalls auch redundant bzw. gespiegelt, eingesetzt werden und benötigen weder eine bestimmte Hardware noch spezifische Betriebssysteme. NCA-Entwicklungs- und Bereitstellungsumgebungen werden zunehmend als Produkte am Markt angeboten.

An einem kleinen Beispiel sei diese Auflösung des systembezogenen Denkens und Entwickelns verdeutlicht: In vielen Abteilung oder Arbeitsbereichen wird heute die Führung eines zumeist ressourcen-orientierten Terminkalenders notwendig[349]. Eine solche Funktionalität unterscheidet sich im Grunde zwischen der Radiologie, einer Spezialambulanz, der OP-Raumbelegungsplanung, der Terminplanung für kleinere Leistungsstellen wie EKG, EEG etc. nicht wesentlich. Denn es gibt Ressourcen und Slots und konkret zu planenden Events mit einer bestimmten Plandauer. Bei einem heterogenen KIS ist aber in jedem Subsystem und in der Regel auch im Kernsystem Terminplanungssoftware enthalten, die mit dem Erwerb des entsprechenden Kern-/Subsystems natürlich auch bezogen und bezahlt werden muss. Im Grunde wird also eine für das gesamte Krankenhaus bzw. viele einzelne Organisationseinheiten notwendige Kernfunktionalität mehrfach betrieben und bezahlt.

[349] Zu allgemeinen Betrachtungen siehe Haas, Medizinische Informationssysteme und Elektronische Krankenakten. 2005. S. 530 ff.

Dieses Beispiel lässt sich auf sehr viele andere Funktionalitäten im KIS übertragen – so zum Beispiel die Workflowsteuerung, die klinische Diagnosedokumentation, die Medikationsdokumentation, eine wenn überhaupt vorhandene explizite Symptomdokumentation, die Personaleinsatzplanung, verschiedene Assessments, Anamnesedokumentation, die Verwaltung von Systemstammdaten wie z.B. der Krankenhausstruktur und des zugeordnetes Personals sowie der Benutzer, der Verwaltung von Semantik, die Benutzerverwaltung und das Rechtemanagement u.v.a.m.. Auch eine Patientenstammdaten – und Falldatenverwaltung gibt es im Grunde funktional in ähnlicher Ausprägung im Kernsystem und in jedem patientenbezogenen Subsystem gesondert. Zusätzlich werden so im heterogenen System viele Daten redundant gehalten und der Aufwand der integren Synchronisation ist beträchtlich bzw. für die manuelle Doppelpflege wie das bei den Systemstammdaten üblich ist.

Alle diese vorgenannten Funktionalitäten – bzw. sogar noch granularere daraus – können im Prinzip als gekapselte Module mit loser Kopplung realisiert und in unabhängigen wie auch immer kommunizierenden Containern in einer Cloud betrieben und konsumiert werden.

Ein modulares multivendorfähiges Cloud-KIS (mCloud-KIS) ist also die Summe aller cloudbasierten MicroServices (im Folgenden mit Cloud-Micro Service-Modul[350] bezeichnet, CMSM abgekürzt), die für den operativen Betrieb und die Steuerung sowie für das taktische und strategische Krankenhausmanagement notwendig sind.

Im Gegensatz zum grobgranularen (Hybrid)Ansatz stellt sich ein **feingranulares Cloud-KIS** wie folgt beispielhaft gezeigt dar, hier mit Blick auf die ISO-CCRA beschränkt auf den **User-Layer**.

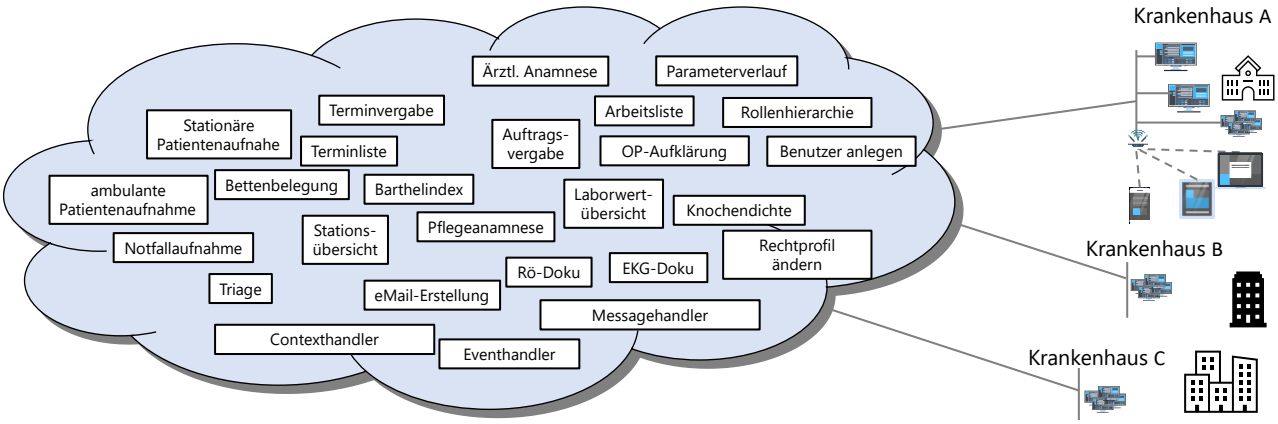

Abbildung 4-9: Beispiel für feingranulares Cloud-KIS (nur User Layer und Auszug)

Zur Identifikation geeigneter Modul-Kandidaten für einen Migrationsprozess im Rahmen des strategischen Designs können folgende Fragen herangezogen werden:

- Handelt es sich um Funktionalitäten in und mit einem beschränkten Kontext für eine dedizierte betriebliche Aktivität – also im Sinne des DDD um eine Subdomäne?
- Wird die Funktionalität von vielen Akteuren in unterschiedlichen Organisationseinheiten des Krankenhauses benötigt?

[350] Der hier gewählt Begriff soll verdeutlichen, dass im Folgenden ein Microservice jeweils ein feinstmöglichstes fachlogisches Modul realisiert.

- Ist die Kontextüberschneidung mit anderen Kontexten und vor allem auch mit dem administrativen bzw. medizinischen Kernsystem klein und damit eine lose Kopplung mit wenig Interaktion möglich? Das heißt: Kann ein isoliertes dediziertes Informationsmodell dafür angegeben werden?
- Wird die Funktionalität flexibel und unabhängig von Raum und Zeit – also ubiquitär – notwendig?

Darüber hinaus kann noch untersucht werden, ob innerhalb des beschränkten Kontextes bzw. der Subdomäne weitere abgrenzbare Aktivitäten existieren und somit eventuell eine weitere Zerlegung sinnvoll sein kann. Eine solche Betrachtung ist wichtig, um nicht direkt wieder zu große abhängige Einheiten entstehen zu lassen.

Daraus ergibt sich eine allgemeine Kriterienliste für Design-/Migrationsentscheidungen:

Tabelle 4-2*: Kriterienmatrix zur Identifikation von CMSM-Kandidaten*

Kriterium	Ja	Nein	Anmerkung
Betriebliche Subdomäne?			
Vielfache betriebliche Nutzung?			
Kontextüberschneidung klein?			
Ubiquitäre?			
Weiter Untergliederung?			

Bezüglich einer Migration von Legacy-Systemen zeigt sich, dass vor allen Dingen bei der Neuentwicklung von Funktionalitäten architektonisch die ersten Schritte in Richtung eines mCloud-KIS vollzogen werden können, indem solche Funktionalitäten in der vorangehend beschriebenen Weise als Cloud-MS-Module (CMSM) realisiert und mittels loser Kopplung und Kontextaustausch in das bestehende Altsystem integriert werden.

4.4.4 Fallbeispiele für CMSMs

Vorbemerkungen

Ein wesentlicher Aspekt ist die Kopplung von CMSM mit Legacy-Systemen bzw. mit anderen CMSM. Gerade für einen Migrationsprozess und die Förderung von Anwendungsinnovationen ist auch eine Zusammenarbeit von CMS_M und Legacy-Systemen von großer Bedeutung. Dabei sind drei Aspekte von grundlegender Bedeutung, die einer Entscheidung und Implementierung bedürfen:

1 Wie erhält das CMSM den mit dem KIS bzw. anderen Modulen überlappenden Kontext?
2 Wie kann der Aufruf des CMSM aus dem Legacy-System (oder anderen CMSM) heraus erfolgen?
3 Welches eigene „Gedächtnis" hat das CMSM, also welche Daten werden dort primär für die Aufgabe gekapselt gespeichert?

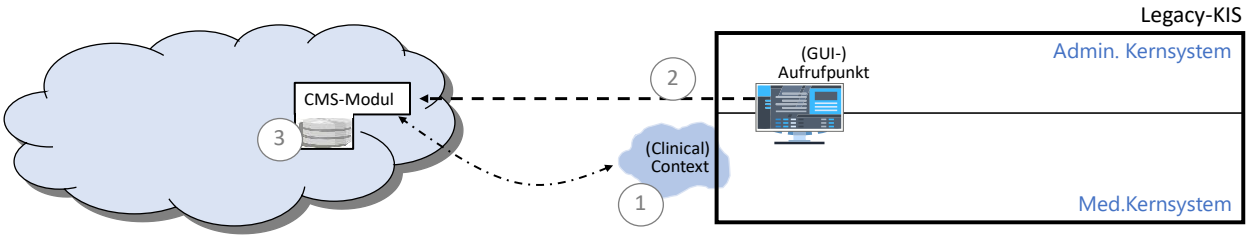

Abbildung 4-10*: Legacy-System und Cloud-Modul*

Für die Implementierung der Aufrufbarkeit ist von Vorteil, dass aufgrund der den CMSM zugrundeliegenden Internettechnologie ein solcher Aufruf aus Legacy-Systemen einfach zu bewerkstelligen ist, da nur eine http-Adresse bzw. Ressource-Adresse und die Übergabeparameter angegeben werden müssen, was einer sehr losen Kopplung entspräche. Andere Formen der Parameterübergabe via Persistenzschicht sind aber auch denkbar. Für eine isolierte Kontextübermittlung – was eine losere Kopplung darstellt und keine direkten Schnittstellenabhängigkeiten schafft – können diverse Ansätze verfolgt werden, die jeweils ihre Vor- und Nachteile haben vor allem mit Blick auf die Kopplungsenge.

- Mittels RPC bzw. mittels Services
- Mittels Event-Bus, ggf. zerteilt in Segmente
- Mittels Messaging-Infrastruktur z.B. Kommunikationsserver
- Mittels Kombination der Ansätze

Weitere Überlegung hierzu finden sich in Kapitel 4.9.3.

CMS-Module können bei entsprechender cloud-konformer Realisierung und als Webanwendung bei Nutzung von Instrumenten des aktuellen Standes der Software-Technik auch responsive sein, und somit auf beliebigen auch mobilen Geräten genutzt werden. Dies ist für viele Funktionalitäten eines KIS bedeutsam, da Versorgung oft in mobilen Kontexten erfolgt und eine zeitnahe Dokumentation am Point-of-Care im Grunde nur mit Mobilgeräten möglich ist. Auch die Einbindung von nativen Apps wird dadurch einfach. CMS-Module sollten containerisiert werden.

Fallbeispiel Medikationsmanagement

Ein Medikationsmanagement ist zentraler Teil jedes medizinischen Informationssystems und der Medikationsplan als persistierter Ausdruck der patientenspezifischen Ist-Situation im Sinne einer Aggregation der aktuellen Medikationen ist nicht nur im lokalen System von Relevanz, sondern als Bundesmedikationsplan auch übergreifend. Die Funktionalität zur Dokumentation von Medikationen kann in verschiedensten Subsystemen eines KIS heute vorkommen bzw. notwendig werden.

Je nach klinischem Setting ist dabei die alleinige Dokumentation der Verordnung ausreichend (so zum Beispiel im ambulanten Bereich), oder aber es muss sowohl die Ausgabe/Stellung von Medikamenten oder sogar die Verabreichung/Einnahme dokumentiert werden. Darüber hinaus gibt es gegebenenfalls die Anforderung, bei allen Verordnungen eine AMTS- Prüfung durchzuführen. Auch ist denkbar, dass die Verblisterung von Medikamentensets auf Basis einer

Aggregation von Anordnungen erfolgen soll. Damit können im Grunde die folgenden Anwendungsfälle mit einem definierten gemeinsamen oder eigenen „Bounded Context" angeben werden:

- Medikationsplan einsehen
- Medikation/Medikament anordnen
- Medikationsanordnung prüfen (AMTS-Prüfung)
- Medikament(e) für Patienten bestellen
- Medikamente zusammenstellen und ggf. Verblisterung durchführen
- Medikament(e) ausgeben
- Medikament(e) einnehmen
- Unverträglichkeit dokumentieren
- Medikationsabsetzung dokumentieren
- Medikationswiederaufnahme dokumentieren

Diese Anwendungsfälle spiegeln auch in gewisser Weise den Objektlebenszyklus einer einzelnen Medikation wider, denn im Verlauf des Behandlungsprozesses ist die Abwicklung einzelner Medikationen ein eigenständiger paralleler Subprozess.

Bezüglich der vorangehenden Fragen ergibt sich für die Medikationsdokumentation folgendes Bild:

Tabelle 4-3: Eignungsbewertung Medikationsmanagement für CMSM (Kriterienmatrix)

Kriterium	Ja	Nein	Anmerkung
Betriebliche Subdomäne?	X		Medikationsverordnungen und alle damit zusammenhängenden Arbeiten sind gut abgrenzbar und im Sinne des
Vielfache betriebliche Nutzung?	X		Im Krankenhaus werden in vielen Abteilungen Medikationen verordnet und Medikamente verabreicht. Natürlich erfolgt die hauptsächlich im Rahmen der fachärztlichen Behandlung auf Station, aber bei vielen diagnostischen oder therapeutischen Maßnahmen wird auch eine (punktuelle) Begleitmedikation notwendig.
Kontextüberschneidung klein?	X		Mit Blick auf den gesamten klinischen Kontext eines Patienten und alle Daten im KIS kann die Kontextüberschneidung als relativ gering angesehen werden.
Ubiquitär?	X		Medikation sollte immer und überall möglich sein.
Weiter Untergliederung?	X		Wie vorangehend beschrieben besteht der ganze Vorgang aus vielen z.T. auch optionalen Schritten/Aktivitäten die zum Teil auch vom Patienten durchgeführt werden können (z.B. Einnahme und Dokumentation dieser).

Damit wird deutlich, dass das Medikationsmanagement gut geeignet ist, als CMSM realisiert und betrieben zu werden.

Nun stellt sich die weitere Frage der Granularität für CMSM für ein Medikationsmanagement-Modul: Soll das gesamte Medikationsmanagement als ein „monolithisches" Cloud-Modul angesehen werden oder ist eine weitere Modularisierung orientiert an den vorgenannten Anwendungsfällen sinnvoll? Bei genauerer Betrachtung zeigt sich, dass fast alle o.a. Anwendungsfälle auch im klinischen Alltag weitgehend isoliert bearbeitet werden. Lediglich eine Übersicht zur aktuellen Medikation wird in fast allen Kontexten notwendig. Es kann jedoch auch diskutiert werden, ob dies überall der Fall ist, denn um ein Medikament auszugeben oder einzunehmen/zu verabreichen oder einen Satz von angeforderten Medikamenten zu verblistern, bedarf es nicht unbedingt des Wissens über alle aktuellen Medikationen, zumal AMTS-Prüfungen vor einer Ausgabe bzw. Verblisterung geschehen sein müssen. In diesem Sinne könnte ein Medikationsmanagement-Modul auch in weitere CMSM zerlegt werden.

Die Aspekte sollen am Medikationsmanagement in Anlehnung an den Bundesmedikationsplan (auf Basis der aktuellen Anlage 3 zur Vereinbarung gemäß § 31a Abs. 4 Satz 1 SGB V über Inhalt, Struktur und Vorgaben zur Erstellung und Aktualisierung eines Medikationsplans sowie über ein Verfahren zur Fortschreibung dieser Vereinbarung, publiziert durch die KBV[351]) aufgezeigt werden.

Tabelle 4-4: Anwendungsfälle Medikationsmanagement und Bounded Context (vereinfacht)

Medikationsliste	Patienten-ID, alle Angaben zum Medikament, Dosierschema, Grund, Start, Bis
Verordnen	Patienten-ID, alle Angaben
Einnehmen	Patienten-ID, Med-ID, Medikamentenname, Datum, Uhrzeit, Menge
Absetzen	Patienten-ID, Med-ID, Medikamentenname, Datum, Uhrzeit
Ausgeben	Patienten-ID, Med-ID, Medikamentenname, Datum, Uhrzeit, Menge
Wiederaufnehmen	Patienten-ID, Med-ID, Medikamentenname, Datum, Uhrzeit
Unverträglichkeit dokumentieren	Patienten-ID, Med-ID, Medikamentenname, Datum, Uhrzeit, Unverträglichkeit

Wie deutlich wird, braucht ein Medikationsmanagementmodul bzw. ggf. die einzelnen granularen CMSM im Wesentlichen folgenden Kontext aus dem KIS: Den Patientenbezug, einige klinische Parameter, ggf. ein Set aktueller Laborwerte. Letztere bilden sich im Modell aus dem BMP aber nicht allgemein und generisch ab. Ebenso muss auf einen möglichst standardisierten Medikamentenkatalog – also ein entsprechendes Bezugsobjektrepository – zugegriffen werden können. Die spezifizierte Semantik zu einzelnen Attributen kann gekapselt werden, bei Vorhandensein eines lokalen oder globalen Terminologieservers aber auch regelmäßig mit diesem synchronisiert werden. Damit ergibt sich das nachfolgend gezeigte Bild für mögliche Microservicemodule des Medikationsmanagements.

[351] Kassenärztliche Bundesvereinigung, Spezifikation für einen bundeseinheitlichen Medikationsplan (BMP) gemäß § 31a SGB V. 2019. S. 47 ff und 76 ff.

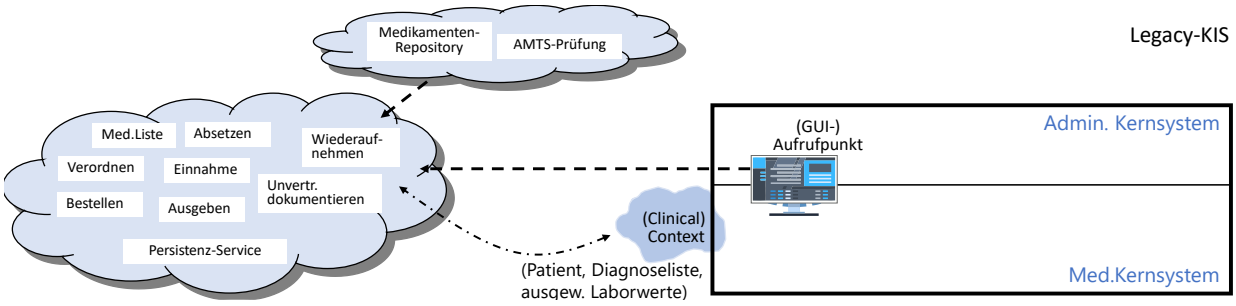

Abbildung 4-11: *Medikationsmanagement als Cloud Microservice Modul-Bundle und Legacy-System*

Für das Design, die Implementierung und die Interoperabilität der CMSM untereinander aber auch mit anderen CMSM und mit dem Repository können dabei die FHIR-Services aus dem „Medications Modul“[352] genutzt werden:

- *Medication* und *Medication Knowledge* für Zugriff auf Medikamentenstammdaten und Zusatzinformationen zu Medikamenten.
- *Medication Request* für die Verordnung
- *MedicationDispense* für die Ausgabe
- *Medication Statement* für die konkrete Medikation
- *MedicationAdministration* für die Verabreichung bzw. Einnahme

Analog kann das vorangehend dargestellte Vorgehen und der Lösungsansatz auch für viele andere klinischen Dokumentationsaspekte gelten, im Grunde für alle z.B. im HL7 EHR-System Functional Model angegeben Funktionalitäten oder für die im vorangehend gezeigten Schichtenmodell in den einzelnen Modulen enthaltenen Funktionalitäten.

Fallbeispiel kontextsensitiver Wissensabruf

„Wissen ist heute in wissensintensiven Branchen ein kritischer Erfolgsfaktor. Dies gilt einmal mehr für die Medizin. Die Geschwindigkeit der Generierung neuen Wissens und dessen Menge sind enorm – das gilt für alle medizinischen Fachrichtungen und v. a. auch für die Onkologie. Dieser Wissenszuwachs jährlich übersteigt inzwischen das individuell vom einzelnen Arzt oder anderen Gesundheitsberufen anles- und umsetzbare Wissen.“[353]

Die Entscheidungsunterstützung in der Medizin hat viele Facetten, die schon bei einer Wissensvermittlung beginnen, ohne das Algorithmen schon direkt Patientendaten bewerten und Entscheidungen vorschlagen.

Ein kontextsensitiver Wissensabruf direkt aus Funktionen des KIS heraus kann daher zu mehr Qualität der Versorgung und zeitgleich gleitender Weiterbildung der Ärzte führen. Eine webbasierte Cloud-Anwendung kann hier isoliert als Proxy zu beliebigen Wissensbasen dienen und so direkt aus dem klinischen Kontext heraus dem Benutzer Wissen vermitteln.

[352] Siehe https://www.hl7.org/fhir/medications-module.html.

[353] Haas: Wissensmanagement in der Medizin. 2016.

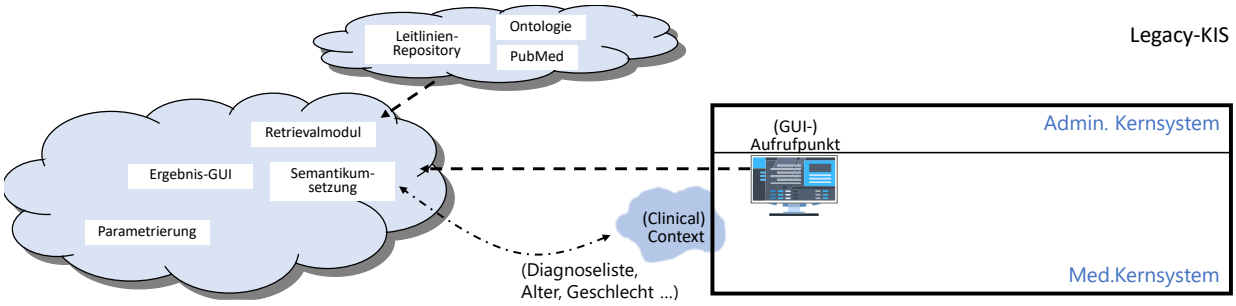

Abbildung 4-12: Kontextsensitives Wissensretrieval

Dabei kann die Kontextübermittlung, da hier anonymisierte Daten reichen, direkt mit dem Aufruf des Wissensmoduls erfolgen. In einer Implementierung mit einem Legacy-KIS[354] konnte gezeigt werden, dass ein solcher modularer Ansatz als Add On gut realisierbar ist.

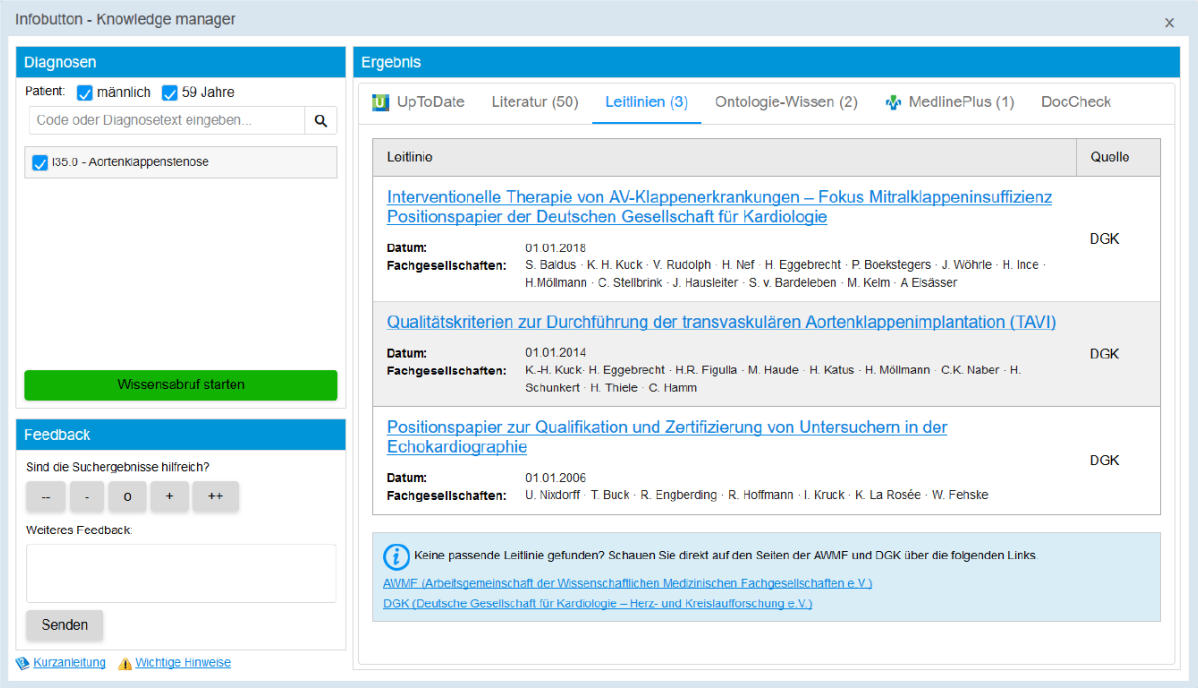

Abbildung 4-13: Beispielbildschirm Ergebnis Wissensrecherche

4.4.5 Kandidaten und Vorgehen

Für eine „Cloudisierung" von KIS bzw. KIS-Funktionalitäten eigenen sich zwar alle Anwendungssysteme und Module in gleicher Weise, sind aber nicht von gleicher strategischer Relevanz, wenn es darum geht, eine sukzessive Umsetzung vorzunehmen. Wie bereits vorangehend in den formulierten Kernfragen/Kriterien ausgeführt, sind vor allem Systeme/Module, die nur einer losen Kopplung mit den Kernsystemen bzw. anderen Systemen bedürfen sowie Systeme/Module die vielfach verwendbar bzw. notwendig sind, geeignete Kandidaten für die ersten Migrationsschritte. Bei entsprechender Verfügbarkeit offener Schnittstellen bzw. Services in den Legacy-Systemen kann so Markt und Wettbewerb für solche Module stimuliert werden.

[354] Mützner, Anforderungen und Lösungsansätze für wissensbasierte kontextsensitiv-reaktive medizinische Informationssysteme. 2020.

Dabei wird deutlich, dass heute viele mit dem Kernsystem „verbackene" Module und Funktionalitäten eigentlich auch nur lose gekoppelt und modular eigenständig entwickelt und betrieben werden können.

Mit Blick auf die Tabelle 4-1 und die Kriterien aus Tabelle 4-2 sind die folgend gelisteten Funktionalitäten für eine Implementierung als CMSM in einem ersten Schritt sehr geeignet:

- Medikationsmanagement mit allen granularen Funktionalitäten
- Patientenportal mit allen granularen Funktionalitäten
- Diagnosedokumentation (granular aus Liste und CRUD-Funktionen)
- Symptomdokumentation (granular aus Liste und CRUD-Funktionen)
- Terminmanagement mit allen granularen Funktionalitäten
- Alle isoliert nutzbaren klinischen (Spezial)Dokumentationsfunktionen wie z.B.
    - Wunddokumentation mit allen granularen Funktionalitäten
    - OP-Dokumentation mit allen granularen Funktionalitäten
    - Anästhesie-Dokumentation mit allen granularen Funktionalitäten
    - Spezialisierte Maßnahmendokumentationen wie Anamnese und Zwischenanamnese, Körperliche (Eingangs)Untersuchung, Visiten-Dokumentation, Ergebnisdokumentation zu diagnostischen Maßnahmen, Dokumentation von Therapiesitzungen und Therapiemaßnahmen
- Pflegedokumentation mit allen isoliert nutzbaren medizinischen (Spezial)Dokumentationsfunktionen wie z.B.
    - Pflegeanamnese
    - Pflegeplanung
    - Pflege-Leistungserfassung
    - Pflegekurve
- Notaufnahmemanagement inkl. Triage
- Einweisungs- und Entlassmanagement
- Entscheidungsunterstützende Zusatzfunktionalitäten wie z.B. kontextsensitive Wissensrecherche, AMTS-Checks, Wissensabruf, Hypothesengenerierung, Warnhinweise, Erinnerungsfunktionen
- Verwaltung von Systemstemmdaten die den Kontext des KIS abbilden wie z.B.
    - Krankenhaus-Organisationsstruktur Aufbauorganisation
    - Mitarbeiterverwaltung und Benutzerverwaltung
    - Berechtigungsmanagement
    - medizinische Ordnungssysteme
    - Wertebereiche für vielfältig genutzte Attribute (Attribut-Vokabulare, „Domains")
    - Medikamente
    - Materialien

Hinzu kommen eine Reihe von spezialisierten technisch unterstützenden Services z.B. für die Benutzeridentifikation und den Single Sign On, die Policy Administration und -durchsetzung, Kontext-Übermittlung bzw. Event- und Message-/Service-Bus, Eventsynchronisation usw.

4.4.6 Die besondere Rolle von Repositories

In Enterprise Informationssystemen und den enthaltenen Subsystemen wird die Nutzung von Daten notwendig, die eigentlich von vielen Anwendungssystemen in gleicher Weise benötigt werden[355]. Hierbei handelt es sich zum Großteil um sogenannte „Stammdaten" bzw. Bezugsobjekte, auf die die Anwendungssysteme der Unternehmen in Ihrer Verarbeitung Bezug nehmen, deren Verwaltung aber nicht Kern der Business-Funktionalität des Systems ist. Bezüglich der digitalen Sammlung solcher Bezugsobjekte spricht dann auch von **Repositories**, die in vielen Branchen heute als Webservices – oft gegen entsprechende Nutzungsgebühren – verfügbar sind. Zu diesen „Stammdaten" gehören z.B. im Gesundheitswesen Daten über Organisationen (Kostenträger, Krankenhäuser, Sozialdienste, Beratungsstellen u.v.a.m.), über Materialien und Produkte (Arzneimittel, Heil und Hilfsmittel, Materialien, Blutprodukte u.v.a.m.), über bestimmte semantische Bezugssysteme und Kataloge (Gebührenordnung, DRGs, ICD, OPS, SNOMED u.v.a.m.) oder über medizinisches Wissen (Klinische Pfade, Leitlinien, AMTS-Informationen, Ontologien). Solche Daten werden heute redundant in vielen lokalen Systemen oftmals manuell gepflegt und fortgeschrieben – sogar redundant innerhalb der Anwendungssysteme eines heterogenen KIS. Oftmals ist die Integrität dieser quasi lokalen isolierten Repositories untereinander zweifelhaft. Solche Daten als DaaS verfügbar zu machen und nur durch eine zuständige Organisation oder eine zuständige Community pflegen zu lassen, hat erhebliche positive qualitative und ökonomische Effekte.

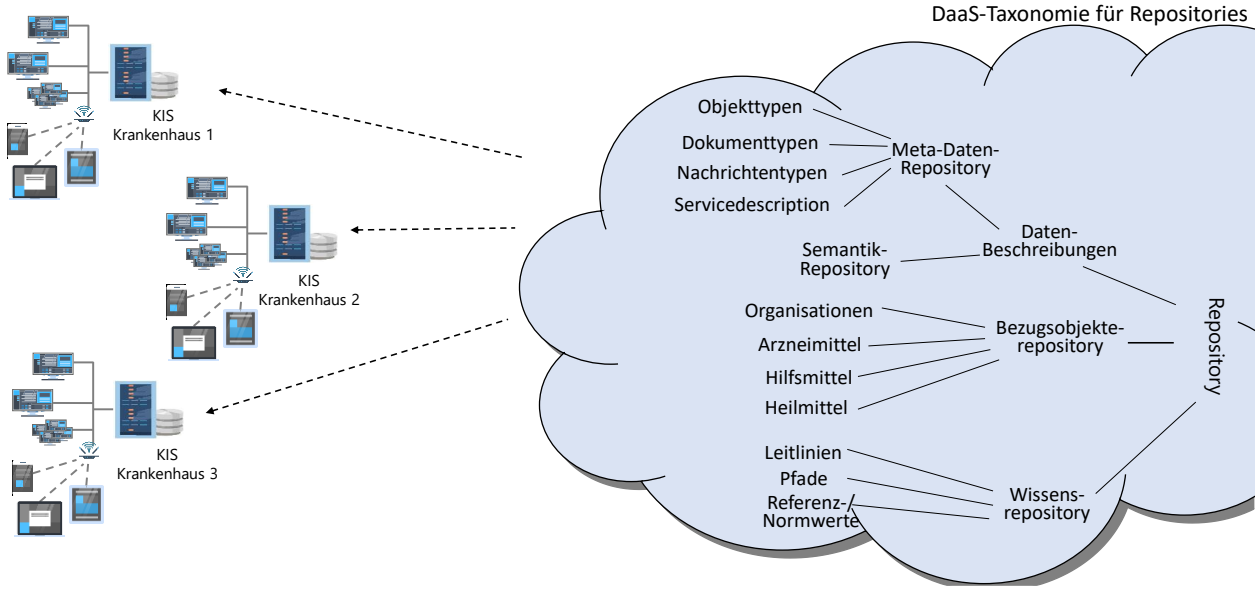

Abbildung 4-14*: Repositories und Anwendungssysteme in Anlehnung an Haas*[356]

Cloud-Implementierungen für KIS sollten also nicht ohne entsprechende Implementierung oder Verfügbarkeit entsprechender Repositories erfolgen.

[355] Haas, Informatische Artefakte für eine Gesundheitstelematikplattform, in Goetz/Grode (Hg.) Thesenpapier zur Gesundheitstelematik, 2013, S. 78–84.

[356] Haas, Repositories als unabdingbare Infrastrukturelemente für telematische und telemedizinische Anwendungsszenarien, in Haas et al: Nutzung, Nutzer, Nutzen von Telematik in der Gesundheitsversorgung – eine Standortbestimmung, 2013, S. 78–84.

Prinzipiell steckt in der Pflege der entsprechenden Daten über eine Community – z.B. mittels entsprechender Module in einer Community-Cloud – erhebliches wirtschaftliches Potenzial, da die aufwändigen und in jedem Krankenhaus immer in gleicher Weise durchzuführenden Arbeiten minimiert werden.

4.4.7 Contextmanagement und -handling

Ein wesentlicher Aspekt für die Ermöglichung des Einsatzes von CMSM ist das Context-Sharing zwischen dem Legacy-System bzw. den Kernsystemen und den Cloud-Modulen bzw. den Cloud-Modulen untereinander.

Erstaunlicherweise hat sich bereits um das Jahr 2000 eine HL7-Arbeitgruppe mit der Idee beschäftigt, zur Laufzeit Context zwischen Systemen bzw. Modulen auszutauschen – die Clinical Context Object Workgroup[357] – die 2010 in die Infrastructure and Messaging Work Group integriert wurde. Die Idee hier war ähnlich den nun aktuell diskutierten für CMSM: Heterogene Anwendungen tauschen Kontext aus, sodass der Benutzer sich bruchlos über diese verschiedenen Anwendungen „hinwegbewegen" kann, indem er z.B. seinen Bearbeitungskontext bzw. Teile davon bei Systemwechsel „mitnimmt". Die Idee kam aber zu früh, da viele proprietäre Systeme nicht in der Lage waren einen solchen Ansatz zu unterstützen; auch die Technologie war noch nicht soweit. Zur Motivation und zum Hintergrund der Entwicklung wurde ausgeführt:

„CCOW was developed largely at Duke University to address the problem of using sixty different systems. In a short time, the committee has developed and ratified five versions of the CCOW Standard. This unprecedented pace has been, in part, due to the modular component-based nature of the architecture upon which the standard is based, enabling new specifications to be developed in a complementary and add-on manner. CCOW's Context Management Architecture (CMA) was founded on the principle that common context can be established across applications by identifying things, such as the current patient context, or clinical encounter context in a manner that different applications can nevertheless recognize. The core architecture is comprised of three main types of components: the set of active applications; a context manager that coordinates and synchronizes applications; and mapping agents that can represent the various synonymous real-world identifiers used to identify clinical patients, users, etc. …".

"Clinical context is state information that a user establishes and modifies while interacting with healthcare applications at the point-of-use (e.g., a clinical desktop). The context is common because it establishes parameters that should uniformly affect the behavior or operation of multiple healthcare applications. The context needs to be managed so that the user has a way of controlling it, and so that applications have a way of robustly coordinating their behavior as the context changes. Examples of clinical context include but are not limited to: The identity of a patient whose data the user wants to view or update via the applications; the identity of the user who wants to access the applications; a moment in time around which temporal data

[357] Siehe http://www.hl7.org/implement/standards/product_brief.cfm?product_id=1, hier ist auch der Dokumentensatz zur Version 1.6 herunterladbar.

displays should be centered by the applications; a particular patient encounter that the user wants to review via the applications."[358]

Kontext wird in CCOW als Wissen zu Attributausprägungen bestimmter im Kontext relevanter Informationsobjekte betrachtet, so z.B. bestimmte Informationen über den aktuellen User, den Patienten, den Behandlungsbesuch, die Untersuchung bzw. Maßnahme, Anzeige Objekte, DICOM-Bilder u.v.a.m.[359] Heute können dafür die betreffenden FHIR-Ressourcen genutzt werden. Im CCOW werden folgende Kontext-Objekttypen besonders hervorgehoben:

- Angaben zum Benutzer und ggf. seinen Rechten
- Angaben zum Patienten inkl. ggf. verschieden benutzte IDs
- Angaben zum Patientenkontakt (Encounter Identity Objekt), ggf. Auflösen mittels Hierarchie Fall -> Episode -> Patientenbesuch -> Patientenkontakt
- Angaben zur klinischen Anordnung bzw. dem Auftrag
- DICOM Study Identity Object
- Ansichts-/Listenobjekt (View Object)
- Spezielles Business Objekt (Custom Identity Object)

Dabei werden je Objekttyp nur minimale Daten übergeben bzw. in den Kontext aufgenommen. Im Grunde reichen bei einer Microservice-Architektur zum Teil schon die eindeutigen Objekt-IDs der entsprechenden Objekte um im Gesamtzusammenhang – analog zu den Referenzen bei FHIR – die Bezüge herzustellen. So brauchen z.B. viele Funktionen den konkreten Patienten mit seinen demographischen Angaben gar nicht zu kennen, es reicht, wenn die eindeutige ID den Datensätzen des Moduls zugeordnet wird. Im Grunde ist das auch bei regelhaften relationalen Datenbankentwürfen bereits so, denn Tabellen zur Dokumentation spezifischer klinischer Aspekte enthalten ebenfalls lediglich als Fremdschlüssel die Patienten-ID, um den Bezug herzustellen.

Bei prozessorientierten klinischen Systemen sollte auf jeden Fall noch die klinische Maßnahme bzw. das klinische Phänomen im Kontext enthalten sein, falls der mit der Anwendungsfunktion verbundene Arbeitsschritt im Kontext eines klinischen Phänomens (Maßnahme, Diagnose, Symptom etc.) erfolgt.

Die Idee und Konzeption von CCOW ist verblüffend nahe an den Ansätzen des Domain Driven Design und der Implementierung mit MicroService-Modulen und ihrem Bounded Context. Im Rahmen der CCOW-Spezifikation ist ein Satz von fünf Dokumenten entstanden, unter anderem eine Architekturbeschreibung und mehrere Umsetzungsbeschreibungen für bestimmte technische Bindings, so auch für Web/http für Cloud-fähige Systeme.

Auch IHE behandelt – wenngleich in kleinerem Maße als CCOW – die Problematik des klinischen Kontextes, was im Profil „Patient Synchronized Applications"[360] sich niedergeschlagen hat. Das Profil setzt auf Arbeiten des CCOW auf.

---

[358] Seliger et al, HL7 Context Management Specification Version 1.6 Technology – and Subject-Independent Component Architecture Version 1.6. 2016. S. 13.

[359] Seliger et al, HL7 Context Management Specification Version 1.6 Technology – and Subject-Independent Component Architecture Version 1.6. 2016, S. 17 ff.

[360] Siehe https://wiki.ihe.net/index.php/Patient_Synchronized_Applications.

Mit Blick auf Abbildung 4-9 kann also bezogen auf die aktive Arbeit eines Benutzers immer angegeben werden, in welchem Kontext sich dieser gerade „informationstechnisch" befindet, und da in einem KIS es auch immer um bestimmte zumeist patienten- und fallbezogene Datenretrieval- oder Datenerfassungsfunktionen geht, ist gut definierbar, was der generelle überlappender Kotext zwischen CMSM und Legacy-System bzw. Core-Domäne ist. Und was dann der Bounded Context eines Moduls ist (siehe auch Beispiele in Kapitel 4.3.4).

4.4.8 Resultierende Anforderungen

Die vorangehenden Anwendungsbeispiele zeigen, dass für neue Funktionalitäten oder den Ausbau von bisher wenig ausgeprägten Funktionalitäten eine Cloud- und SaaS-fähige Modularisierung und die Implementierung von Cloud-MicroService-Modulen für Krankenhausinformationssysteme als Erweiterung der Legacy-Systeme schon heute in weitreichendem Maße realisierbar ist. Dabei ist es unerheblich, ob die Implementierung durch den Legacy-Hersteller im Rahmen der Weiterentwicklung oder einer Migrationsstrategie erfolgt oder aber durch unabhängige andere Softwarehersteller. Wichtig wäre nur, dass zur Unterstützung des Innovationsprozesses hin zu klinischen Cloud-Funktionalitäten die Legacy-Systeme entsprechende Aufrufschnittstellen anbieten.

„Microservices erlauben es, die Legacy-Systeme um Funktionalitäten zu erweitern, ohne dabei den Code anzupassen. Ein Aufruf, der eigentlich für ein Legacy-System bestimmt ist, kann von einem Microservice abgefangen und verarbeitet werden. Der Microservice kann die Anfrage bearbeiten oder an das Legacy-System weitergeben. So können Funktionalitäten des Legacy-Systems ersetzt oder ergänzt werden, ohne dabei den Code des Legacy-Systems anzupassen. Solche Anpassungen sind bei Legacy-Systemen oft schwierig. Daher sind Microservices für die Weiterentwicklung von Legacy-Systemen oft ein nützliches Werkzeug."[361]

Migration und Weiterentwicklung und Innovationen in Richtung Cloud-KIS können jedoch nur stattfinden, wenn eine geeignete semantische Interoperabilität zwischen den Legacy-Systemen und den CMSM ermöglicht und realisiert wird. Dies setzt eine gewisse Standardisierung von Schnittstellen bzw. Services auf beiden Seiten voraus. Eine solche Standardisierung hat in den letzten 30 Jahren weltweit in der Health-IT kontinuierlich stattgefunden und brachte im letzten Innovationszyklus das Konzept von FHIR (Fast Healthcare Interoperability)[362] hervor – vermutlich die Interoperabilitätsbasis für die nächste Dekade im Gesundheitswesen. Da es sich um einen kontinuierlichen Entwicklungs- und Standardisierungsprozess gehandelt hat und auch FHIR in Teilen auf dem RIM von HL7 aufsetzt, existiert eine weitgehende Kongruenz zwischen den bisher allseitig genutzten HL7-Nachrichten und FHIR-Ressourcen und damit Mapping-Möglichkeiten, die auch gut die Möglichkeit der Mitnutzung bzw. Migration vorhandener Interoperabilitätsmechanismen ermöglichen.

[361] Wolff, Microservices – Agilität durch Modularisierung. 2016. Blogbeitrag unter https://www.innoq.com/de/articles/2016/04/microservices-agilitaet/.

[362] Siehe http://www.hl7.org/fhir/.

Anforderungen an die Legacy-Systeme/Hersteller:

- Öffnung der Systeme durch Ergänzung um FHIR-Services zum Abruf und ggf. der Rückübergabe wesentlicher (Kontext)Daten an/von Cloud-Subsysteme und -Anwendungsmodule, damit Ermöglichung der Integration innovativer Funktionsmodule von Drittanbietern.
- Implementierung von GUI-Elementen zum Aufruf von Cloud-Anwendungsmodulen an geeigneten Stellen bzw. eine generische parametrierbare Aufruf-Bildschirmseite/Menüleiste
- Zurverfügungstellung oder Ankopplung eines (Clinical)Contextmanagers und eines Event-Bus für System-Offenheit und moderne Interoperabilität
- Konkrete Kontextlieferungen bzw. FHIR-Services für von vielen Cloud-Modulen benötigten Kontextdaten wie Patient, Fall, Auftrag, Diagnosen usw.[363]
- Öffnung und Interoperabilität in dem Sinne, dass Repository-Inhalte und Semantik auch aus DaaS-Instanzen bezogen/genutzt werden können.
- Anbindung von in der Cloud verfügbaren Basisdiensten wie z.B. Single Sign On, Policy- und Rechtemanagement, Kryptographiedienste, Pseudonymisierungsdienste, Zeitsynchronisationsdienste

Anforderungen an die CMSM:

- Berücksichtigung der internationalen Standards für Domänenmodell, Semantik und Interoperabilitäts-API, vor allem von HL7, IHE und SNOMED, aber auch andere Semantikstandards
- Offengelegtes Interoperabilitäts-API
- Hohe Aufgabenangemessenheit der GUI
- Durchgehend Web-basiert und Web-nutzbar
- Responsives Verhalten
- Bezug von standardisierter Semantik und Bezugsobjekten wo möglich aus verfügbaren Cloud-Repositories (DaaS-Instanzen)
- Nutzung von Open Source Werkzeugen, Bibliotheken und Komponenten für die Implementierung

Anforderungen an die Krankenhäuser

- Bei Ausschreibungen und Neubeschaffungen sollte neben der Offenheit auf Basis von HL7-Nachrichten auch eine Offenheit gefordert werden, die servicebasierte Interoperabilität, wo möglich auf Basis von FHIR, einfordert. Ebenso Aufrufpunkte – ggf. parametrierbar durch das Krankenhaus – zum Aufruf von Cloud-Modulen; auch von Drittanbietern.

Anforderungen an die Politik

- Mitaufnahme des Kriteriums Offenheit bzw. offene Service-Schnittstellen und Aufrufpunkte in Förderkriterien von Förderprogrammen.

[363] Eine erste Beschreibung der in Frage kommenden Objekttypen findet sich bei Seliger et al, HL7 Context Management Specification Version 1.6 Subject Data Definitions Version 1.6. 2016. S. 17 ff.

- Schaffung von Rahmenbedingungen für den diskriminierungsfreien Marktzugang von Spezialanbietern und Ausgründungen etc.
- Analog dem IOP-Portal bzw. dem DIGA-Verzeichnis sollte ein nationales Produktverzeichnis zu CMSM für KIS aufgebaut werden, ggf. - auch durch die zuständige Selbstverwaltungsorganisation DKG, die dafür entsprechend auszustatten ist.
- Ggf. Regelungen für die Zulassung von medizinischen Cloud-Modulen analog zu dem DIGA-Verfahren. Denkbar auch Delegation an Selbstverwaltungsorgane, ähnlich wie dies im ambulanten Bereich der Fall ist.
- Förderung der Realisierung und des Betriebs von Cloud-Repositories gemäß Abbildung 4-14 für die lokale oder Community-bezogene oder globale Nutzung

Des Weiteren gibt es vielfältige spezielle technische Aspekte und Anforderungen, die im Folgenden weiter betrachtet werden.

Hinsichtlich der technischen Anforderungen an den sicheren performanten und hochverfügbaren Betrieb von Cloud-KIS gibt es keine Unterschiede zu anderen Branchen, die bereits erfolgreich Cloud-Lösungen im Einsatz haben.

4.4.9 Konsequenzen und Fazit

Cloud-KIS können – die Extrema betrachtet – *grobgranular* oder *feingranular* sein. **Mit Blick auf die gegebene Ausgangssituation dürfte in naher Zukunft kein wirkliches für SaaS geeignetes Cloud-KIS gesamtheitlich verfügbar werden.** Strategisch gesehen – aus Sicht der Krankenhäuser, der Gesundheitspolitik, der Wirtschaftspolitik und auch der vermutlich der Hersteller – ist aber die Einleitung eines Migrationsprozesses wünschenswert, der vor allem in einem ersten Schritt Legacy-Systeme öffnet und ertüchtigt, in geeigneter Weise Cloud-Microservice-Module (CMSM) über offene bzw. offengelegte Services so anzubinden, dass sich Benutzer bei ihrer fachlichen Arbeit bruchlos über die Systemgrenzen hinweg bewegen und Funktionalitäten des Legacy-Systems und von CMSM integriert nutzen können. Dies würde auch die Entwicklung/Entstehung von branchenspezifischen bzw. regionalen Ökosystemen in Form von Community-Clouds befördern.

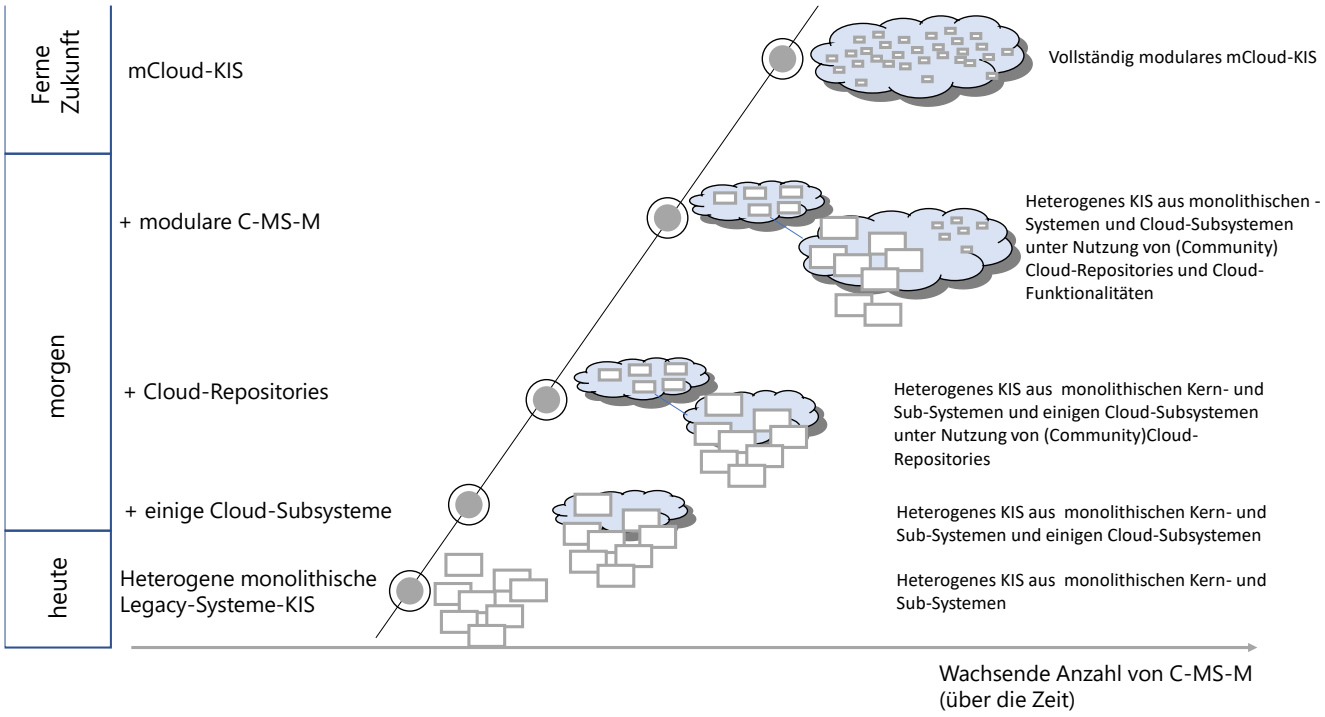

Abbildung 4-15*: Entwicklungsperspektiven hin zum Cloud-nativen KIS*

Für eine nachhaltige und wettbewerbsfördernde und ressourcenschonende Weiterentwicklung der Anwendungslandschaften für Krankenhausinformationssysteme erscheinen folgende Aspekte als besonders wichtig:

- mCloud-KIS werden nicht oder nur in geringem Maße disruptiv entstehen, sondern als Ergebnis eines langjährigen Migrations- und Transformationsprozesses.
- mCloud-KIS sind eine Chance für mehr Innovation und Wettbewerb und ermöglichen auch jungen Unternehmen und SpinOffs mit spezialisiertem KnowHow, innovative fachlich fokussierte Lösungen zu entwickeln und einfach in ein größeres Ganzes zu integrieren.
- mCloud-KIS ermöglichen den Krankenhäusern je nach Art und Größe und Digitalisierungs-Strategie genau jene Lösung einzusetzen, die sie gerade benötigen und ermöglichen ihnen auch, am allgemeinen Fortschritt zu partizipieren.
- Softwarehersteller von KIS sollten bei Neuentwicklungen oder Zusatzentwicklungen von abgrenzbaren Funktionalitäten auf eine cloudfähige Microservice-Modularisierung und Implementierung achten.
- Neuentwicklungen finanziert durch öffentliche Fördergelder sollten für Projekte und KIS-Ergänzungen als Kriterium zur Förderung eine Implementierung auf Basis einer cloudfähigen Microservice-Modularisierung einfordern
- Krankenhäuser sollten bei Ausschreibungen und Neubeschaffungen von KIS auf zukunftsfähige Strategien des Herstellers und nachhaltige Technologie-Architekturen des Produktes achten.
- Bei allen Implementierungen sind vorhandenen internationalen Standards zu prüfen und so weitgehend wie möglich einzusetzen. Dies schließt auch die neue Spezifikation spezieller Profile mit ein.

4.5 Cloud-spezifische Anforderungskataloge, Standards und Zertifizierungen

Im Jahr 2016 legte das Bundesministerium für Wirtschaft und Energie im Rahmen des Kompetenznetzwerkes „Trusted Cloud"[364] eine erste Ausarbeitung zu Cloud-Standards vor.[365] Im Vorspann heißt es u.a.:
„Obwohl cloud Computing im Allgemeinen als etwas Neues wahrgenommen wird, stellt es aus technischer Sicht nicht grundsätzlich Neues dar.

Neu ist, dass beispielsweise Software, Datenspeicher oder auch Rechenkapazität statt wie bisher im Eigenbetrieb und statisch, nunmehr über ein Netzwerk und dynamisch an den Bedarf der Nutzer angepasst als Dienste zur Verfügung gestellt werden.

Neu ist auch das Ausmaß, in dem die Bereitstellung dieser Dienste erfolgt. Sie zielen nicht mehr auf die Bereitstellung möglichst individualisierte Lösung ab, sondern auf die massentaugliche Standardisierung der Angebote."

Vor diesem Hintergrund sind in den vergangenen 10 Jahren eine fast unüberschaubare Anzahl von cloud-relevanten und cloud-spezifischen Standards entstanden, die sowohl technische, vertragliche, ökonomische und betriebsbezogene Aspekte betreffen. Aus technischer Sicht sind hier vor allem Standards zu Datei-, Daten- und Austauschformaten relevant, dann Standards für Webservices und Serviceschnittstellen, Standards zu speziellen Protokollen und Schnittstellen, Programmier- und Architekturmodelle sowie Standards zu Benchmarking und Tests. Aber auch Standards für das Identifikations- und Rechtemanagement sowie die Sicherheitsmechanismen in Cloud-Anwendungen sind wichtig und heute verfüg- und anwendbar.

Die Einhaltung von bestimmten Standards sowie vor allem die sachgerechte Implementierung von Datenschutz- und Sicherheitsmechanismen kann heute im Consumer-Bereich durch die Endkunden/Nutzer, aber auch im Bereich von kleinen bis mittelgroßen Geschäftskunden/Anwendern von Cloud-Lösungen nicht mehr selbst überprüft und nachvollzogen werden, dazu fehlt die Personalkapazität und die Expertise. Dies gilt auch für die Krankenhäuser. Vor diesem gibt es ebenfalls seit einigen Jahren Bemühungen um Zertifizierungen bzw. Zertifikate von Cloud-Angeboten, die vor allem auch darauf abzielen, die Informationssicherheit zu prüfen und zu zertifizieren. Zertifikate werden entlang der Zertifikatsanforderungen orientierten Audits durch Dritte an Produkte bzw. Cloud-Angebote vergeben. Bekannte Zertifikate sind z.B. das Gütesiegel SaaS von EuroCloud, CSA STAR, TÜV Trust IT.[366] Zudem kann auch das BSI-Grundschutz-Zertifikat herangezogen werden, das um cloud-spezifische Aspekte erweitert wurde bzw. der C5[367]-Kriterienkatalog „Cloud Computing" des BSI[368], der mit der neuen Version vor allem die Sicherheit der Cloud-Dienste selbst fokussiert, und nicht nur auf die Erbringung von Service-Leistungen. Auch wurden einige Anforderungen zur Produktsicherheit aus dem EU Cybersecurity Act abgeleitet, aber auch viele weitere internationale Prüfschemata, Richtlinien und

[364] https://trusted-cloud.de/de.

[365] BMWi, Cloud-Standards und Zertifizierungen im Überblick – Was Cloud-spezifisch betrachtet werden sollte. Version 1.0. 2016.

[366] Quelle: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/CloudZertifizierung (unter Cloud Computing > Cloud Zertifizierung).

[367] C5 = Cloud Computing Compliance Controls Catalogue.

[368] Bundesamt für Sicherheit in der Informationstechnik, Kriterienkatalog Cloud Computing C5, 2020.

Best Practices berücksichtigt. In einer eigenen Kreuztabelle sind Teile dieser anderen Standards/Zertifikate den C5-Kriterien zugeordnet. Auch werden Hinweise zum Umgang mit Ermittlungsanfragen staatlicher Stellen integriert. Neben den Rahmenbedingungen und der Beschreibung entsprechender Angaben und Parametern werden sodann Basiskriterien, Zusatzkriterien und ergänzende Informationen definiert. Die Europäische Agentur für Cybersicherheit (enisa – EUROPEAN UNION AGENCY FOR CYBERSECURITY[369]) publiziert auf ihrer Website eine Liste von 13 Zertifizierungs-Schemata und der zugehörigen Zertifikate und Organisationen.

Mit dem aktualisierten BSI-C5-Anforderungskatalog steht ein unter Beteiligung der einschlägigen Community entwickelter Katalog zur Verfügung, der auch für Cloud-KIS-Prüfungen herangezogen werden kann. Im Katalog werden 121 Titel unterteilt in die folgend dargestellten Bereiche spezifiziert, unterhalb jeden Titels finden sich weitere einzelne Kriterien:

Tabelle 4-5: Anforderungsbereiche des C5-Kataloges des BSI

Bereich	Anzahl Titel
Organisation der Informationssicherheit (IOS)	7
Sicherheitsrichtlinien und Arbeitsanweisungen (SP)	3
Anforderungen an das Personal (HR)	6
Asset Management (AM)	6
Physische Sicherheit (PS)	7
Maßnahmen für den Regelbetrieb (OPS)	24
Identitäts- und Berechtigungsmanagement (IDM)	9
Kryptographie und Schlüsselmanagement (CRY)	8
Kommunikationssicherheit (COS)	8
Portabilität und Interoperabilität (PI)	3
Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV)	10
Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO)	5
Security Incident Management (SIM)	5
Sicherstellung des Geschäftsbetriebes und Notfallmanagement (BCM)	4
Compliance (COM)	4
Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ)	4
Produktsicherheit (PSS)	12

Die Kriterien – in diesem Sinne auch Anforderungen an Cloud-Lösungen – sind auf allgemeinem Niveau angegeben und bei Auditierungen muss dann geprüft werden, mit welchen konkreten technischen und/oder organisatorischen Maßnahmen diese erfüllt werden.

Neben den üblichen Kriterien für den Betrieb von sicheren Rechenzentren – deren Erfüllung per se für Cloud-Anbieter vorausgesetzt werden muss – müssen also für Cloud-Anwendungen noch weitere Aspekte Berücksichtigung finden.

Cloud-KIS sollten mit Blick auf die fokussierten nationalen Arbeiten des BSI ein entsprechendes Audit durchlaufen und nach dem C5-Katalog zertifiziert sein. Darüber hinaus sollten dann für

[369] Siehe unter https://resilience.enisa.europa.eu/cloud-computing-certification

die Laufzeitumgebungen die Provider z.B. gemäß BSI-Grundschutz und ISO/IEC 27001 zertifiziert sein.

Da die Grundidee von SaaS perspektivisch modulare Softwarelandschaften sind, können und müssen jedoch auch einige Kriterien auf Subsysteme und CMSM heruntergebrochen werden, sodass eine Betrachtung von im Sinne der Zertifizierung vorhandener Leistungsmerkmale nicht nur Gesamtsysteme betrachtet werden sollten, sondern auch modular eine Zertifizierung von Subsystemen und Modulen möglich sein sollte bzw. erfolgen muss.

Anforderungen an Cloud-KIS und Betreiber:

- Zumindest Erfüllung der im C5-Kriterienkatalog des BSI enthaltenen Kriterien.

4.6 Verfügbarkeit, Performance und Skalierbarkeit

4.6.1 Verfügbarkeit

Hinsichtlich Verfügbarkeit kann zwischen der örtlichen und der zeitlichen Verfügbarkeit eines Informationssystems unterschieden werden. Während die örtliche Verfügbarkeit eine Nutzbarkeit in allen betrieblichen Situationen und an allen für die Nutzung notwendigen Orte bedeutet, ist die Zeitliche Verfügbarkeit ein Maß, zu wieviel Prozent der potentiellen Nutzungszeit eine Lösung auch für die Nutzung verfügbar ist.

Die **örtliche Verfügbarkeit** ist in Krankenhäusern zunehmend ein wichtiger Aspekt, denn Informationsabruf und Dateneingabe sollte am Point of Care möglich sein. So sollten z.B. am Krankenbett erhobene Messwerte, Visitennotizen u.v.a.m. direkt erfassbar sein, ohne auf Papier zwischennotiert werden zu müssen. Eine hohe örtliche Verfügbarkeit ist mit nur fest installierten Endgeräten in bestimmten Räumen nur schwerlich zu bewerkstelligen bzw. es müsste faktisch in jedem Raum, in dem medizinische Maßnahmen stattfinden – aber auch in anderen Räumen – ein Endgerät installiert sein. Örtliche Verfügbarkeit kann in Ergänzung zu festinstallierten Endgeräten durch mobile Geräte jeglicher Art gut erreicht werden. Dazu müssen die entsprechenden Softwareanwendungen aber responsiv sein – sich also die Oberfläche an die Art und Größe des Bildschirmes automatisch anpassen, was z.B. bei responsiven Websites der Fall ist. Cloud-KIS-Anwendungen bzw. -module müssen daher responsive sein. Daneben – was aber keine speziellen Anforderungen von Cloud-KIS ist – muss natürlich eine vollständige Netzabdeckung im Krankenhaus gegeben sein.

In einem dienstleistungsintensiven Unternehmen, das Leistungen rund um die Uhr erbringen muss und oft eine zeitnahe Reaktionsnotwendigkeit (z.B. Notfälle, Rückfragen) besteht- was alles auf Krankenhäuser zutrifft – muss die **zeitliche Verfügbarkeit** sehr groß sein. Ausfälle bzw. Stillstand wegen Sicherung, Wartung, Update sollten faktisch nicht vorkommen bzw. maximal minimiert werden. Selbst bei einer Verfügbarkeit von 99 % bedeutet dies pro Jahr immerhin eine Ausfallzeit von 87,6 Stunden, bei 99,9 % sind es noch rund 9 Stunden! Die durch die zeitliche Nichtverfügbarkeit nicht erfolgten Datenerfassungen müssen nachgeholt werden, da ein Elektronische Patientenakte nicht unvollständig belassen werden darf. Bei der Menge von Daten, die pro Stunde in einem Krankenhaus anfallen, ist aber eine manuelle Nacherfassung faktisch unmöglich bzw. mit sehr hohem Aufwand und Kosten verbunden. Auch kommt hinzu, dass wichtige Daten bis alles nacherfasst ist nicht im wieder laufenden System zur Verfügung stehen, was eventuell zu Behandlungsfehlern führen kann.

Für KIS muss heute eine Verfügbarkeit von nahe 100 % gefordert werden. Typischerweise bedeutet heute Hochverfügbarkeit „five 9s" oder höher, also 99,999 % also im Mittel 5 Minuten Downtime pro Jahr, was für ein KIS als akzeptabler Wert angesehen werden kann, gegebenenfalls sind auch „four 9s" akzeptabel. Während eine fast 100-prozentige Verfügbarkeit früher nicht als realisierbar galt, kann diese heute durch die Kombination verschiedener Hardware- und Softwaremechanismen erreicht werden und performante Hochverfügbarkeitsinfrastrukturen sind in vielen Branchen und für viele Geschäftsmodelle unabdingbar geworden. Eine Nichtverfügbarkeit z.B. von Verkaufsplattformen und elektronischen Marktplätzen für einige Stunden kann bei manchen Anbietern schon zu einem Umsatzverlust in Millionen-Höhe führen. Im Krankenhaus geht es aber weniger um wirtschaftlichen Schaden, sondern dass bei einem Ausfall des IT-Systems die Versorgung von kranken Menschen und Notfällen nicht mehr vollumfänglich gewährleistet werden kann. Gerade in den vergangenen Jahren hat sich gezeigt, was für ein Schaden – hier zumeist durch Cyberattacken – ein Ausfall von KIS zum Teil für über mehrere Tage hinweg verursachen kann. Ein Hochverfügbarkeit des KIS ist daher eine conditio sine qua non, was dann für alle Komponenten des Technologiestacks (Netze und Netzkomponenten, Server, Storage Infrastructure, Middleware) gilt. Awendungshochverfügbarkeit und „Business continuity"[370] setzen also die Fehler-Umgehung bzw. Selbstheilung von IT-Infrastrukturen voraus. Heute wird durch vielerlei Maßnahmen der Rechenzentren – bis hin zur Spiegelung ganzer Betriebsumgebungen und Georedundanz – eine Verfügbarkeit erreicht, die nicht durch lokal betriebene KIS in entsprechender Weise oder mit verhältnismäßigem Aufwand garantiert werden kann.

Ein möglicher Single Point of Failure kann die Netzwerkverbindung zwischen dem internen Krankenhausnetz und der Cloud-Infrastruktur sein. Hier sind multiple Redundanzen vorzusehen, die auch im Regelbetrieb parallel und durch Load-Balancing optimal genutzt werden können, was den Durchsatz erhöht. Dabei muss darauf geachtet werden, dass die Netzanbindungen über unterschiedliche Infrastrukturen laufen.

Für Cloud-Anwendungslandschaften werden in der Regel trotz dem Ziel der weitegehenden Kapselung und Unabhängigkeit der einzelnen fachlogischen Anwendungssysteme/-module zentrale für alle diese zu nutzende Querschnittsanwendungen notwendig, wie z.B. der Event-Bus oder Policy Decision und Enforcement Points, die einen Single Point of Failure (SPOF) darstellen. Daher sollten diese doppelt oder sogar dreifach ausgelegt sein und die diese Dienste konsumierenden Anwendungen oder ebenfalls mehrfach ausgelegte „Proxies" die gerade verfügbare Instanz des SPOF-Dienstes dynamisch auswählen. Der Einsatz von z.B. Kubernets kann dies z.B. sicherzustellen.

„Durch ein erfolgreich etabliertes Business Continuity Management (BCM) ist es Unternehmen möglich, besser mit den unternehmensrelevanten Bedrohungen und deren Auswirkungen auf die betriebliche Wertschöpfung umzugehen. Die Vorbereitung auf eine Störung erfolgt prä-

[370] Business Continuity ist die Fähigkeit, Geschäftsprozesse ohne Unterbrechung fortführen zu können.

ventiv durch gezielt auf das Unternehmen entwickelte Kontinuitätsstrategien, aus denen operative Notfallpläne abgeleitet werden."[371] Dienstleister und ein Cloud-KIS nutzendes Krankenhaus müssen in diesem Sinne gemeinsam ein BCM etablieren. Für das BCM hat die ISO 2019 die internationale Norm 22301 herausgegeben[372].

4.6.2 Performance und Skalierbarkeit

Ein wesentlicher Aspekt von Cloud-Lösungen bei Betrieb in Dienstleistungsrechenzentren ist die beliebige Skalierbarkeit und Lastbalancierung bei sich ändernden Lasten vor dem Hintergrund garantierter Antwortzeiten. Für ein gegebenes Krankenhaus ist das dynamische Lastverhalten bzw. wachsende Last im längeren Zeitverlauf weniger ein wichtiger Aspekt, da sich die Last bei gegebener Anwendungslandschaft in einem Krankenhaus in der Regel nicht ändert bzw. die Lastprofile über den Tag verteilt ebenfalls nicht zufällig sind, sondern vorausschaubar kalkulierbar. Lediglich wenn neue Anwendungen hinzukommen, sind Anpassungen notwendig. Hier kann ein Vorteil von Cloud-KIS vor allem darin liegen, dass bei nutzungsbezogenem Entgelt Investitionsgüter nicht brachliegen – wie das z.B. bei lokalen Systemen in Form der lokalen Serverinfrastruktur zwischen 18 Uhr und 7 Uhr in der Regel der Fall ist, sondern eben nur nutzungsadäquate Kosten anfallen. Hier könnten sich durch Cloud-KIS Kostenvoreile ergeben.

Perfomance hat viele Facetten – sei es der Rechenleistung, der Datenzugriffe, der Bandbreite zwischen Komponenten und zwischen Server und Endgeräten usw., aber am Ende kulminieren alle diese Aspekte in der Antwortzeit für den Benutzer. Das sogenannte „Nutzererlebnis" ist heute in vielen Branchen für eine Akzeptanz einer Softwarelösung entscheidend, und dieses Erlebnis wird nicht nur durch eine aufgabenangemessene Funktionalität und Benutzeroberfläche beeinflusst, sondern auch maßgeblich durch das **Antwortzeitverhalten**. In der Krankenversorgung im Krankenhaus ist Zeit ein entscheidender Faktor – umso mehr vor dem Hintergrund des aktuellen Personalmangels. **Daher ist zu fordern, dass Cloud-KIS ein Antwortzeitverhalten in Form von „Echtzeit" gewährleisten.** Gegenüber lokalen Infrastrukturen kann die Skalierung hierzu in Cloud-Umgebungen weitaus besser und flexibler gestaltet werden, aber am Ende ist die Netzlaufzeit der Bottleneck. Breitbandige Anbindung ist notwendig aber heute auch Stand der Technik. Ein weiterer Ansatz bei Webanwendungen ist, diese z.B. auf Basis des Konzeptes der Single Pages (SPA) zu realisieren, dadurch sinkt die Transferlast zwischen Server und Browser-Client erheblich, da nur noch Nutzdaten und sich ändernde Angaben in der Oberfläche zwischen Server und Client-Browser ausgetauscht werden. Lediglich beim lokalen Start einer Anwendung kommt es zu einem größeren Übertragungs-Volumen, wobei dieses durch dynamisches Nachladen von Anwendungsteilen ebenfalls minimiert werden kann. Die Technologieentwicklung in diesem Bereich ist derzeit noch im Fluss, so arbeiten große Hersteller an WebAssembly, mittels dem eine weitere und erhebliche Optimierung von Lade- und Ausführungszeiten erreicht werden soll. Es kann davon ausgegangen werden, dass in naher Zukunft auch diese Ressourcendiskussion obsolet werden wird, wie das in vielen Bereichen angefangen bei Speichervolumen bis zu Rechenleistung in der Vergangenheit der Fall war.

[371] Meyer/Hein, Franziska: Business Continuty Management. 2016. S. 1.

[372] International Standards Organization, Security and resilience - Business continuity management systems - Requirements (ISO 22301:2019).

4.6.3 Datenverfügbarkeit

Wie bereits vorangehend angemerkt, ist eine hochverfügbare Softwareanwendung ohne entsprechende Datenverfügbarkeit in der Regel wertlos. Datenverfügbarkeit gibt an, inwieweit Daten auch unter besonderen Umständen also z.B. bei Fehlerfällen verfügbar bleiben. Diese Verfügbarkeit bezieht sich auf die Verfügbarkeit für das Onlinesystem.

Im klinischen Kontext ist die Verfügbarkeit vorhandener Informationen ein entscheidender Faktor. Klinische Entscheidungen basieren auf guten und vollständigen Informationen. Dies zuallererst bezüglich der Informationen über den Patienten, seine Historie und den aktuellen Istzustand bezüglicher der Diagnosen, aller Befunde, der Medikation usw., aber auch was ggf. in naher Zukunft an Maßnahmen geplant ist. Also in Summe muss ein KIS jederzeit für einen Patienten Auskunft geben können über: Was war, was ist und was wird/soll sein? Aber auch Informationen über Produkte (v.a. Medikamente) und organisatorischem Kontext sind wichtig. **Krankenhäuser sind daher daten- bzw. informationsgetriebene Unternehmen. Insofern ist einen Anwendungshochverfügbarkeit ohne entsprechende Datenverfügbarkeit wertlos.**

Bei zunehmender Digitalisierung bis hin zum „papierlosen Krankenhaus" wird auch eine leistungsfähige Speicherinfrastruktur zum kritischen Erfolgsfaktor. Vor diesem Hintergrund müssen Cloud-KIS auch eine nahe 100-prozentige Datenverfügbarkeit gewährleisten und es dürfen auch keinerlei Datenverluste („data loss") auftreten.

Damit sind sowohl Recovery Time Objective (RTO) als auch Recovery Point Objective (RPO) wichtige und kritische Größen für ein KIS – also die Parameter, wieviel Datenverlust maximal vorkommen kann und wie lange ein System ausfällt. Zu entsprechenden Metriken wird auf einen Beitrag im Online-Magazin „Informatik aktuell" verwiesen[373].

Den Zusammenhang für die Kontinuität der Prozesse und betrieblichen Vorfallabwicklung zeigt nachfolgende Abbildung[374], wobei man bei einem KIS von einer „Mission Cricital"-Anwendung ausgehen kann:

[373] Held, Hochverfügbarkeit und Downtime: Metriken. 2015. unter https://www.informatik-aktuell.de/betrieb/verfuegbarkeit/hochverfuegbarkeit-und-downtime-metriken.html

[374] Gravic inc., Choosing a Business Continuity Solution to Match Your Business Availability Requirements. White Paper. 2020.

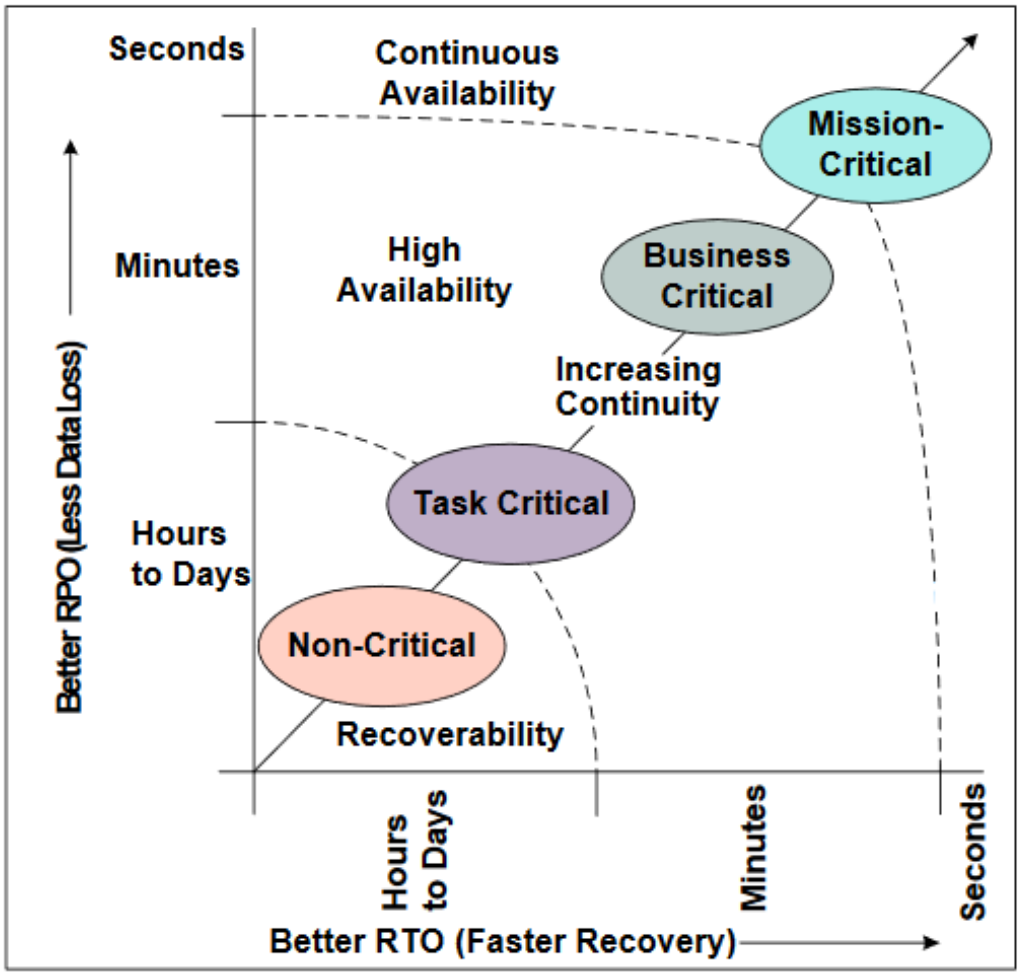

Figure 2 – The Business Continuity Continuum

Abbildung 4-16: Business Continuity und RTO und RPO[375]

Im Rahmen des BCM sind für die entsprechenden Parameter in den Verarbeitungsverträgen zugesicherte Werte zu vereinbaren.

4.6.4 Zusammenfassung und Maßnahmen

Zusammenfassend kann festgestellt werden, dass für Cloud-KIS – aber auch für lokale Legacy-Systeme – folgende besonders hervorzuhebenden Anforderungen bestehen:

- Sicherstellung der „Business Continuity“ durch geeignete Maßnahmen
- Etablierung eines Business Continuity Managements
- Hochverfügbarkeit der Anwendungen (99,99 % oder mehr)
- Unverzögerte Antwortzeiten für die Benutzer bei Dialogaufgaben
- Kleine RPO und RTO
- Hohe örtliche Verfügbarkeit, responsive Anwendungen für Nutzung auch auf mobilen Geräten beliebigen Typs

[375] Abdruck mit freundlicher Genehmigung der Gravic inc. vom 25.11.2020

Neben den üblichen Maßnahmen, die heute standardmäßig durch kommerzielle Cloud-Anbieter bzw. Rechenzentren ergriffen werden, um Skalierbarkeit, Verfügbarkeit und Performance sicherzustellen, sind für ein Cloud-KIS insbesondere Folgende zu nennen:

- Datenreplikation
- Replikation/Spiegelung der gesamten Laufzeitumgebung(en), der Anwendungscontainer
- Schnelles Disaster Recovery (RPO und RTO gegen Null)
- Georedundanz für Daten- und Systemreplikation/-spiegelung
- Multi-redundante Netzwerkanbindungen

4.6.5 Technische Rahmenbedingungen

Wie bereits vorangehend dargestellt, bestehen an Cloud-KIS höchste Anforderungen bezüglich Performance und Verfügbarkeit. Der Betrieb bei Cloud-Dienstleistern kann dies gewährleisten. Kritische Infrastrukturkomponente bleibt die Anbindung von lokaler Infrastruktur an die Cloud-Infrastruktur. Dabei stellt die Bandbreite nicht unbedingt eine kritische Größe dar, denn bei Cloud-KIS und Nutzung von nachladenden Single-Page Anwendungen in geschickter Weise ist der Nutzdatenverkehr je Arbeitsplatz relativ gering. Umfangreiche Erfahrungen mit Anbindungen gibt es bereits durch die vielen Rechenzentrums-Betriebsmodelle. Daher ist vor allem auf die Verfügbarkeit der Verbindung zu achten, die durch Mehrfachredundanz sichergestellt werden muss.

4.7 Datenschutz- und Datensicherheitsmechanismen

4.7.1 Einführung und Überblick

In einem KIS werden vielfältige Datenkategorien verwaltet, viele davon die über die physische und psychische Verfassung und die Behandlung von Patienten Auskunft geben und die besonders schutzwürdig sind. Oftmals wird mit dem Begriff „Datenschutzmechanismen" nur ein entsprechendes Berechtigungsmanagement assoziiert, aber Datenschutz hat viele weitere Facetten, die in der nachfolgenden Abbildung zusammengefasst sind.

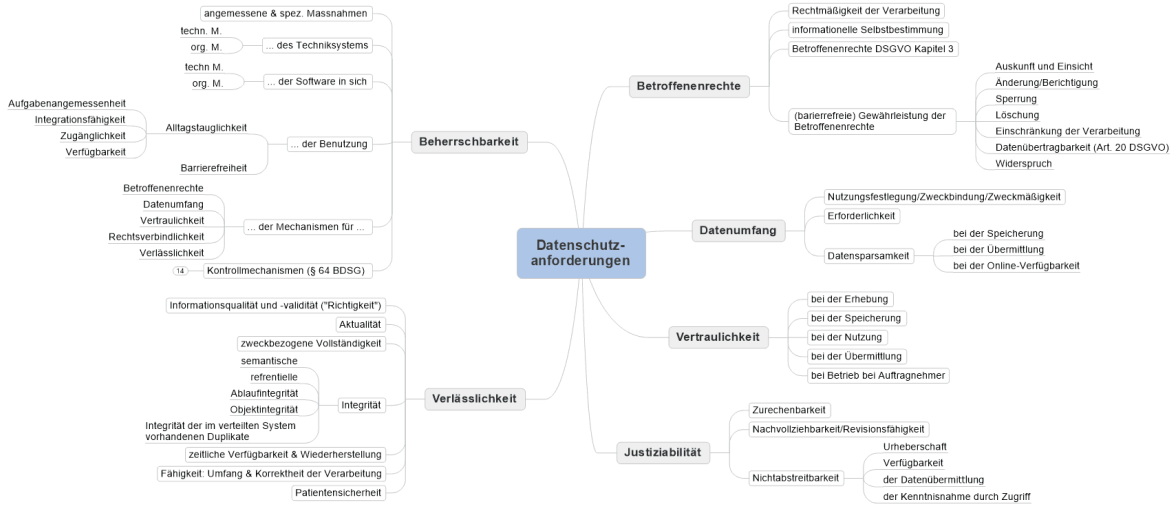

Abbildung 4-17*: Facetten des Datenschutzes*

Vor diesem Hintergrund haben die Arbeitskreise „Gesundheit und Soziales" und „Technik" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche seit 2008 an einer Orientierungshilfe Krankenhausinformationssysteme (OH-KIS) gearbeitet, die in der Version 1 im Jahr 2011 und sodann im Jahr 2014 in einer Version 2[376] herausgegeben wurde. Diese beschreibt in einem Teil I Rechtliche Rahmenbedingungen für den Einsatz von Krankenhausinformationssystemen in Form von 48 Anforderungen und Hinweisen zum Teil entlang eines krankenhausinternen Behandlungsprozesses und in einem Teil II Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen sowie einen Katalog von Szenarien zulässigen Datenaustauschs zwischen stationären und ambulanten Leistungserbringern. Im technischen Teil werden detaillierte Muss/Soll-Anforderungen unterteilt in den folgenden genannten acht Klassen angegeben. Dabei wird auch unterschieden, ob die Erfüllung der Anforderungen durch die Hersteller oder den Betreiber oder beide erfolgen muss. Eine solche Unterscheidung hilft auch, jene Anforderungen zu identifizieren, die durch ein Cloud-KIS inhärent erfüllt werden müssen.

Tabelle 4-6: Anforderungsklassen in der OH-KIS

Kap.	Titel	Anzahl Anforderungen
I	**Rechtliche Rahmenbedingungen für den Einsatz**	
	Aufnahme	5
	Behandlung	3
	Zugriffe durch Ärzte	7
	Zugriffe durch den pflegerischen Stationsdienst	3
	Zugriffe außerhalb der bettenführenden Fachabteilungen	3
	Einschränkung der Zugriffsrechte nach Abschluss des Behandlungsfalls	5
	Löschung	1
	Zugriffe für Abrechnung, Controlling, Qualitätssicherung und Ausbildung	4
	Verarbeitung durch verschiedene Leistungserbringer	6
	Technische Administration	3
	Besonders schutzwürdige Patientengruppen	2
	Zugriffsprotokollierung und Datenschutzkontrolle	3
	Auskunftsrechte des Patienten	3
II	**Technische Anforderungen**	
1	Struktur der Daten im PAS	16
2	Systemfunktionen	19
3	Anwendungsfunktionen	12
4	Rollen- und Berechtigungskonzept	18
5	Datenpräsentation	4
6	Systemzugang	5
7	Protokollierung / Auswertung von Protokolldaten	2
8	Technischer Betrieb, Administration	7

[376] Arbeitskreise „Gesundheit und Soziales" sowie „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe Krankenhausinformationssysteme. 2014. Das Originaldokument steht zum Download bei den Datenschutzaufsichtsbehörden des Bundes, der Länder und der Kirchen zur Verfügung

Die OH-KS kann als „Goldstandard" für datenschutzbezogene Anforderungen an KIS gesehen werden. Eine umfangreiche Kommentierung mit weiteren detaillierten Hinweisen wurde von der Fachgesellschaft GMDS ergänzend herausgegeben[377].

Die Anforderungen aus der OH-KIS können uneingeschränkt auf Cloud-KIS übertragen werden.

Hinzu kommt, dass Krankenhäuser prinzipiell – zumindest solche mit über 30.000 stationären Fällen pro Jahr – zur kritischen Infrastruktur gehören.[378] Vor allem die Fähigkeit zur Notfall- und Rettungsversorgung ist hier besonders bedeutsam, aber auch der Ausfall ganzer Krankenhäuser vor allem ab der Regelversorgungsstufe kann viele Menschen in einer Region gefährden. Bei einer Zielprojektion „Papierloses Krankenhaus" wird die IT-Infrastruktur mit allen Ihren Facetten zum Nervensystem eines Krankenhauses, d.h.: Ohne funktionierendes KIS keine regelhafte Krankenversorgung. Sowohl das Bundesamt für Sicherheit in der Informationstechnik als auch die Deutsche Krankenhausgesellschaft haben dementsprechende Leitfäden herausgegeben[379], in denen detaillierte Anforderungen und Handlungsempfehlungen für den Betrieb von Krankenhausinformationssystemen gegeben werden.

In den DKG-Empfehlungen werden im Kapitel 7 168 Maßnahmen zum Teil detailliert beschrieben, die dem Bereich Technisch-Organisatorische (TOM) Maßnahmen zugeordnet werden können. Es sind also auch Maßnahmen organisatorischer Art enthalten, so z.B. Maßnahmen zur Einrichtung und Aufrechterhaltung eines IT-Risikomanagements. Aber auch Maßnahmen die eher die Aspekte Patientensicherheit und Behandlungseffektivität betreffen werden angegeben. Die Maßnahmen zielen ebenfalls auf die im vorangehenden Kapitel erwähnte „Business Continuity" ab, als einen unterbrechungsfreien Betrieb der IT-Lösungen in einem Krankenhaus.

Tabelle 4-7: Übersicht Anforderungsklassen im B3S Medizinische Versorgung

Kapitel	Text	Anzahl Anforderungen
7	Anforderungen und Maßnahmenempfehlungen zur Umsetzung	
7.1	Informationssicherheitsmanagementsystem (ISMS)	
7.2	Organisation der Informationssicherheit	
7.2.1	Geschäftsführung / Leitung	7
7.2.2.	Beauftragter für Informationssicherheit (ISB, CISO)	14
7.2.3	Prozess- /Anwendungsverantwortlicher	6
7.3	Meldepflichten nach § 8b Absatz 4 BSI-Gesetz	3
7.4	Betriebliches Kontinuitätsmanagement	12
7.5	Asset Management	9
7.6	Robuste/resiliente Architektur	6
7.7	Physische Sicherheit	4
7.8	Personelle und organisatorische Sicherheit	10
7.9	Vorfallerkennung und Behandlung	6
7.10	Überprüfungen im laufenden Betrieb	8
7.11	Externe Informationsversorgung und Unterstützung	2
7.12	Lieferanten, Dienstleister und Dritte	5
7.13	Technische Informationssicherheit	

[377] GMDS e.V., Stellungnahme und Kommentierung der „Orientierungshilfe Krankenhausinformationssysteme". 2014.

[378] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 10 Jahre "KRITIS-Strategie". 2020. S. 14, 79,80

[379] Bundesamt für Sicherheit in der Informationstechnik, Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. 2013. / Deutsche Krankenhausgesellschaft: Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus. 2019.

Kapitel	Text	Anzahl Anforderungen
7.13.1	Netz- und Systemmanagement (Netztrennung und Segmentierung)	2
7.13.2	Absicherung Fernzugriffe	5
7.13.3	Härtung und sichere Basiskonfiguration der Systeme und Anwendungen	3
7.13.4	Schutz vor Schadsoftware	3
7.13.5	Intrusion Detection / Prevention	2
7.13.6	Identitäts- und Rechtemanagement	3
7.13.7	Sichere Authentisierung	2
7.13.8	Kryptographische Absicherung (data in rest, data in motion)	3
7.13.9	Mobile Sicherheit, Sicherheit Mobiler Zugang und Telearbeit (ggf. BYOD)	5
7.13.10	Vernetzung von Medizingeräten	2
7.13.11	Datensicherung, Datenwiederherstellung und Archivierung	3
7.13.12	Ordnungsgemäße Systemadministration	5
7.13.13	Patch- und Änderungsmanagement	3
7.13.14	Beschaffungsprozesse	5
7.13.15	Protokollierung	6
7.13.16	Umgang mit Datenträgern, Austausch von Datenträgern	5
7.13.17	Sicheres Löschen und Entsorgung von Datenträgern	8
7.13.18	Softwaretests und Freigaben	9
7.13.19	Datenschutz	1

Die aufgeführten Maßnahmen sollten analog auch beim Betrieb eines Cloud-KIS Anwendung finden. Dabei sind viele der angegebenen Maßnahmen nicht vom (Cloud-)Dienstleister umsetzbar, sondern fallen in den Verantwortungsbereich des Krankenhauses bzw. in gemeinsam im Rahmen der Auftragsdatenverarbeitung vereinbarten Vorgehensweisen

Im branchenspezifischen Sicherheitsstandard „Medizinische Versorgung" der DKG heißt es auch:

> „Die heterogene Systemlandschaft in den Krankenhäusern stellt eine der Herausforderungen in der Umsetzung eines Sicherheitsstandards im Krankenhaus dar, da eine durchgängige Standardisierung der eingesetzten Systeme nicht vorausgesetzt werden kann."

Für die Zukunft besteht gerade in feingranularen Cloud-KIS und deren Betrieb in Hochverfügbarkeits- und Hochsicherheitsinfrastrukturen professioneller Cloud-Dienstleister die Chance, eine neue Qualität der IT-Verfügbarkeit und -Sicherheit für Krankenhäuser zu erreichen. Aber auch systemweite „horizontale" Dienste – im Sinne der ISO/IEC-CCRA sogenannte Multi-Layer-Funktionen – z.B. für das User-, Authentifikations- und Berechtigungsmanagement können realisiert werden.

4.7.2 Authentifikations- und Berechtigungsmanagement

In einem Cloud-KIS, das – unabhängig ob es sich um ein grob- oder feingranulares Cloud-KIS oder um eine hybride Form handelt – eine verteilte Anwendungslandschaft bzw. ein verteiltes System darstellt, sollte im Gegensatz zu den Situationen der heterogenen Vor-Ort-Systeme, bei denen oftmals die Benutzer in jedem eigenständigen Subsystem neu angelegt, verwaltet und autorisiert werden müssen, ein **systemweites Identifikations-, Authentifikations- und**

Berechtigungsmanagement existieren. In der ISO 17789-CCRA ist dies als Multi-Layer-Funktion im Bereich Security verortet („Authentification and identity management")[380]. Anforderungen dazu finden sich sowohl in der OH-KIS in Form der Nummern 6-26 und 4.1 bis 4.18 als auch im B3S „Medizinische Versorgung" z.B. in 7.13.6 und 7.13.7.

Umfangreiche Anforderungen sind im IT-Grundschutz-Kompendium des BIS im Baustein ORP.4 zu finden.[381]

Eine Lösung besteht heute oftmals in der Nutzung eines Active Directories und Integration per LDAP, womit sich Benutzerkonten, Passwörter und Zusatzattribute synchronisieren lassen. Auch ein solcher Ansatz kann weiterhin für Cloud-Anwendungssystemlandschaften genutzt werden und Zwei-Faktor-Authentifizierung und Single Sign z.B. via SAML, OAuth oder Kerberos umgesetzt werden. Entsprechende Lösungen sind heute am Markt erhältlich.

Prinzipiell sollte es aber perspektivisch ein Cloud-KIS-weites Benutzerverzeichnis geben, dass als umfangreiches Repository angesehen werden kann und in dem auch für die Anwendungen nutzbare Informationen zum Benutzer abgelegt sind, die über die heute üblichen und mit LDAP verwalteten minimalen Daten für die Benutzeridentifikation und -authentifikation und das Rechtemanagement hinausgehen. Die Verwaltung der Benutzer muss einhergehen mit der Abbildung der gesamten Krankenhausaufbauorganisation, zumal die meisten Benutzer Mitarbeiter sind. So kann ein **Abteilungs- und Mitarbeiter-Repository** auch Grundlage für die Kompetenzverwaltung und auch das Retrieval von Expertise im Krankenhaus sein. Das Repository kann auch genutzt werden, um das Krankenhaus nach außen z.B. auf einer Website darzustellen, sodass auch hier keine doppelte Datenpflege der Krankenhausstruktur mehr notwendig wird. Das Modul kann gut isoliert werden und hat einen gut definierbaren Bounded Context. Eine Grundlage hierfür bietet das IHE HPD-Integrationsprofil[382].

[380] International Standards Organisation, ISO/IEC 17789 Information technology – Cloud computing – Reference architecture. 2014. S. 31, 34.

[381] Siehe https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html.

[382] IHE, Healthcare Provider Directory (HPD) - Rev. 1.8. 2020. https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_HPD.pdf.

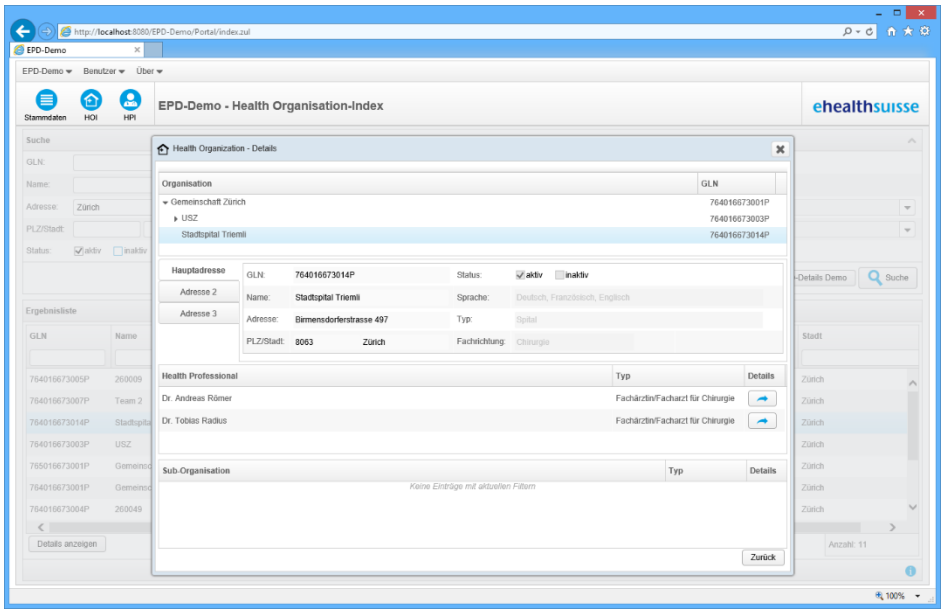

Abbildung 4-18: Beispiel Abteilungs-Mitarbeiterrepository auf Basis HPD[383]

Ein weiteres Modul im Cloud-KIS sollte das **Berechtigungsmanagement** kapseln. ANF-MN108 bis NAF-MN110 im branchenspezifischen Sicherheitsstandard „Medizinische Versorgung"[384] sind alles MUSS-Anforderungen und entsprechend in einem Cloud-KIS umzusetzen. Hier wird ein Rollen- und Rechtekonzept gefordert sowie eine Richtlinie für die Zugriffskontrolle, „die Zugriffsrechte und -beschränkungen auf Informationen und Funktionen im Informationsmanagementsystem und dessen Erteilung bzw. Entzug regelt". Dies schließt ein, dass Rechte auch nach Beendigung des Arbeitsverhältnisses zeitnah entzogen oder bei geänderter Rolle entsprechend geändert werden. Auch in der Orientierungshilfe KIS wird darauf in Kapitel 4 detailliert eingegangen. Dort wird auch ein attributbasiertes Berechtigungsmanagement gefordert.[385] Bei einem attribut-basierten Ansatz entscheidet ein Modul über die Nutzbarkeit-/Zugreifbarkeit durch einen Benutzer nicht nur anhand dessen Rolle und strukturellen Rechte wie etwas bei RBAC, sondern auch auf Basis bestimmter Attributausprägungen des Zugreifenden selbst und Attributausprägungen des Sicherheitsobjektes[386]. „ABAC unterscheidet sich von klassischen rollenbasierten Modellen (Rolle „Arzt" darf x und y, Rolle „Pflegepersonal" darf nur y) dadurch, dass sich sehr komplexe und beliebig granulare Zugriffsberechtigungen in relativ einfacher sowie natürlicher Art und Weise abbilden lassen. Hierzu spielen Attributausprägungen des Zugreifenden („Sicherheitssubjekt") und Attributausprägungen des Informationsobjektes, welches eingesehen, eingefügt, geändert oder gelöscht werden soll ("Sicherheitsob-

[383] Mützner/Haas, Health Provider Directory - eine standardkonforme Trial Implementierung. 2015.

[384] Deutsche Krankenhausgesellschaft, Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus. 2019. S. 74-78.

[385] Arbeitskreise „Gesundheit und Soziales" sowie „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe Krankenhausinformationssysteme. 2014. S. 10 ff.

[386] Bittner/Haas, Access granted: So lassen sich Zugriffs-Berechtigungen in Elektronischen Patientenakten flexibel und individuell regeln. 2014. Unter https://blog.der-digitale-patient.de/zugriffsberechtigungen-elektronische-patientenakten/.

jekt"), eine wichtige Rolle (Beispiel: „Jeder Radiologe darf nur Röntgenbefunde einsehen"). Dabei können auch implizite Attributentsprechungen benutzt werden (wie die Übereinstimmung von Fachgebiet des Arztes und Dokumenttyp, Beispiel: Fachgebiet = „Rad" für „Radiologe", Dokumenttyp = „Rad" für „Radiologischer Befund")."

Mit Blick auf DAC, MAC und RBAC die mehrheitlich aus einer Zeit geschlossener Einzelanwendungen stammen führen Dürbeck et al[387] aus: „Flexibler und dafür besser geeignet zeigen sich attributbasierte Zugriffskontrollrichtlinien (attribute-based access control, ABAC), in denen allgemeine Nutzerattribute zur Laufzeit ausgewertet, mit Objekt- und Umfeldbedingungen abgeglichen und dadurch die Zugriffskontrollentscheidung dynamisch (ereignisgesteuert und zur Laufzeit) gestaltet werden kann,"

Während Pflege der Rollen und Rechte und eine konsistente Definition und Durchsetzung von Policies in einer heterogenen Systemlandschaft bestehend aus isoliert entwickelten und inkompatiblen Subsystemen aufwändig und oft nicht in gleicher Weise umsetzbar ist, können Policy-Definitionen und deren Durchsetzung in einem Cloud-KIS durch ein entsprechendes Modul bzw. Module systemweit konsistent verwaltet, umgesetzt und eingesetzt werden. Alle fachlogischen CMSM müssen dementsprechend die Services der Berechtigungsinfrastruktur nutzen. In der ISO 17789-CCRA ist dies als „Multi-Layer-Funktion" im Bereich Security verortet („Authorization and service policy management")[388]. Ergänzend kann diese auf die Microservice-Repository-Einträge zugreifen, die im Grunde dann Sicherheitsobjekte darstellen, für die Rechte vergeben werden können.

Bei attributbasierten Lösungen müssen aber den Modulen die entscheiden sollen, was ein Benutzer darf, sehr viele evtl. auch vertrauliche Informationen mitgegeben werden, daher erscheint es geboten, die Zugriffsprüfung in eigene spezielle Module zu verlagern. Für verteilte Umgebungen wie ein Cloud-KIS kann eine verteilte Autorisierungsinfrastruktur bestehend aus Policy Decision Point (PDP), Policy Enforcement Point (PEP), Policy Administration Point (PAP), Policy Information Point (PIP) und Policy Retrieval Point (PRP) implementiert werden, bei der Kenntnisse über Attributausprägungen nur dort und nicht beim Diensteanbieter notwendig sind, um über Zugriffsrechte zu entscheiden (ebenfalls bei Dürbeck et al beschrieben).

Schon im Jahr 2000 wurde mit dem RFC 2748[389] ein einfaches Anfrage-/Antwort-Protokoll für entsprechende Interoperabilität zwischen Services (Common Open Policy Service (COPS)) spezifiziert, heute kann für eine ausdrucksstarke Interoperabilität die eXtensible Access Control Markup Language (XACML) gut genutzt werden. Alle o.a. Policy-Points können gut als eigenständige Module im Cloud-KIS betriebene werden, ein konkretes fachlogisches Modul kann dann einfach beim PEP anfragen, ob ein Benutzer in einem konkreten Kontext dieses benutzen darf und welche Zugriffsrestriktionen ggf. bestehen.

[387] Dürbeck et al, Eine verteilte Autorisierungsinfrastruktur unter Berücksichtigung von Datenschutzaspekten. Informatik_Spektrum_34_3_2011.S. 265 ff.

[388] International Standards Organisation, ISO/IEC 17789 Information technology – Cloud computing – Reference architecture. 2014. S. 31, 35.

[389] Siehe unter https://tools.ietf.org/html/rfc2748.

Insgesamt gibt es inzwischen umfangreiche methodische Arbeiten und Implementierungen für Cloud-Systeme, um ein differenziertes Policy-Management zu implementieren.

Anforderungen an mCloud-KIS:

- Cloud-KIS eigene Cloud Identity Authentication möglichst auf Basis des HPD-Profils
- Alternative An-/Einbindbarkeit anderer Identity Authentification Services
- Vollständige Abbildbarkeit der Aufbauorganisation des Krankenhauses (Organisationseinheiten und Personen)
- Unterstützung von Berechtigungsmechansimen auf Basis von RBAC und ABAC auf Basis differenzierter Rollenhierarchien.
- Auch regelbasierte Berechtigungsformulierungen
- Trennung von Berechtigungsprüfung und Fachmodulen durch eine gesonderte Autorisierungsinfrastur, möglichst als verteilte Micro-Services
- Prüfmethoden für die Prüfung der Integrität der parametrierten Berechtigungen
- Ermöglichung der Durchsetzung der Anforderungen aus der OH-KIS und dem B3S „Medizinische Versorgung" unter Berücksichtigung der entsprechenden Passagen aus dem Leitfaden zum Schutz Kritischer Infrastrukturen für Krankenhaus-IT des BSI

4.7.3 Vertraulichkeit gegenüber dem Provider

Bei allen Einsatzszenarien, bei denen ein Cloud-KIS nicht vor Ort betrieben wird, muss die Vertraulichkeit der beim Provider gespeicherten Patienten- und Behandlungsdaten durch vertragliche und/oder technische und organisatorische Maßnahmen sichergestellt werden. Die hohe Schutzwürdigkeit der Daten erfordert hier, dass alle Regelungen und Maßnahmen hierzu transparent zwischen Krankenhaus und Cloud-Betreiber festgelegt sind und regelmäßig überprüft werden. Es ist davon auszugehen, dass beliebig skalierende Verteilung von Daten auf beliebigen Servern weltweit in einer nicht definierten Infrastruktur für Cloud-KIS nicht akzeptabel ist.

Ein erster wichtiger Aspekt ist es hier, dass sowohl der Rechtsbereich, in dem die Infrastruktur liegt, geklärt ist als auch die Regeln für die dynamische Verteilung von Daten und Ressourcen und somit die Verschiebung vertraulicher Informationen auf andere Server als initial an- und abgelegt. Entgegen allgemeiner Gepflogenheiten beim Cloud-Computing, wo es in der Regel durch Anbieter keine Zusicherungen gibt, an welchem Ort und wie Daten gespeichert und ihre Vertraulichkeit sichergestellt wird, muss dies bei Cloud-KIS im Rahmen der Auftragsdatenverarbeitung differenziert vereinbart sein. Cloud-KIS sind auf jeden Fall nur in auditierten und zertifizierten Rechenzentren zu betreiben und es sind die heute üblichen am Stand der Technik orientierten technisch-organisatorische Maßnahmen umzusetzen.

Ein probates Mittel zur Sicherung der Vertraulichkeit gegenüber Dritten ist die verschlüsselte Speicherung der Bestandsdaten. Diese kann in einem ersten Ansatz durch Plattenverschlüsselung realisiert werden, was für manche Szenarien und Anwendungsfälle bereits ausreichend ist[390]. Eine solche Plattenverschlüsselung ist heute in Rechenzentren normalerweise verfügbar. Soll die Systemadministration vom Betreiber gesamtheitlich durchgeführt werden, muss der Schlüssel aber dem Betreiber bekannt gemacht werden, da er zu jedem Neustart des Systems eingegeben werden muss. Eine solche Verschlüsslung schützt also nicht vor Zugriffen z.B. durch

[390] Vgl. Bitkom, Verschlüsselung von Bestandsdaten aus Rechenzentrumssicht. 2009. S. 4.

Administratoren beim Provider, wobei die Anzahl der Personen auch dort begrenzt werden kann, z.B. auf zwei Personen oder ein sicheres organisatorisches Verfahren, wie ein Administrator den Schlüssel erhält. Auch ein Vier-Augen-Prinzip ist umsetzbar.

Eine Alternative ist, dass der Schlüssel durch das Krankenhaus selbst verwaltet wird, was aber mit Blick auf die Praktikabilität z.B. bei Neustart von Systemen wenig sinnvoll erscheint. Bei Microservice-basierten Systemen in Containern wird die Problematik verschärft, da im Grunde jeder Container einen gekapselten Rechner darstellt.

Mancherorts wird eine Ende-zu-Ende-Verschlüsselung für medizinische Datenverarbeitungsverfahren in der Cloud gefordert. Endpunkte wären hier der Persistenzspeicher beim Provider (z.B. die Datenbank) und der Browser auf dem Endgerät im Krankenhaus. Eine solche Lösung erscheint derzeit im Allgemeinen und auch speziell für Cloud-KIS aber wenig praktikabel, da auf den Daten zur Laufzeit in Multi-User-Umgebungen gearbeitet und selektiert werden muss und bei Cloud-/Webanwendungen eigentlich nur ein Browser auf dem Client vorausgesetzt wird. Zwar ist es inzwischen möglich, auch auf verschlüsselten Daten zu suchen und mit ihnen zu arbeiten[391], das setzt aber wiederrum eine Entschlüsselung auf dem Client voraus, was aber bei Webanwendungen, die ja auf dem Server laufen und nur auf dem Browser Seiten ausgeben, dann auch eine Entschlüsselung auf dem Server zu Laufzeit erfordert. Wenn also als Endpunkte der Datenspeicher und der Browser angesehen werden müssen, sind Technologien wie Sie heute für Verfahren bei client-Server-Systemen z.B. zur sicheren Dateiablage in der Cloud genutzt werden, ungeeignet. Zwar ist es heute schon möglich, auf verschlüsselten Daten zu suchen, aber eine funktionale Nutzung geht weit darüber hinaus. Forschungsarbeiten für solche Ansätze sind bereits publiziert, aber noch nicht routinefähig. Auch eine Schlüsselnutzung im Browser auf Basis von JAVA Script mit lokalen Schlüsseln erscheint problematisch, bieten sich doch hier auf dem Client dann weitere Angriffspunkte.

Auch Verfahren des Boxcrypting für die gekapselten Anwendungs- bzw. Microservicemodule und ihre Daten ist wenig praktikabel, denn diese müssten erst insgesamt heruntergeladen und dann lokal gespeichert, entschlüsselt und dann ausgeführt werden – mit allen dazugehörigen Daten. Und auch das Schlüsselmanagement erscheint hier je nach Ausprägung zu komplex und wenig praktikabel.

Gerade bei medizinischen Anwendungen lassen sich Patienten- und Falldaten gut gegenüber den medizinischen Daten abgrenzen, so brauchen Funktionalitäten und Datenspeicherungen zur Erfassung und Verarbeitung von Diagnosen, Symptomen, Laborwerten, Assessments u.v.a.m. im Grunde gar nicht zu wissen, um welche konkrete Person es sich handelt, können also zumindest pseudonymisiert betrieben werden. Generische Konzepte und Software hierzu wurden bisher für die medizinische Forschung genutzt und eingesetzt.[392] Diese lassen sich aber nicht 1:1 in Systeme für den Versorgungsalltag übernehmen, da bei Bearbeitung und zur Laufzeit immer der Patient bekannt und seine Angaben an der Benutzeroberfläche zugemischt werden müssen, also nicht nur eine punktuelle Zuordnung zum Entstehungszeitpunkt notwendig und erforderlich ist, wie das für die Forschungsdatenbestände der Fall ist.

[391] Antonopoulos, Azure SQL Database Always Encrypted. 2020.

[392] Reng et al, Generische Lösungen der TMF zum Datenschutz für die Forschungsnetze in der Medizin. 2006.

Ein möglicher Ansatz für Cloud-KIS könnte also in der Trennung von Daten und somit in der Implementierung der vollständigen physischen Trennung von Nutzdaten und Identifikationsdaten bestehen, also einem Secret Sharing in der Form, dass kein Provider alle Daten hat, um medizinische Sachverhalte zu einer Person in Erfahrung zu bringen. Dies ist prinzipiell umsetzbar, da jene CMSM, die medizinischen Daten verarbeiten und speichern, gar nicht den Patienten selbst kennen müssen, also quasi auf pseudonymisierter Basis arbeiten können. Eine entsprechende Pseudonymauflösung muss dann entweder zur Laufzeit in einem speziellen sehr vertrauenswürdigen Dienst erfolgen – wobei diesem dann sehr wohl der konkrete Patient bekannt ist, aber nicht die zugehörigen medizinischen Informationen – oder aber noch besser lokal vor Ort im Client im Rahmen der Anzeige und Verarbeitung von Daten, in dem die konkreten Patientendaten zugemischt werden. Im erstgenannten Fall wird wegen der notwendigen Zumischung der konkreten Patientenangaben in den Ausgabestrom eines Moduls zumindest jedoch im Hauptspeicher des Provider der das Modul bzw. den zugehörigen Container hostet diesem dann doch der konkrete Patient offengelegt. Der zweitgenannte Fall lässt sich derzeit nur schwerlich umsetzen. Gegebenenfalls können die Daten über zwei Browserverbindungen und permanenter paralleler Nutzung einer Pseudonymauflösungs-Anwendung optisch für den Benutzer zusammengebracht werden z.B. mittels eines iFrame, wobei dann sicherzustellen ist, dass die Patientenzuordnung korrekt ist.

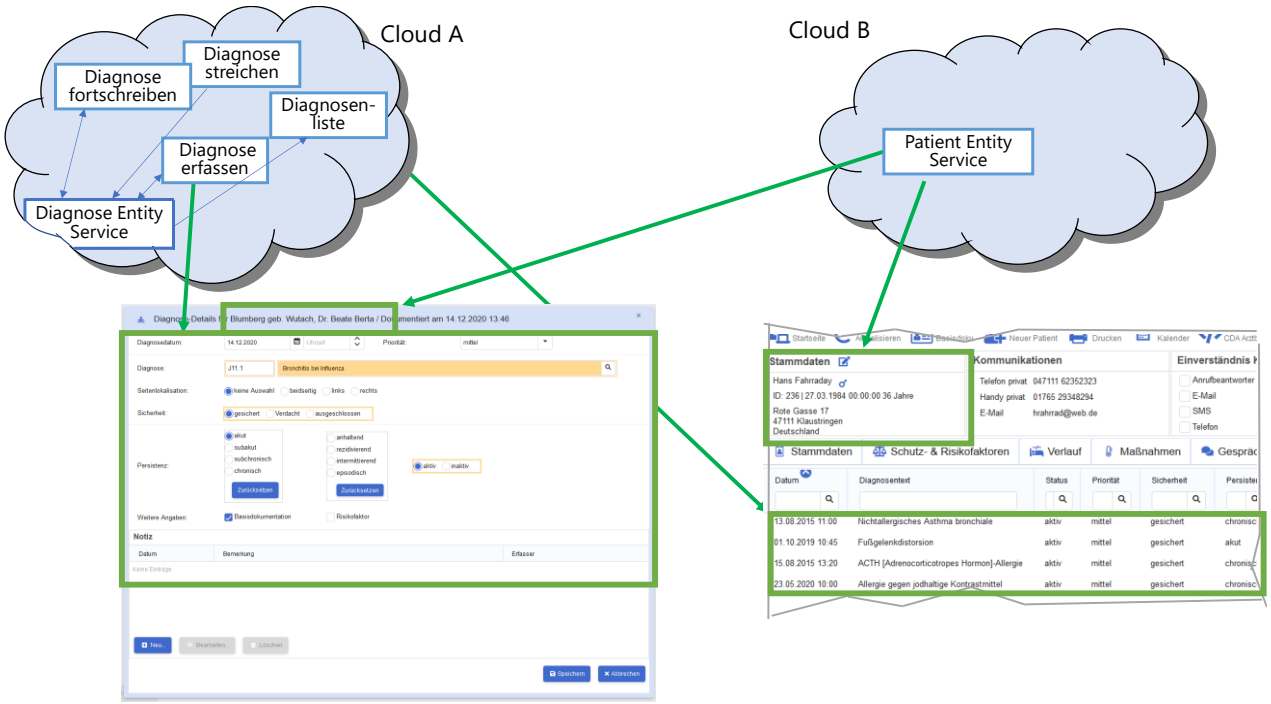

Abbildung 4-19*: Trennung von medizinischen und identifizierenden Daten am Beispiel Diagnosedokumentation im System ophEPA*

Da jedoch auch eine pseudonymisierte Verarbeitung eine personenbezogene Verarbeitung ist, fällt auch diese unter die DSGVO und bedarf eines Erlaubnistatbestandes.

Eine weitere Möglichkeit besteht darin, die Datenspeicherung hybrid vorzunehmen, so bieten einige kommerzielle Cloud-Plattformen die Möglichkeit, dass Daten hybrid, also teilweise in der Cloud und teilweise lokal, gehalten werden und die Verarbeitung selbst nur in der Cloud stattfindet. So könnten alle Patientenstammdaten lediglich lokal vorhanden sein. Natürlich

muss dann sichergestellt sein, dass in den Freitext-Attributen der medizinischen Dokumentation keine Angaben gemacht werden zur Person, die eine Re-Pseudonymisierung zulassen oder direkt Name und Vorname enthalten („Frau Müller, geb. am 7.5.1958 berichtet über ….").

Letztendlich können die vorgenannten Ansätze auch mit kryptographischen Konzepten des Secret Sharings noch weiter verfeinert werden. So wäre denkbar, dass jedes MSCM eine Anwendungsverschlüsselung vornimmt und den „eigenen" Schlüssel über eine sichere Authentifizierung und Verbindung zur Laufzeit aus einer anderen Cloud eines anderen Providers bezieht. Es besteht jedoch noch Forschungsbedarf zu solchen Ansätzen.

Anforderungen an mCloud-KIS:

- Es muss ein differenziertes Konzept für die Sicherstellung der Vertraulichkeit der beim Provider gespeicherten Patienten- und Behandlungsdaten vorliegen, welches auch den Aspekt der Zugreifbarkeit/Einsichtnahme durch den Provider selbst berücksichtigt. Dieses muss Teil des Auftragsdatenverarbeitungsvertrages sein.
- Für Patienten- und Behandlungsdaten ist zumindest eine Plattenverschlüsselung vorzusehen.
- Je nach Auftragsdatenverarbeitungsvertrag und rechtlichen Rahmenbedingungen sind weitere Absicherungsmaßnahmen gegen Inkenntnisnahmemöglichkeiten durch den Provider vorzusehen so z.B.
    - Verschlüsselung durch Anwendungssoftwaremechanismen
    - Verteilte Geheimnisse und physische Trennung von Patientenstamm- und Falldaten von den medizinischen Daten (= pseudonymisierte Speicherung der medizinischen Daten)
    - Hybridspeicherung der Daten in Cloud und vor Ort

4.7.4 Datensicherheitsmechanismen

Unter Datensicherheit werden alle Maßnahmen verstanden, die dem Schutz aller Daten in einem Unternehmen dienen. Im Grunde können hier auch die zuvor angesprochenen Aspekte des Datenschutzes subsummiert werden. Das BSI definiert in seinem Glossar „Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein modernerer Begriff dafür ist „Informationssicherheit"".[393] Im ISO/IEC 17789-Standard heisst es hierzu: „It is critical to recognize that security is a cross-cutting aspect of the architecture that spans across all views of the reference model, ranging from physical security to application security. Therefore, security in cloud computing architecture is not solely a cross-cutting aspect under the control of cloud service providers, but also affects cloud service customers, cloud service partners and their sub-roles."[394]

Für Cloud-Services bzw. Cloud-Anwendungssystemlandschaften werden neben den in der BSI-Definition genannten Aspekten zu berücksichtigen, dass auch umfangreiche Management- und Kontrollfunktionalitäten für die Cloud-Anwendungslandschaft wichtig sind, wie die Erken-

[393] Siehe https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html.

[394] ISO, ISO/IEC 17789 Information technology – Cloud computing – Reference architecture. 2014. S. 27 ff.

nung, Diagnose und Behebung von Ressourcen- und servicespezifischen Problemen, das systemweite Logging, Aktivitätsüberwachungen und Erkennung von Auffälligkeiten bei der Nutzung, Session Monitoring, Monitoring des Laufzeitverhaltens und alle Maßnahmen die der Cybersicherheit dienen.

Der Einsatz entsprechende Datensicherheitsmechanismen muss für Cloud-KIS zwischen Krankenhaus und Dienstleister in den Service Level Agreements vereinbart werden. Insofern gelten für Cloud-KIS alle Anforderungen, wie sie heute auch für jedes KIS gelten, zusätzlich sind aber wie im ISO-Standard angegeben Mechanismen für die Überwachung der verteilten Anwendungslandschaft – so auch für ein Cloud-KIS – zu implementieren. Cloud-KIS dürfen daher nur in z.B. nach BSI-Grundschutz und ISO/IEC 27001 zertifizierten Rechenzentren und DSGVO-konform betrieben werden.

Anforderungen an Cloud-KIS:

- Neben den üblichen Maßnahmen ist eine Überwachung der verteilten Anwendungslandschaft sicherzustellen.

4.8 Integritätsaspekte in einem Cloud-KIS

4.8.1 Einführung

Integrität ist eine der wesentlichen Anforderungen in der Informatik: Daten bzw. Datenbestände sollen in sich schlüssig, nicht widersprüchlich und bezogen auf den abzubildenden Realitätsausschnitt korrekt – also richtig und vollständig –sein. Aber auch Verarbeitungsprozesse sollen analog dazu in sich schlüssig, nicht widersprüchlich und bezogen auf ihre funktionale Aufgabe korrekt sein. Die Integrität von betrieblichen Informationssystemen ist als Faktor der Strukturqualität zuzurechnen und hat einen direkten Einfluss auf die Prozess- und Ergebnisqualität. Wie bereits einführend herausgestellt, ist moderne, effektive, qualitative und sichere Patientenversorgung ohne medizinische Informationssysteme nicht mehr erbringbar. „Der Schutz der Integrität von Daten, Systemen und Prozessen wird wichtiger und ist eine wesentliche Grundlage für die anderen Schutzziele: Verfügbarkeit und Vertraulichkeit."[395] Darüber hinaus ist eine zugesicherte und durch technische und organisatorische Maßnahmen sichergestellte Integrität auch unabdingbare Voraussetzung für die Vertrauenswürdigkeit eines Informationssystems. Zu Betrachtungen und Beispielen wird auf Kapitel 3 des ZVEI-Whitepapers[396] verwiesen.

Informationssysteme bilden Realitätsausschnitte durch verschiedene in nachfolgender Abbildung angegebene inhärente Aspekte ab, die als „Wissens- und Erfahrungshintergrund" eines Informationssystems angesehen werden können.

[395] ZVEI, Whitepaper Integrität von Daten, Systemen und Prozessen als Kernelement der Digitalisierung. S. 9.

[396] ZVEI, Whitepaper Integrität von Daten, Systemen und Prozessen als Kernelement der Digitalisierung. S. 20 ff.

Schema	Semantik	Business-objekte	Bezugsobjekte	Verhalten
Informations- & Daten-modell führt zu Struktur des Datenspeichers („domänenontologi-sches Wissen“ der Entwickler bzw. des Systems über Objekt-typen des Realweltaus-schnittes und deren charakterisierenden Attribute)	Inhaltliche Festlegungen für bestimmte Attribute der Objekttypen (erlaubte Ausprägungen in qualita-tiver oder quantitativer Hinsicht, Wertebereiche)	Die gemeinsamen „Geschäfts-Datensätze“, also die prozess-, verar-beitungs- und kommuni-kationsrelevanten konkereten Objekte, über die man kommuniziert (früher oft als „Bewegungsdaten“ bezeichnet)	Objekte, auf die im Rahmen der Kommuni-kation Bezug genommen wird, aber nicht haupt-sächlicher Gegenstand der Kommunikation sind (rüher oft als „Stamm-daten „bezeichnet)	Die Algorithmen, also Programme zur Verarbeitung der Daten, Reaktionen des Systems etc.

Abbildung 4-20: Wissens- und Erfahrungshintergrund eines Informationssystems[397]

Integrität in einem verteilten System wie einem Cloud-KIS kann nur hergestellt werden, wenn in den überdeckenden Kontexten der verschiedenen Systeme bzw. Module diese Aspekte strukturell und inhaltlich gleich oder kongruent und überführbar untereinander abgebildet werden.

Für Datenhaltungen bzw. im Bereich der Datenbanken werden im Wesentlichen

- Objektintegrität
- Referentielle Integrität
- Semantische Integrität und
- Ablaufintegrität

unterschieden. Die Sicherstellung wird im Bereich der Datenhaltungen von Datenbankmanagementsystemen mit entsprechenden Mechanismen vollständig unterstützt, sofern gewisse Designprinzipien beim Entwurf des Datenmodells eingehalten werden. Oftmals wird die semantische Integrität auch mittels referentieller Integrität sichergestellt, in dem qualitative Wertebereiche für Attribute („Domains“) in eigenen Tabellen abgelegt werden und der Primärschlüssel als Fremdschlüssel in der entsprechenden Objekttyptabelle zum Attribut wird, sodass nur semantisch korrekte Einfügungen von Werten auf Datenbankebene möglich sind. Weitere Ansätze sind die Nutzung von Triggern, z.B. um quantitative Integritätsbedingungen abzubilden.

Auch die Integrität während der Laufzeit von Datenoperationen wird sichergestellt, also die jederzeitige Konsistenz der Datenhaltung. Transaktionen bzw. Transaktionssicherheit dienen dazu, die Datenhaltung von einem integren Zustand in einen neuen integren Zustand zu überführen.

In einem verteilten System bzw. einer verteilten Anwendungssystemlandschaft wie z.B. in einem Cloud-KIS, in der die gleichen Daten – seien es Businessobjekte, Bezugsobjekte oder Semantikkataloge – redundant in den verschieden Anwendungssystemen oder Cloud-Modulen gehalten werden müssen, sind die o.a. klassischen Integritätsbedingungen sowie die Konsistenz

[397] Haas, eLearningeinheit „Einführung in die semantische Interoperabilität (1)“. 2019.

von Daten über alle Systeme und Module hinweg ebenfalls in geeigneter Weise analog sicherzustellen. Dabei kann und ist es ein Ziel beim Zuschnitt einer Cloud-Lösung, diese Redundanzen so klein wie möglich zu halten, was durch optimale Kohäsion und geringstmöglichste Überdeckung des „Bounded Context" zwischen Systemen bzw. Modulen erreicht werden kann. Dann wird nicht mehr über alle Daten eine sequentielle Konsistenz erforderlich, sondern es reicht eine kausale Konsistenz.

Neben den o.a. datenhaltungsbezogenen Integritätsbedingungen können jedoch auch noch weitere angeführt werden: Einerseits ist die integre Verarbeitung zu nennen, d.h. alle Systeme die Daten in gleicher Weise benutzen und verarbeiten, tun dies algorithmisch bzw. hinsichtlich von Verarbeitungsergebnissen identisch, man könnte hier von **funktionaler Integrität** sprechen. Ein Beispiel: Existieren mehrere AMTS-Dienste, so sollten diese alle bei gegebenem Input auch die gleichen Prüf-AMTS-Ergebnisse liefern. Andererseits sollte auch die Gesamtsumme der Softwaremodule vollständig im Sinne der Zielerreichung sein, man könnte hier von einer „**Softwareintegrität"** sprechen. Gerade in modularen skalierbaren Software-Umgebungen muss sichergestellt sein, dass die intentional orchestrierte Gesamtsumme der Funktionalitäten jederzeit – auch bei Austausch von Modulen – vorhanden ist. Wenn also von einem Cloud-KIS erwartet wird, das AMTS-Prüfung enthalten ist, sollte sichergestellt sein, dass diese auch vorhanden ist. In diesem Sinne müssen alle Teile eines Gesamtsystems sich in einer zentralen Instanz registrieren können. Dies ist nicht gleichbedeutend mit der in Kapitel 4.4 diskutierten Verfügbarkeit.

4.8.2 Datenintegrität

Bezüglich der Datenintegrität sind in einem verteilten System in Analogie zu den einführend genannten Aspekten in einem Cloud-KIS die überlappend gespeicherten also redundant vorhandenen Daten integer zu halten. Die ist vor allem in einem modularen Cloud-KIS im Sinne eines Cloud-Nativ-Systems von besonderer Bedeutung, da durch die in den einzelnen Modulen mit ihrem Bounded Context und der eigenen Datenhaltung für den überlappenden Bereich gehaltenen Daten zu mehr Redundanz führen als bei klassischen Legacy-Systemen. Bei konsequenter Berücksichtigung des Prinzips der maximalen Kohäsion sollte aber der Überlappungsbereich zumeist sehr klein sein.

Insgesamt erscheinen folgende Aspekte für Cloud-KIS von besonderer Bedeutung:

- **Objektintegrität**: Alle Informationsobjekte unabhängig von ihrer Granularität müssen in allen ihren Instanziierungen mit dem gleichen Objekt-Identifier (OID) geführt werden, der nichtsemantisch sein muss. Hierzu sollten die initial solche Informationsobjekte generierenden Anwendungen eine ISO-konforme weltweit eindeutige ID generieren. Werden Objekte aggregiert, müssen sie innerhalb der Aggregationen ebenfalls weiter ihr Objekt-ID mitführen.
- In diesem Zusammenhang sollte auch jede (instanziierte) Anwendung des Cloud-KIS über eine weltweit eindeutige **Instanz-Anwendungs-ID** identifiziert sein, also eine Stufe tiefer als die UDI bei Medizinprodukten, da jede Instanziierung im Rahmen einer Cloud-Anwendungssystemlandschaft eindeutig sein sollte. Die sollte sich zusammensetzen aus einer weltweit eindeutigen Produktnummer, einer Instanz-Nummer und der Softwareversion.

- **Strukturintegrität:** Für die überdeckenden Aspekte von Business- und Bezugsobjekten müssen die Schemata identisch oder kongruent sein.
- **Semantische Integrität:** Verwendung der gleichen Wertebereiche für gleiche charakterisierende Attribute der Objekttypen
- **Businessobjekt-Integrität:** Redundant in den verschiedenen Systemen bzw. Modulen gehaltene Daten – in diesem Sinne der zwischen diesen Systemteilen „überdeckende" Realweltausschnitt in Form bestimmter Objekttypen und ausgewählter charakterisierender Attribute – müssen identisch sein. Dies bezieht sich sowohl auf das Informationsschema als auch die konkreten Datenobjekte.
- **Bezugsobjekt-Integrität:** Werden in den Systemen bzw. Modulen bestimmte Organisationen, Personen, Materialien, Medikamente, Hilfsmittel etc. verwendet und nicht nur referenziert, müssen die redundant gehaltenen Bezugsobjekte sowohl hinsichtlich des Informationsschemas als auch der konkreten Ausprägungen identisch sein. Werden diese nur referenziert (z.B. Verwendung einer Material-ID, einer Org-ID), ist die Integrität über die referentielle Integrität sicherzustellen.
- **Referentielle Integrität:** Alle von Systemen/Modulen referenzierte Informationsobjekte und Semantikausprägungen anderer Systeme/Module oder aus Repositories müssen vorhanden sein und dürfen nicht mehr unabhängig gelöscht werden.
- **Medizinische Aktenintegrität:** Alle medizinischen Informationsobjekte in einer Patientenakte müssen für eine Weiternutzung im Rahmen von Behandlungsentscheidungen freigegeben sein und Zughörigkeit und der Kontext Ihrer Entstehung vorhanden sein (z.B. Patientenbezug, wer hat wann warum im Rahmen welches Behandlungsevents Informationen eingefügt, geändert, freigegeben, siehe auch Muß-Angaben im CDA-Header)
- **Zurechnungsintegrität:** Jeder Information muss dem „Ersteller" (einer Person in ihrer Rolle in einer Organisationseinheit oder einem medizintechnischen Gerät)

Ein wesentlicher Aspekt in verteilten Systemen und so auch in Cloud-Software und Cloud-KIS ist die systemweite Synchronisation von Replikaten bzw. Informationsobjektinstanzen, wobei nicht immer dafür ein „führendes" System bzw. Modul angegeben werden kann, da manchmal auch mehrere Systeme/Module nach erster Instanziierung eines Objekttyps Daten dieser Instanz ändern und ergänzen dürfen. Hier reicht als Grundmechanismus ein „Multi-Cast" vom führenden System abgehend, wie das heute bei den Nachrichtenbasierten Synchronisationen via Kommunikationsserver der Fall ist, dann nicht aus. Zumindest für die einzelnen Repositories kann je nach Art jedoch ein führendes System angegeben werden, so sollten z.B. nutzende Systeme/Module nicht Medikamentenstammdaten, Materialstammdaten usw. ändern können dürfen, sondern solche Änderungen dürfen nur die Repository-Module durchführen.

Für Cloud-KIS gibt hier aber einige eher „vereinfachende" Aspekte, die generell für medizinische Patientenaktensystemen gelten und die sich so auch in den internationalen Interoperabilitätsstandards abbilden: Es gibt zwei wesentliche „Core Business"-Objekttypen: **Patient und Fall**. Jede medizinische Information in einem KIS muss immer einem Patienten und einem Fall bis mehreren Fällen zugeordnet werden, zumindest hinsichtlich der Entstehung einer Information. Wichtige Informationen sind aber auch oftmals für alle Fälle des Patienten relevant, so dass gegebenenfalls auch medizinische „Core Objects" zu berücksichtigen sind.

Eine Cloud-KIS-weite Integrität kann im Wesentlichen über folgende Repositories (siehe auch Kapitel 4.4.6) und Mechanismen erreicht werden:

- Repository der Krankenhaus-Organisationseinheiten und Mitarbeiter (internes Health Provider Directory)
- Repositories zu allen systemweit relevanten Bezugsobjekten
- Repository zur systemweit relevanten Semantik (Terminologieserver)
- Synchronisationsmechanismen für kontrollierte Redundanz der mehrfach (evtl. teilweise) vorhandenen Instanzen eines Informationsobjektes,
- Master Patient Index als Referenz-Repository für Patientenidentifikation und Patientenstammdaten
- Fallindex als Referenz-Repository aller administrativen Fälle und deren Falldaten

4.8.3 Entitäten-übergreifenden Patientenidentifizierung

Ein besonderer Aspekt in medizinischen Informationssystemen ist es, dass im Kern fast alle anfallenden und zu verwaltenden „Business-Objekte" im Rahmen von Patientenbehandlungen anfallen und immer einem konkreten Patienten zugeordnet werden können müssen. Zumeist ich auch eine Zuordnung zu einem administrativen Fall notwendig, wünschenswert wäre auch eine Zuordnung zu einem medizinischen Fall, um medizinische Fallsichten zu ermöglichen. Damit wird eine systemweite eindeutige Patientenidentifizierung notwendig, die es auch Nutzern erlaubt, jederzeit festzustellen, ob der informationstechnische Kontext, in dem er sich bewegt und arbeitet, auch dem richtigen Patienten zugeordnet ist.

Für eine systemweite Patientenidentifikation in einem verteilten System im Gesundheitswesen hat sich in der Vergangenheit das Konzept des Master Patient Index etabliert, dessen Funktionalität darin besteht, wie ein Patienten-Repository zu funktionieren – manchmal auch als „zentraler Verzeichnisdienst für Patienten" bezeichnet. Hier werden alle Patientenidentitäten aus den verschiedenen Systemen zusammengeführt und abgeglichen, der MPI enthält aber nur IDs und für die (Re)Identifikation notwendige Attribute. Kein System in einem Verbund darf ohne vorangehende Abfrage des MPI einen neuen Patienten anlegen, da ohne Abgleich viele nicht automatisierbar zusammenführbare Dubletten entstehen würden. Außerdem kann ein MPI eine ID-Umsetzung zwischen verschiedenen Systemen unterstützen. Heute sind eine Reihe von kommerziellen MPI-Produkten verfügbar. Auch für MPI hat IHE mit dem PIX-Integrationsprofil[398] eine detaillierte Spezifikation vorgelegt, die Kommunikation erfolgt hier auf Basis von HL7-V3-Nachrichten.

Für ein modulares Cloud-KIS im Sinne eines Cloud Native Anwendungssystems wird genau genommen kein MPI in der heute gegebenen Form mehr notwendig, da die einzelnen CMSM nicht mehr selbstständig Patientenstammdaten erfassen lassen, sondern eben ein systemweit verfügbarer Microservice hierzu genutzt wird. Im Grunde hat dieser Microservice ähnliche Aufgaben und Funktionalitäten wie der MPI, aber die ursprüngliche Problemstellung aufgrund derer MPI entworfen wurden existiert so zumindest innerhalb eines mCloud-KIS eines Krankenhauses nicht mehr. Da aber von einem längeren Migrationsprozess ausgegangen werden muss und es sicher über die Zeit zu Hybridlösungen kommt, die einer heterogenen Systemlandschaft

[398] Siehe https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf#nameddest=23_Patient_Identifier_Cross_ref.

entsprechen, wird auch ein MPI in einem Cloud-KIS erst einmal weiter betrieben werden müssen. Im Sinne einer losen Kopplung und maximaler Kohärenz sollte diese Funktionalität auch nicht mit dem nativen Microservice für die Patientenverwaltung vermischt werden. Zusätzlich ist zu erwarten, dass ähnlich wie das bei eHealth Suisse umgesetzt wurde mit den „Gemeinschaften", dass ein MPI in einem verteilten Öko-System interoperierender Cloud-Primärsysteme weiterhin – z.B. in einer Community Cloud – eine Rolle spielen wird.

4.8.4 Funktionsintegrität und Softwareintegrität

Neben der oftmals in den Vordergrund gerückten Datenintegrität spielt in einem modularen Gesamtsystem auch die **Integrität der Funktionalität** sowie die funktionale **Gesamtsystemintegrität** des eine wichtige Rolle. Dies bedeutet, dass sich einerseits alle Funktionalitäten wie gewünscht und beschrieben verhalten, aber eben auch in verschiedenen Systemen oder Modulen gleichartig vorhandene Funktionalitäten auch gleichartig verhalten. Darüber hinaus muss dann auch sichergestellt sein, dass entsprechende Funktionalitäten nicht unberechtigterweise verändert werden, also funktionale Änderungen und Weiterentwicklungen nur durch definierte Deployment-Prozesse durch dazu berechtigtes Softwarelieferanten eingebracht werden dürfen. Es sind da in einem Cloud-KIS auch entsprechende Mechanismen zur Überwachung der funktionalen Integrität einzubauen.

Funktionale Integrität wirkt sich dort, wo einzelne Benutzer gleichartige Funktionalitäten verschiedener Systeme benutzen, auch direkt auf die Erwartungskonformität aus. Bei sachgerechter funktionaler Zerlegung dürften jedoch funktionale Dopplungen nicht mehr vorkommen, es sei denn, der Provider unterstützt eine Multi-Vendor-Cloud, dann kann es für gleich Funktionalitäten auch mehrere alternativ nutzbare Module geben. Für gewisse Funktionen können daher eine Vielfalt und auch abweichende Bedienung und Funktionalität erwartet und akzeptiert werden, dort aber wo direkt durch Algorithmen behandlungsbezogene Aspekte betroffen sind wie z.B. bei den AMTS-Prüfungen, ist sicherzustellen, das gleiche Module sich auch gleich verhalten.

Für ein feingranulares cloud-KIS sind eine Vielzahl von CMSM zu erwarten, sodass für ein Krankenhaus schnell der Überblick verloren werden kann, was einerseits prinzipiell verfügbar ist, andererseits was vertraglich genutzt wird/werden kann und was ggf. mit welcher Häufigkeit genutzt wird. Hier ist es sicher hilfreich, wenn die Module selbstbeschreibend sind – also über gewisse Metadaten verfügen z.B. zu den durch sie verwalteten Objekttypen und Funktionen - und jedes Modul automatisch beim Deployment in die (Multi-)Vendor-SaaS-Umgebung automatisch in einem Modul-Repository mit seinen Metadaten registriert bzw. akkreditiert wird. Dies könnte im Grunde automatisiert und gekoppelt mit entsprechenden Cloud Source Repositories der Hersteller erfolgen. Des Weiteren sollte auch für das Krankenhaus transparent nachvollziehbar sein, welches Modul mit welchen anderen interoperiert bzw. welche Services nutzt, was ebenfalls in der Selbstbeschreibung eines jeden Moduls verzeichnet sein könnte. So können auch für die Überwachung und Transparenz des Cloud-KIS automatisiert Cross-Referenzen generiert werden. Das Modul-Repository ist dann der „Produktkatalog" der mCLoud-KIS-Lösung. Ein Framework hierfür wurde von HL7 spezifiziert[399] („Enterprise Consistency and

[399] HL7 International, Enterprise Consistency and Conformity Framework (ECCF). 2019. S. 44 ff.

Conformity Framework (ECCF)"), das entsprechenden Spezifikationen und Entwicklungen zu Grunde gelegt werden kann.

Für die Spezifikation oder zumindest Verlässlichkeit der Datenverwaltungsfunktionalität gewisser wichtiger Module eines KIS helfen die bereits vorhandenen Standard vor allem von HL7 (HL7-Nachrichten, FHIR-Spezifikationen) und IHE, die oftmals schon Informationsschemata beinhalten und somit eine gewisse Standardisierung zumindest von Datenverwaltungsfunktionalitäten vorgeben. So sind heute viele medizinische Informationsobjekttypen über die diese Standards gut definiert und können für die Modellierung des Bounded Context eines Moduls herangezogen werden. Beispiele sind die Patientenstammdaten, Angaben zu Diagnosen, zu Assessments, zu Laborergebnissen, zu Symptomen und Einzelbefunden. So können in verteilter und agiler Weise von unterschiedlichsten Firmen schema- und semantikkonforme Implementierung vorgenommen und bruchlos in das mCloud-KIS bzw. die Multi-Vendor-SaaS-Umgebung von Providern eingefügt werden.

4.8.5 Parametrierungs- und Konfigurationsintegrität

Parametrierungsintegrität

In betrieblichen Informationssystemen wird das Konzept der Parametrierbarkeit weitreichend eingesetzt, auch um Standardprodukte an die Gegebenheiten des Kunden ohne Programmieraufwand anzupassen. Systeme haben also strukturelle und funktionale „Unschärfen", die durch Parametrierung in der Kundeninstanz geschärft werden. Damit soll auch eine gewisse Robustheit gegenüber Änderungen im Kontext (z.B. Änderung von Abrechnungssätzen, Änderung von Diagnosekatalogen u.v.a.m.) erreicht werden. Man kann hier von einer **Struktur- und Verhaltensflexibilität** sprechen. Vor dem Einsatz muss also in der Regel ein umfangreiches Customizing durchgeführt werden. Parametrierbarkeit kann sich z.B. beziehen auf die Parametrierung[400]

- von Wertebereichen für Attribute in den einzelnen Dokumentationsfunktionen,
- von einfachen bis komplexen Integritätsbedingungen,
- von Bezugsobjekten,
- der Ablaufdynamik und des Systemverhalten,
- der Workflowsteuerung,
- von Verarbeitungseigenschaften wie Preisberechnungen, Kostenbewertungen etc.,
- der Zugriffs- und Nutzungsmöglichkeiten und die
- der verwalteten Inhalte und der zugehörigen Benutzeroberfläche (generische Funktionen).

Für ein Enterprise-System kann von einigen Tausenden von Parametern ausgegangen werden.

Während in einem Legacy-System mit in der Regel einer systemweiten Datenbank solche Parameter auch systemweit zugreifbar sind, stellt sich dies in einer Microservice-basierten Implementierung nicht mehr so dar. Wenngleich postuliert werden kann, dass durch das Prinzip der Kohäsion Parameter auch nur in einem CMSM gebraucht werden, gibt es doch weiterhin viele, die auch in einigen bis vielen CMSM oder sogar systemweit gültig sind und genutzt werden müssen. Wird die Parametrierung dann je CMSM notwendig, kann es schnell zu abweichenden Parameterausprägungen kommen. Es ist daher eine Parametrierungsinfrastruktur in einem

[400] Haas, Medizinische Informationssysteme und Elektronische Krankenakten. 2005. S. 94 ff.

mCloud-KIS zu implementieren, bei der z.B. die Parameternutzung selbst über Microservices ermöglicht wird (was aber stark den Traffic zwischen Microservices erhöht) oder aber durch kontrollierte Redundanz, bei der Änderungen automatisch in die CMSM repliziert werden. Da die meisten Parameter wenig volatil sind, erscheint zweitgenannter Ansatz effizienter. Aber auch Hybridansätze sind denkbar, denn wo Parameter tatsächlich ausschließlich in den Kontext eines CMSM fallen, können sie auch nur lokal verwaltet werden.

Konfigurationsintegrität

Unabhängig von der Konfigurationsintegrität der von der Cloud-Plattform zur Verfügung gestellten Services und Ressourcen müssen auch die fachlogischen CMSM in ihrer Summe integer sein. Dies bedeutet, dass sowohl gewisse Bundles die für eine fachliche Gesamtfunktionalität zusammengehören oder CMSM die in ein-/gegenseitiger Abhängigkeit stehen auch vorhanden sind. Dies bedeutet, dass bei Buchung bzw. Zusammenstellung der konkreten Konfiguration das Konfigurationsportal auf Basis der CMSM-Registry solche Zusammengehörigkeiten und Abhängigkeiten berücksichtigt werden müssen. So wäre es für das Medikationsmanagement-Beispiel aus Kapitel 4.3.4 zwar denkbar, einige Funktionen herauszulassen, aber der Kern – also das minimal notwendige CMSM-Bundle müsste zumindest – wenn wir einmal annehmen, dass wir auch nicht die Einnahme dokumentieren wollen – aus *Medikationsplan einsehen*, *Medikation/Medikament anordnen*, *Unverträglichkeit dokumentieren*, *Medikationsabsetzung dokumentieren* und *Medikationswiederaufnahme dokumentieren* bestehen.

Jede Cloud-Plattform unterstützt heute ein entsprechendes Konfigurationsmanagement, in dem auch Abhängigkeiten festgelegt werden können.

4.8.6 Authentizität, Zurechenbarkeit und Kontext.

In medizinischen Informationssystemen werden nicht nur sehr sensible Daten gespeichert und verarbeitet, sondern auch solche, die im Rahmen einer weiteren Behandlung oder für in der Zukunft liegende Vorfälle und Behandlungen eine bis hin lebenswichtige Rolle spielen. Eine verlässliche Weiternutzung für den weiteren Behandlungsprozess kann nur erfolgen, wenn sich Nachnutzer auf die Authentizität und Zurechenbarkeit der Informationen belastbar verlassen können. Dazu ist auch eine Sicherstellung der Authentizität des Benutzers. Diese Anforderungen sind aber unabhängig von der technischen Ausprägungsform eines KIS, ob Legacy-System oder mCloud-KIS. Wie bereits in Kapitel 4.4.7 angesprochen, muss jedes medizinische CMSM neben den eigentlichen fachspezifischen Daten die es verwaltet auch Kontext- und Referenzinformationen enthalten, die auch Authentizität und Zurechenbarkeit sicherstellen. Diese Kontextdaten sollten strukturell über alle medizinischen CMSM gleich sein. Als Grundlage für eine Spezifikation könnten z.B. Angaben aus dem CDA-Header dienen. Die FHIR-Ressourcen selbst haben zum Großteil keine Attribute für entsprechende Angaben wie Autor oder Ersteller oder ein Attribut für die digitale Signatur.

Perspektivisch sollten bei Verfügbarkeit von elektronischen Heilberufs- und Berufsausweisen auch kryptographische Verfahren von Cloud-KIS unterstützt werden, also die (qualifizierte) elektronische Signatur.

Neben der Authentizität der Nutzer und Nutzdaten sollten auch die Cloud-Services selbst gegenüber dem Benutzer authentifizieren, um mögliche Man-in-the-Middle- Angriffe oder die Übertragung und Verarbeitung von Daten durch bösartige Cloud-Services zu verhindern.

Auch die Zurechenbarkeit bezieht sich in einem Cloud-System nicht nur auf die Nutzdaten, sondern jegliche Aktion im Cloud-System – so auch die Änderung von Ressourcenzuweisungen, das Einspielen neuer Versionen von Micro-Services u.v.a.m. – muss zurechenbar sein. Auf technischer Ebene gewährleisten das aber die kommerziellen Plattformen.

Neben allen vorgenannten Maßnahmen muss ein Cloud-KIS auch ein umfassendes Logging durchführen, mittels dem auch vor endgültiger Freigabe bzw. Signatur eines Informationsobjektes vorgenommene Manipulationen (Änderungen, Fortschreibungen) zurechenbar sind, da oftmals mehrere Akteure/Personen an der Erstellung eines Informationsobjektes beteiligt sind.

4.8.7 Integritätsaspekte Zusammenfassung

Cloud-KIS müssen, wie alle Cloud-Anwendungen und -Systeme, in umfassender Weise die Integrität sicherstellen. Gerade in der Medizin ist diese von besonderer Bedeutung, werden doch die Daten in umfangreicher Weise für medizinische Behandlungen genutzt und Integritätsfehler können dann zu Behandlungsfehlern führen, im Extremfall bis hin zu schweren Folgeschäden oder Tod.

Anforderungen an Cloud-KIS:

- Durch geeignete Mechanismen ist die Datenintegrität sicherzustellen, u.a. sind hier zu nennen
  - Objektintegrität
  - Strukturintegrität
  - Semantische Integrität
  - Businessobjekt-Integrität
  - Bezugsobjekt-Integrität
  - Referentielle Integrität
  - Medizinische Aktenintegrität
  - Zurechnungsintegrität
- Durch geeignete Mechanismen ist die eindeutige Patientenidentifikation sicherzustellen. Hierzu sollte ein Cloud-KIS über einen Microservice-basierten MPI verfügen.
- Durch geeignete Mechanismen ist die Funktionsintegrität sicherzustellen. Da bei einem Multi-Vendor-Cloud-KIS eine Funktionalität von verschiedenen Herstellern stammen können, sollten sich diese zumindest algorithmisch bei den die direkte Behandlung unterstützenden Funktionalitäten (Beispiel AMTS) gleich verhalten.
- Durch geeignete Mechanismen ist die Softwareintegrität sicherzustellen. Dies bezieht das kontrollierte Deployment von Microservice-Modulen mit ein.
- Zurechenbarkeit, Authentizität und Entstehungskontext von Medizinischen Informationsobjekten müssen gewährleistet werden.
- Durch geeignete Mechanismen ist die Parametrierungsintegrität sicherzustellen.
- Durch geeignete Mechanismen ist die Konfiguarionsintegrität sicherzustellen.

4.9 Semantische Interoperabilität

4.9.1 Einführung

Semantische Interoperabilität ist nach IEEE die „Fähigkeit von zwei oder mehr Systemen oder Komponenten zum Informationsaustausch sowie zur adäquaten Nutzung der ausgetauschten

Information."[401] Eine adäquate Nutzung impliziert analog zur Kommunikation zwischen Menschen, dass empfangene Nachrichten verstanden – also interpretiert und in (weiter)genutzt werden können. „Nutzung" bedeutet in diesem Sinne, das Anwendungssysteme in der Lage sind, als Reaktion auf empfangene Nachrichten eines Senders die enthaltenen Daten und Dokumente

- korrekt „einsortieren"/ ablegen zu können,
- Objekte und Begriffe selbstständig korrekte klassifizieren zu können,
- neue Daten mit Bereits vorhandenen ggf. auch semantisch und nicht nur referentiell „Inbezug-Setzen" zu können,
- eine korrekte (Weiter)Verarbeiten oder Konvertierung vornehmen zu können,
- auf eingehende Nachrichten im Bedarfsfall reagieren und Antworten rückgeben zu können,
- Meldungen auslösen zu können z.B. für Benutzer, eMails etc.
- ggf. „Dazuzulernen" (z.B. lokale Semantik oder Bezugsobjekte selbstständig ergänzen)
- eine wissensbasierte Interpretation der empfangenen Daten vornehmen zu können.[402]

Wie bereits in *Abbildung* 4-20 dargestellt, bilden sich der „Wissens- und Erfahrungshintergrund" eines konkret betriebenen Anwendungssystems in verschiedenen Aspekten ab, die alle für eine gelingende semantische Interoperabilität eine Rolle spielen. Ein gegenseitiges Verstehen setzt voraus, dass einerseits keine kommunikationsverhindernden strukturellen und semantischen Missmatches bestehen, aber auch der „Erfahrungshintergrund" in Form der vorhandenen Informationsobjekte der Kommunikationspartner gleich bzw. kongruent ist. Dies bedeutet konkret,

- dass es bezogen auf die Informationsstruktur von kommunikationsrelevanten Objekttypen keine Schema-Missmatches geben darf,
- dass alle teilnehmenden Systeme und Module die gleiche oder kongruente Semantikkataloge für gleiche charakterisierende Attribute benutzen,
- dass die referenzierten Bezugsobjekte (auch Stammdaten oder Grunddaten genannt) vorhanden und da ich eindeutig identifiziert und gleich sind und
- dass die Business-Objekte, über die Daten und Dokumente ausgetauscht werden bekannt sind.

Unabdingbare Voraussetzung für semantische Interoperabilität sind daher zuerst einmal das Vorhandensein akzeptierter und breit um- und eingesetzter Interoperabilitätsstandards, die Struktur und Semantik von Nachrichtentypen bzw. Service Schnittstellen festlegen, ebenso bestimmte Interaktionsmodelle. Darüber hinaus wird dann für Anwendungslandschaften notwendig, dass die Ausprägungen zu bestimmten für alle Teilnehmer relevanten Informationsobjekten systemweit in Form von verschiedenen Repositories (siehe Kapitel 4.3.6) zur Verfügung stehen.

[401] IEEE, A Compilation of IEEE Standard Computer Glossaries New York, Standard 1990.

[402] Haas, eLearningeinheit „Einführung in die semantische Interoperabilität (1)". 2019.

4.9.2 Semantische Interoperabilität im Gesundheitswesen

Im Gesundheitswesen hat semantische Interoperabilität eine inzwischen auf nationaler und internationaler Ebene eine lange Tradition. In Deutschland war zuerst vor allem der ambulante Bereich führend mit der Spezifikation und Nutzung der sogenannten xDT-Standards vor allem zuerst genutzt für die Labordatenübertragung, dann aber auch für andere Zwecke. International und in den USA entwickelte sich vor allem im stationären Bereich der Bedarf rasant und führte 1987 zur Gründung von Health Level 7 und in der Folge zur Entwicklung weltweit führender Health IT Standards. Für KIS ist heute vor allem eine Message-basierte Interoperabilität auf Basis von HL7-Nachrichten der Versionen 2.x und 3 etabliert und in Betrieb, meist koordiniert über eine systemweit vermittelnde Middleware – den Kommunikationsserver. In der Folge wurden aber auch spezielle Standards z.B. in der Radiologie mit DICOM geschaffen. Darüber hinaus hat IHE umfangreiche Profile für die digitale Zusammenarbeit in verschiedenen medizinischen Domänen entwickelt, in denen wiederum Basisprofile aus einer definierten IT-Infrastruktur (IHE-ITI) zum Einsatz kommen. Dabei setzen IHE-Profile auch auf den Standards von HL7 auf und berücksichtigen international verfügbare Semantikkataloge.

Prinzipiell muss zwischen den eigentlichen inhaltlichen Definitionen eines Kommunikations- bzw. Interoperabilitätsstandards und dem (software)technischen Binding für den konkreten technischen Datenaustausch unterschieden werden. So können Nachrichten auf technischer Ebene via Mail, via Interprozesskommunikation oder via Webservices ausgetauscht werden, und ihr Inhalt selbst kann ebenfalls mit verschiedensten Techniken bzw. syntaktisch alternativen Formen (z.B. HL7-Message, SOAP-Nachricht, JSON-String etc.) dargestellt bzw. übermittelt werden.

Anzahl und Umfang der für Gesundheitsanwendung verfügbaren Standards und Interoperabilitätsbeschreibungen sind inzwischen fast unüberschaubar geworden und können auf einige zig-Tausend Seiten beziffert werden, zumal aus den Standards dann auch auf nicht gesundheitsspezifische IT-Standards verweisen wird. So gibt es für spezielle Aspekte auch sehr spezielle Festlegungen bzw. Standards. Zu nennen sind hier zum Beispiel Festlegungen für die Datenübermittlung für die stationäre oder ambulante Abrechnung, die Kommunikation zwischen Modalitäten und Informationssystemen, die Kommunikation zwischen und mit Medizingeräten, die Übermittlung von Daten an Patientenakten Systeme, Datenmeldungen im Rahmen von berufsgenossenschaftlichen Behandlungen, die verteilte Verfügbarkeit von Behandlungsdokumenten z.B. via IHE/XDS z.B. beim Einsatz der eFallakte, die Meldung von Daten an verschiedene Register oder an das RKI u.v.a.m.. Aber auch Struktur und Semantik von bestimmten Dokumenten sind und werden zunehmend festlegt (z.B. die durch die kassenärztliche Bundesvereinigung definierten Medizinischen Informationsobjekte (MIO) für die elektronische Patientenakte, der Bundesmedikationsplan, der Notfalldaten Satz, BG-Bericht, Pflegeüberleitungsbericht u.v.a.m.)

Die zukünftige Entwicklung dürfte jedoch geprägt sein vom konsequenten Einsatz führender Standards wie FHIR von HL7 und für die Semantik die WHO-Klassifikationen sowie SNOMED. Für die Profilierung in bestimmten Einsatzszenarien kommen dann die IHE-Profile hinzu, als technische Kommunikationswege werden die sicheren Dienste der nationale Telematikplattform z.B. zum direkten Dokumentenversand an die ePA des Patienten nach SGB V oder für den Punkt-zu-Punkt-Dokumentenaustausch zwischen Leistungserbringern über den Dienst KIM in

Deutschland zumindest rechtlich und innerhalb der Versorgung von GKV-Patienten alternativlos werden.

Insgesamt ist festzustellen, dass die praxisorientierten bewährten verfügbaren Interoperabilitätsstandards für das Gesundheitswesen eine große Chance darstellen, Cloud-KIS und digitale Ökosysteme für das Gesundheitswesen rasch zu implementieren. Während in anderen Branchen noch um gemeinsame Standards gerungen wird, hat hier das Gesundheitswesen einen großen Vorsprung.

Alle die vorgenannten Entwicklungen und vorhanden Spezifikationen muss auch ein (m)Cloud-KIS in geeigneter Weise berücksichtigen und implementieren.

4.9.3 Interoperabilitätserfordernisse für Cloud-KIS

Mit Blick auf die Ausführungen in Kapitel 4.3 und 4.4 ergeben sich für Cloud-KIS Interoperabilitätserfordernisse auf verschiedenen Granularitäts-Ebenen. Für ein mCloud-KIS betrifft dies auf der granularsten Ebene die Zusammenarbeit der verschiedenen Cloud-Microservice-Module. Sodann müssen diese Module evtl. in geeigneter Weise mit anderen Cloud-Diensten – hier vor allem den Repositories – und dann auch fachlichen Cloud-Modulithen oder -Systemen interoperieren können und zuletzt auch mit ggf. vor Ort betriebenen Legacy-Systemen. Daneben müssen aber auch die weiter vorhandenen Legacy-Systeme oder Cloud-Monolithen selbst untereinander kommunizieren können. Für letztgenannte Zusammenarbeit können weiterhin die etablierten Mechanismen weiter genutzt werden.

Letztendlich muss ein Cloud-KIS auch an andere Systeme Daten und Dokumente übermitteln, was aber keinen Unterschied zu den Anforderungen an die heutigen Legacy-Systeme darstellt.

Den Gesamtzusammenhang zeigt nachfolgende Abbildung.

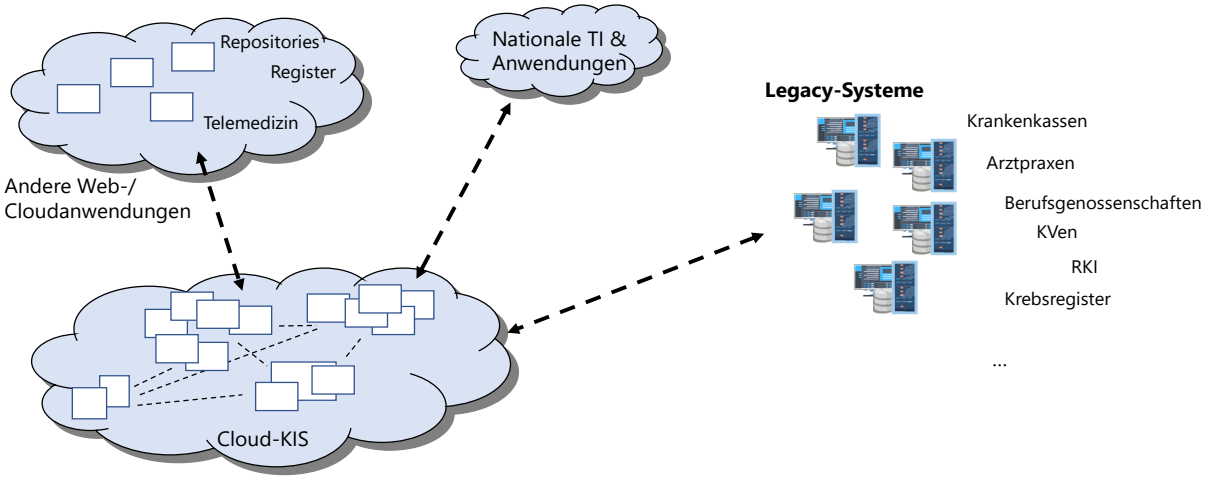

Abbildung 4-21: Interoperabilitätserfordernisse für ein Cloud-KIS

Interoperabilität zwischen den Cloud-KIS Microservice-Modulen

Die fachlogische Interoperabilität zwischen Cloud-KIS Microservices – zumindest jener untereinander der Module im User-Layer – kann und sollte weitgehend auf Basis von FHIR realisiert

werden, zumal viele von den einzelnen Microservices verwalteten klinischen Informationsobjekte im Grunde fast 1:1 in ihrer Struktur FHIR-Ressourcen entsprechen können, da die „Clinical-Resources" weitgehend die klinische Domäne abdecken. Die Idee von FHIR für Interoperabilität entspricht hinsichtlich der Granularität dem Microservice-Konzept für Kapselung und Datenspeicherung: „HL7, weitere Standardisierungsorganisationen sowie der Beraterstab für Wissenschaft und Technik des US-Präsidenten (PCAST) kamen 2011 zu der Überzeugung, dass die Größe der übermittelten Datenpakete weder zu groß (schwer zu handhabende hochkomplexe Datenstrukturen) noch zu klein (die Daten benötigen Metainformationen und Kontext, um ihre Bedeutung zu erhalten) gewählt werden darf. FHIR verwendet kompakte, in sich geschlossene Datenpakete, mit einheitlichem, wohldefiniertem Verhalten, Semantik, Kontext- und Metadaten."[403]

Die Spezifikationen zu den FHIR-Ressourcen können also nicht nur für die Interoperabilität dienen, sondern auch für die Implementierung entsprechender Microservices z.B. für die Dokumentation von Diagnosen, Symptomen, Prozeduren, Medikationen, Laborergebnissen, Pflegeziele und Pflegemaßnahmen, Assessments, klinischen Dokumenten, was eine Implementierung von Cloud-KIS bzw. Migration zu Cloud-KIS – zumindest für den klinischen Teil – erheblich beschleunigen kann.

Daneben ist es auch notwendig, dass mCloud-KIS Microservice Module auch Services der anderen Layer konsumieren. Aber auch hier kann teilweise auf FHIR zurückgegriffen werden wie z.B. die Module im Bereich „Security and Privacy", sofern die für eine Realisierung zugrunde gelegte Plattform nicht andere Serviceschnittstellen und Module erzwingt bzw. bereitstellt.

Interoperabilität eines Cloud-KIS mit anderen Cloud-Systemen und Referenzservices

Ein wesentliches Paradigma von Cloud Native Anwendungen ist es, dass in einer offenen skalierbaren Softwarelandschaft transparent und in einfacher Weise Microservice-Module interoperieren können. Dies gilt dann auch Cloud-übergreifend, wenn gewisse Module in einer Cloud des einen Anbieters aus Clouds anderer Anbieter erreichbar sind, denn diese können dann auch konsumiert werden. Bezogen auf ein Cloud-KIS sind solche „anderen" Cloud-Systeme vor allem in einem ersten Schritt verschiedene Repositories als DaaS (Bezugsobjekte-Repositories und Semantik-Repositories, siehe auch Kapitel 4.3.6), die im Sinne der Vermeidung von Mehrfachpflege z.B. auf regionaler oder sogar auf nationaler Ebene verfügbar sein sollten. So wäre ein nationaler cloud-basierter HPD einerseits einfach herstellbar und könnte sofort als Basis für das entsprechende Repository auch im Cloud-KIS dienen. Gleiches gilt für einen nationalen Terminologieserver.

Cloud-Repositories müssen natürlich ebenfalls hochverfügbar und skalierbar sein (siehe auch Kap. 4.6). Ob die Repository Einträge aus anderen Clouds dann zur Laufzeit direkt genutzt also konsumiert werden oder die Inhalte durch geeignete Mechanismen in die lokalen KIS-Cloud Repositories synchronisiert werden, ist für die semantische Integrität des Gesamtsystems dann unerheblich, solange in den lokalen Kopien nicht geändert wird.

[403] Siehe https://hl7.de/themen/hl7-fhir-mobile-kommunikation-und-mehr/warum-fhir/.

Da bereits auch in FHIR Ressourcen für die Verwaltung bestimmter Bezugsobjekte und von Semantik berücksichtigt wurden[404], können die Services für Cloud-Repositories ebenfalls auf FHIR basieren.

Daneben wird es dann in regionalen Ökosystemen zunehmend möglich, dass ein Cloud-KIS mit anderen Cloud-KIS interoperiert oder aber mit Cloud-basierten Kommunikationspunkten, die als Gateway z.B. für die Kommunikation mit lokal installierten Systemen z.B. in Arztpraxen funktionieren. Auch ein Gateway zu Diensten der nationalen Telematikinfrastruktur – so zum Beispiel zu KIM – ist ebenso umsetzbar. Letztendlich gibt es auch erste Ansätze für Implementierungen für cloud-basierter Arztpraxisinformationssysteme, sodass auch hier perspektivisch eine Cloud-KIS zu Cloud-APIS-Interoperabilität denkbar ist.

Für die Interoperabilität mit nicht nativen Cloud-Anwendungen muss dann vorausgesetzt werden, dass diese über entsprechende Service-Interfaces verfügen oder aber die Zusammenarbeit klassisch via Messaging auf Basis eines Kommunikationsservers geschieht.

Interoperabilität mit anderen nicht Cloud-basierten Anwendungssystemen

Vor allem mittels der heute üblichen Datenübermittlungen und dafür genutzten Technologien zur Kommunikation von KIS mit anderen externen Legacy-Systemen z.B. zu Zwecken der ambulanten und stationären Abrechnung, Übermittlung von BG-Berichten, Entgegennahme von Laborbefunden via LDT etc. müssen die bisher genutzten Mechanismen in ein mCloud-KIS eingebunden werden können. Ergänzend oder vermutlich für eine Übergangszeit unabdingbar wäre der Betrieb eines Kommunikationsservers analog zur heutigen Situation als integraler Teil des Cloud-KIS. Dieser könnte auch eine wichtige Rolle bei der sukzessiven Migration spielen, zumal Kommunikationsserver heute auch schon Serviceschnittstellen bieten.

Was die Anbindung an die Telematik Infrastruktur anbelangt, muss dann die digitale Identifikation der Einrichtung via Konnektor und SMC-B über den Konnektor, der im Cloud-Servicerechenzentrum installiert sein muss, erfolgen. Kommerzielle Angebote für RZ-Konnektoren gibt es bereits. Sollte aus rechtlichen oder technischen Gründen die Installation des Konnektors vor Ort im Krankenhaus erfolgen müssen, müssen dann auch alle Dienste für die Kommunikation über den Konnektor vor Ort installiert sein.

Interoperabilität mit lokalen Medizintechnik-Geräten

Einer besonderen Anbindung bedürfen Medizingeräte an das Cloud-KIS, da diese im Grunde eigenständige gekapselte Informationssysteme sind, deren Verschiebung in die Cloud nicht möglich ist, wenngleich es Ansätze gibt, Verarbeitungslogik für Medizingeräte ebenfalls in eine Cloud zu legen. Medizingeräte müssen daher vorerst als eigenständig einzubindende On-Premises-Systeme betrachtet werden, für die eine eigene Vor-Ort-Infrastruktur vorzuhalten ist, welche die Interoperabilität mit dem Cloud-KIS ermöglicht. Bezüglich der eigentlichen Anbindung[405] ergeben sich keine Unterschiede zur Einbindung in Legacy-KIS. Auch für Cloud-KIS ist der Einsatz einer Middleware z.B. eines Bus-Systems oder Kommunikationsservers denkbar für

[404] Für die Semantik spezifiziert FHIR die Terminology Module (https://hl7.org/FHIR/terminology-module.html), für Medikamente die Ressource medication (https://hl7.org/FHIR/medication.html).

[405] Tanck/Heinlein, Fusion von Medizintechnik und Informationstechnologie. In Kramme (Hrsg): Medizintechnik; S. 763 – 770.

die Übermittlung des Medizingeräte-Outputs an das Cloud-KIS. Auch sind auf Basis der Forschungsarbeiten des vom BMBF geförderten Projektes OR.NET drei service-orientierte IEEE-Standards entstanden (IEEE 11073 SDC Family), die die Interoperabilität von Medizingeräten normieren und es jedem Hersteller ermöglichen durchkonforme Schnittstellen Implementierungen ihre Geräte einfach einbindbar zu machen.[406] Dabei sollen die Anfragen und Nutzdaten mittels XML kommuniziert werden. Die Herausforderung beim Übergang auf IEE 11073 finden sich in einem Whitepaper von Auriga[407].

Prinzipiell sind zwei Anbindungstypen denkbar: Einerseits eine Asynchronanbindung mit loser Kopplung, das Gerät wird eigenständig betrieben und der Output wird nach Abschluss z.B. der Untersuchung in einem geeigneten Format an das Cloud-KIS übermittelt oder es wird eine direkte Interoperabilität im Sinne einer synchronen Kommunikation zwischen einem Cloud-KIS-Modul und dem Medizingerät notwendig, was dann direkt via TCP/IP-Tunnels erfolgen muss. Dabei befördern Telemedizin- und speziell Telemonitoring-Anwendungen und das Internet der Dinge die Entwicklung spezieller Anbindungen z.B. in Form von speziellen Entwicklungskits oder ganzen Infrastrukturen.

Für ein Cloud-KIS stellt sich mit Blick auf die je nach Anzahl der gleichzeitig betriebenen Geräte und dem damit verbundenen Datenübermittlungsaufkommen die Frage, ob für die Medizingeräte-Einbindungen nicht eine vor-Ort-Infrastruktur z.B. ergänzt um ein lokales Zwischenpuffer-PACS aufgebaut und die Übermittlung der entstandenen Medizinischen Informationsobjekte wie EKGs, EEGs, Sonographiebilder abhängig von der Netzlast in das Cloud-KIS transferiert werden sollte. Alternativ könnten die Ergebnisse auch On-Premise im zentralen Knoten für die Medizintechnikgeräte verbleiben und nur nach Anforderung für die Anzeige transferiert werden.

Gegenüber der Anbindung an Legacy-Systeme ergeben sich bezüglich der fachlichen Interoperabilität keine abweichenden Aspekte und Anforderungen.

Interoperabilität mit der zentralen nationalen Infrastruktur

Gegenüber der Anbindung von Legacy-Systemen an die TI ergeben keine abweichenden Aspekte und Anforderungen für Cloud-KIS. Die Anbindung muss entsprechend mittels eines eHealth-Konnektors erfolgen, der auch beim Provider betrieben werden kann. Dabei muss durch Technisch-organisatorische Maßnahmen sichergestellt sein, dass der institutionelle Identifikationsausweis nicht für missbräuchliche Authentifikationen durch Dritte genutzt werden kann.

Anforderungen an Cloud-KIS:

- Die Interoperabilität zwischen den CMSM eines Cloud-KIS – also die interne Zusammenarbeit von Modulen – sollte wo möglich auf FHIR basieren.
- Ein Cloud-KIS muss auch einen Kommunikationsserver zur Message-basierten Kommunikation mit externen (Legacy-)Systemen beinhalten

[406] Quelle: https://ornet.org/services-2-3/.

[407] Auriga, Medical Device Interoperability with Legacy Systems. Whitepaper. 2020. S. 4 ff.

- Ein Cloud-KIS muss die asynchrone und synchrone Anbindung von Medizingeräten durch entsprechende Services – wo möglich auf Basis etablierter Standards – unterstützen.
- Ein Cloud-KIS muss via eHealth-Konnektor alle für die Kommunikation mit der nationalen TI notwendigen Transaktionen durchführen können.

4.10 Sonstige Aspekte und Anforderungen

4.10.1 Administration/Cloud-Management

Sowohl für Cloud-Provider für die angebotene SaaS -Umgebung als auch für Krankenhäuser für die konkrete Orchestrierung der bezogenen Cloud-KIS-Komponenten stehen vor der Aufgabe, die SaaS-Umgebung zu managen und zu orchestrieren. Wesentliche betriebsbezogene Aufgaben für den Cloud-Provider sind[408]

- Service Deployment bzw. Deployment Management und Überwachung
- Sicherstellung der Integrität der Gesamtumgebung über den gesamten Cloud-Stack hinweg, auch der funktionalen Integrität der SaaS bei (modularen) Softwareupdates jeglicher Art
- Service Orchestration (über den ganzen Cloud-Stack hinweg von den physischen Ressourcen bis zur Microservice-Orchestrierung)
- Cloud Services Management (Vielfältige Aufgaben und Tools, vom Kunden- und Vertragsmanagement über die Abrechnung und das Auditing über Aktivitäten für Konfiguration/Bereitstellung, Hochverfügbarkeitsbetrieb bis zur Sicherstellung von Portabilität und Interoperabilität)
- TOMs für Security
- TOMs für Privacy

Während also der der Provider umfängliche Aufgaben und Maßnahmen mit Blick auf alle Elemente einer Cloud von der Hardware-Ausstattung und Skalierung der Infrastruktur und Plattformen bis zum Deployment- und Patch-Management der Cloud-Anwendungssoftware hat, ist es genau das Ziel von Cloud-SaaS, die Kunden und hier bei Cloud-KIS die Krankenhäuser von aufwendigen technischen Arbeiten zu entlasten und ihnen es zu ermöglichen, sich auf die strategischen und operativen Aspekte des Informationsmanagements in der nutzenden Einrichtung zu kümmern. Dies bedeutet für ein Krankenhaus, dass im Wesentlichen die nachfolgend gelisteten Aufgaben verbleiben, die teils initial sind, teils fortlaufend. So müssen bei Bezug bzw. Freischaltung von zusätzlichen Funktionalitäten auch Berechtigungen angepasst werden.

Für das Krankenhaus verbleiben folgende Arbeiten analog der Einführung von Legacy-Systemen:

- Initiale und eErgänzende Orchestrierung der „bezogenen" Anwendungsumgebung.
- Umfängliche Parametrierung ggf. auch in verfügbaren Community-Repositories
    - Anlage der internen Organisationsstruktur und der Personen.
    - Anpassungen für das Berechtigungsmanagement zur Umsetzung der lokal gültigen Policy (Rollen, Rechte, Rollenzuweisungen etc.).

[408] Liu et al, NIST Cloud Computing Reference Architecture. 2011. S. 7.

    - Durchführung von fachlogischen Parametrierungen (Customizing), die lokale Spezifika berücksichtigen helfen. Dies je nach Granularität für Parameter auf Microservice-, Funktionskomplex, Subsystemebene oder systemweit gültige Parameter.
    - Durchführung von systemtechnischen Parametrierungen (Customizing) für systemtechnische Einstellungen vielfältiger Art.
- Ein-/Anbindung noch lokal betriebener Systeme wie zum Beispiel von Medizintechnikgeräten.
- Orchestrierung der Interoperabilität mit anderen Systemen außerhalb des Krankenhauses, d.h. „Scharfstellen" vorhandener Schnittstellen.
- Entwicklung bzw. Inauftraggabe der Entwicklung von ggf. notwendigen individuellen Schnittstellen oder Service-Modulen.

Für eine einfache und krankenhausspezifische Anwendungssoftware-Orchestrierung bzw. den gewünschten Bezug von Anwendungen und Anwendungsteilen sollten in einer Cloud-SaaS vorgefertigte Sets im Sinne von Modul-Bundles (z.B. Medikationsmanagement") oder ganzer Subsystem-Bundles (z.B. „Radiologieinformationssystem", „PACS", „Pflegeinformationssystem") hinterlegt sein, die dann einfach bezogen werden oder auf einer tieferen Ebene dann weiter profiliert werden können, z.B. durch Zuwahl weiterer optionaler Funktionalitäten. Damit wäre auch gleichzeitig jederzeit eine gute funktionale Transparenz der eingesetzten Cloud-KIS möglich.

Der Bezug von Software würde so durch einfaches Abarbeiten eines hierarchischen Funktionsbaumes – z.B. analog dem HL7-Funktional Model für EHR (siehe Abbildung 4-6) oder dem in Tabelle 4-1 gezeigten beispielhaften Funktionsbaumes – erfolgen, Zu- und Abwahl von Funktionalitäten wären darüber einfach zu handhaben. Dahinter können dann auch entsprechende Abrechnungsmodelle stehen, wobei für horizontale in vielen Bundles vorkommende Funktionen, ein entsprechender kostenreduzierender Ansatz implizit sein sollte, damit eine Funktionalität nicht mehrfach bezahlt werden muss bzw. bei degressiven Kostenmodellen (z.B. bezogen auf Anzahl Nutzer für ein Modul oder Anzahl Transaktionen) die Berechnung dann kumulativ erfolgt.

4.10.2 Compliance-Aspekte

„Unter dem Bereich der Compliance werden alle regulatorischen Themen zusammengefasst, die eine Auswirkung auf die Schutzziele haben können."[409] Die Fraunhofer -Studie nennt hier die Aspekte Datenschutz, gesetzliche Rahmenbedingungen, Risikomanagement und Governance. Der 15-Punkte-Check des BSI für Cloud-Anbieter nennt unter Punkt 13 „Datenschutz und Compliance" die Aspekte Gewährleistung nach deutschem Recht, Speicherung/Verarbeitung in EU/EWR, Garantieverarbeitung in EU/EWR, Einhaltung von gesetzlichen Vorgaben, Einhaltung von Datenschutz Richtlinien und Gesetzen und Kontrollrechte der verantwortlichen Stelle.

Im Grunde geht es um die Durchsetzung aller im Unternehmen bzw. im Krankenhaus spezifizierten Policies und der Einhaltung aller gesetzlichen Rahmenbedingungen, die sich im Grunde

[409] Streitberger, Ruppel: Cloud Computing. Schutzziele. Taxonomie. Markübersicht. 2009. S. 42.

aber auch zum Großteil in den internen Policies niederschlagen müssen. Aber auch die Bedienbarkeit der gesetzlich vorgeschriebenen Datenübertragungen bzw. Interoperabilitätsmechanismen z.B. für die Nutzung der TI und der Belieferung der Anwendungen der TI fallen hierunter. Heute muss konstatiert werden, dass dies nicht immer der Fall ist, dies scheitert zum Teil schon an den wenig ausgeprägten Berechtigungsmechanismen in Legacy-KIS.

Für ein Cloud-KIS ergeben sich bezüglich Compliance keine anderen Anforderungen als für die heute eingesetzten Legacy-Systeme, wobei eine Besonderheit gegebenenfalls darin besteht, dass die SaaS-Angebote und Lösungen mit Blick auf den Betrieb in der Cloud – also bei einem externen Dienstleister – hinsichtlich aller Compliance-Aspekte geprüft und die entsprechenden vertraglichen Vereinbarungen mit dem Auftragsverarbeiter getroffen werden müssen. Gerade bei einer Multi-Cloud-Nutzung betrifft dies dann jeden einzelnen Provider. So kann schon ein nicht ausreichend geschützter HPD in einer außerhalb der Privat- oder Community-Cloud liegenden anderen Cloud zu datenschutzrechtlichen Verletzungen in Bezug auf das darin verwaltete Krankenhauspersonal führen. Gefahren sind z.B.[410]:

- Die Nutzung von Services eines nicht vertrauenswürdigen Providers kann zu Verlust von Unternehmensgeheimnissen oder zu Missbrauch von Endkunden-Daten führen.
- Fehlende Kenntnisse im Bereich Compliance können zu strafrechtlichen Maßnahmen und Strafzahlungen führen.
- Fehlende technische Kenntnisse können dazu führen, dass verschiedene Services genutzt werden, die am Ende wieder nur mit sehr großem Aufwand in die Unternehmenslandschaft integrierbar sind.
- Des Weiteren haben viele Unternehmen in den letzten Jahren Projekte zur Konsolidierung von Hardware und Applikationen gestartet, die unter Umständen durch eine ungesteuerte Cloud-Computing-Nutzung torpediert werden.

Compliance hat im Grunde aber **2 Aspekte**: Die Abbildbarkeit und Durchsetzbarkeit im Cloud-KIS selbst und die Einhaltung durch organisatorische Vorgaben und die personellen Aktionsträger im Krankenhaus aber auch beim Provider. Regelhaftes Verhalten in Bezug auf die Nutzung und Anwendung von IT-Verfahren bedeutet zum einen für die Benutzer, dass sie das KIS bestimmungsgemäß nutzen und zum anderen für die Administratoren, dass sie das KIS bestimmungsgemäß „einrichten", also dort wo durch Parametrierung Compliance-relevante Aspekte angepasst werden können, diese auch entsprechend der Policy vornehmen. Letzteres betrifft vor allem auch die Einrichtung von Schnittstellen zum Datenaustausch zwischen internen und internen mit externen Systemen und die gesamte Parametrierung der Rollen, Rechte und Rollenzuweisungen sowie die personenbezogene Einrichtung von Nutzern.

Heute beim Einsatz von Legacy-Systemen vor Ort muss die Compliance der gesamten Infrastruktur durch das Krankenhaus-IT Personal realisiert werden, was bei Cloud-Lösungen teilweise auch durch den Cloud-Provider auf Basis der Vertragslage geschehen kann.

4.10.3 OH-KIS konforme Mandantentrennung

„Der Begriff „Mandant" oder „Mandantenfähigkeit" wird häufig verwendet, wenn es Unternehmen, Behörden oder Organisationen ermöglicht werden soll, Daten in einer Datenbank logisch

[410] BITKOM, Cloud Computing – Was Entscheider wissen müssen. Leitfaden. S. 25.

zu trennen und zu verwalten. Mit Hilfe der Mandantenfähigkeit können z. B. Daten verschiedener Abteilungen einer Organisation / eines Unternehmens oder verschiedener Kunden eines IT-Services / Rechenzentrums getrennt vorgehalten werden."[411]

In den Anforderungen 32 bis 37 werden in der OH-KIS Gründe und Anforderungen an die Mandantenfähigkeit von KIS dargestellt und es wir deutlich gemacht, dass mandantenübergreifende Zugriffe aus datenschutzrechtlicher Sicht wie Datenübermittlungen angesehen werden müssen. Die Formulierung (hier vor allem Nr. 36) legen nahe, dass jeder Mandant eine eigene physische Datenhaltung hat, denn es heißt „Übermittelte Daten sind in die Primärdokumentation des empfangenden Krankenhauses zu übernehmen. Benutzen übermittelndes und empfangendes Krankenhaus unterschiedliche Mandanten des gleichen KIS, so müssen die übermittelten Daten von dem empfangenden Mandanten in seinen Datenbestand übernommen werden." Manchmal werden aber oft Daten in einer Datenbank gehalten und nur durch ein Mandantenkürzel logisch voneinander getrennt, was aber gegen das Trennungsgebot verstößt.

Mit Blick auf Cloud-KIS ist zuerst einmal eine Mandantentrennung per se in Cloud-Ansätzen enthalten, denn SaaS kann nur funktionieren, wenn Kunden des Betreibers auch eigene Datenbestände nutzen und eine konsequente Datentrennung bzw. Datenisolierung implementiert ist. „Cloud Computing stellt mandantenfähige Services mit hoher Skalierbarkeit bereit. Diese Eigenschaften sind inhärenter Bestandteil der Konzeption von Cloud-Services."[412]

Dabei können prinzipiell die applikationsseitige Trennung, Trennung der Datenhaltung, Trennung der Umgebungen oder mandantenspezifische Verschlüsselung unterschieden werden.[413] Eine applikationsseitige Trennung scheidet dabei eigentlich aus, denn im Grundschutz-Katalog heißt es: „Die Trennung der Datenbestände verschiedener Mandanten darf nicht nur rein applikationsseitig umgesetzt werden, sondern muss nach Möglichkeit durch eine logisch getrennte Datenhaltung mit separaten Datenbank-Accounts für den Zugriff und entsprechend eingeschränkten Berechtigungen unterstützt werden." Prinzipiell bleiben – da die Verschlüsselung additiv ist – im wesentlich also nur zwei Varianten übrig: Die physische Trennung „unterhalb" des entsprechenden CMSM bzw. gesonderte Datenhaltungen unterhalb der Objekttyp-Services oder die Neuinstanziierung jedes CMSM für jeden Mandanten.

Da die Trennung in der Persistenzschicht der Module schon in der Software-Architektur angelegt sein muss, ist also beim Einsatz von SaaS in Privat- oder Community-Clouds zu prüfen, wie die konkrete Mandantentrennung erfolgt. Im Grunde trifft der Aspekt Mandantentrennung nicht nur auf die Datenspeicherung zu, sondern auch auf die Event- und Messagestreams. Die Trennung dieser könnte, um weiter die Skalierbakeit und Performanz einer einzigen Infrastruktur dafür ausnutzen zu können, über kryptographische Verfahren erfolgen.

Ein größeres Problem ergibt sich für mandantenübergreifende Zugriffe, die bei einem „Legacy-Ein-Datenbank-System" leichter zu realisieren sind, denn physisch befinden sich dort die Daten

[411] Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe Mandantenfähigkeit. 2012. S. 2.

[412] BITKOM, Cloud Computing – Was Entscheider wissen müssen. 2019. S. 79.

[413] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzkataloge. 2014. S. 4115.

von Mandanten zumeist in einer Datenbank und werden nur durch ein Mandantenkürzel logisch voneinander getrennt oder stehen zumindest in getrennten, aber strukturgleichen Tabellen. Damit sind mandantenübergreifende Zugriffe oder Auswertungen einfach zu bewerkstelligen. In einem mCloud-KIS, in dem die Daten zu bestimmten Aspekten gekapselt in den Containern der CMSM liegen, aber auch in getrennten Datenbanken, ist dies weniger leicht zu bewerkstelligen, sodass für mandantenübergreifende Aufgaben – z.B. für ein mandantenübergreifendes Data Warehouse, für mandantenübergreifende betriebswirtschaftliche Vorgänge etc. – vermutlich redundante Kopien in einer übergreifenden Instanz geführt werden müssen.

4.10.4 Versions- und Patchmanagement

Versions- und Patchmanagement bzw. die technischen und organisatorischen Maßnahmen und Vorgaben sind bei Cloud-Lösungen Aufgabe des Providers. Im branchenspezifischen Sicherheitsstand B3S „Medizinische Versorgung" werden hierzu die Muss-Anforderungen 131 – 133 angegeben[414]. Diese betreffen den Aspekt der Freigabe von Änderungen an Systemen also Hard- und Software (ANF-MN 131), die vertraglichen Regelungen zur Wartung von Hardware- und Software durch externes Personal (ANF-MN 132) sowie die regelmäßige Überprüfung der Einhaltung der Freigabeprozesse (ANF-MN 133).

Für Hardware- und Betriebssystem-Änderungen bzw. selbstskalierende Systeme kann für Cloud Infrastrukturen bezweifelt werden, dass jede Veränderung gegenüber der Initialinstallation tatsächlich einem Freigabeprozess unterzogen werden kann, dies würde ja bedeuten, dass sogar bei der Allokation neuer Plattenspaces auf anderen Plattenspeichern eine Freigabe erfolgen muss und im Prinzip die Cloud-Idee per se ad absurdum führen. In Teilen kann dies auch für die Anwendungssoftware so gesehen werden, denn in einer skalierbaren, sich selbst überwachenden Infrastruktur mit hoher Patch- und Versionsfrequenz der Microservice-Module erscheint eine manuelle Freigabe jeder Änderung ebenfalls als unrealistisch.

Gegenüber Legacy-Systemen ist ein Deployment bei mCloud-KIS sowohl granularer als auch agiler durchführbar. Die bessere und zeitnahe Deploybarkeit von Patches und Modul-Versionen ist auch eine Motivation zur Entwicklung von Cloud Native Architekturen, Microservices können je nach Bedarf sogar täglich aktualisiert werden. Durch Kohärenz und lose Kopplung treten dabei keine oder nur geringe Nebeneffekte auf, solange die API nicht geändert wird. Daher muss sichergestellt werden, dass ein geupdatetes CMSM konformant ist zu den geltenden Schnittstellenbeschreibungen und im CMSM-Repository eingetragen wird. Hier wird man dann auch die entsprechenden Release-Notes hinterlegen. Heutige Technologien wie z.B. Docker-Container erlauben es, direkt aus den Code-Repositories die Container durchzugenerieren.

4.10.5 Technische Revision

Das Bundesamt für Sicherheit in der Informationstechnik hat 2018 einen speziellen Leitfaden für die IT-Revision herausgegeben. Dieser berücksichtigt auch Anforderungen aus anderen Leitfäden wie z.B.

[414] Bundesamt für Sicherheit in der Informationstechnik, Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. 2013. / Deutsche Krankenhausgesellschaft, Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus. 2019. S. 79 f.

Im vorgenannten Leitfaden heißt es „Bei der IT-Revision stehen die drei Prüfkriterien **Wirtschaftlichkeit** (IT-Prozess, IT-Organisation, Sicherheitsmaßnahmen), **Sicherheit** und **Ordnungsmäßigkeit** (Einhaltung von Rechnungslegungsgrundsätzen wie Vollständigkeit, Richtigkeit, Zeitgerechtigkeit, Nachvollziehbarkeit, Ordnung) gleichwertig nebeneinander. Die Gewichtung dieser drei Ziele bestimmt individuell die Institution bzw. der Revisor und ist abhängig von der Unternehmens- bzw. Behördenstrategie sowie dem konkreten Prüfauftrag."[415]

Daneben wird ausgeführt, dass die IS-Revision darüber hinausgeht und als „neue" Disziplin auf allen Ebenen vor allem den Schwerpunkt auf die ganzheitliche Prüfung der Informationssicherheit vom Aufbau einer Informationssicherheitsorganisation über Personalaspekte bis zur Konfiguration von Systemen betrifft. Auch hierfür ist in wesentlichen Teilen der Provider zuständig.

Bei SaaS ist im Kern die technische IT-Revision und die IS-Revision Aufgabe des Cloud-Providers und Regularien dazu sollten im Auftragsdatenverarbeitungsvertrag zwischen Krankenhaus und Provider festgelegt sein.

Gegebenenfalls sollte ein Krankenhaus oder bei Community-Ansätzen eine Gruppe von Krankenhäusern aber selbst regelmäßig stichprobenartig vor allem die Ordnungsmäßigkeit der Anwendungsverfahren überprüfen, so z.B. auch die Ordnungsmäßigkeit der klinischen Dokumentation und nicht nur die der buchhalterischen Aspekte.

Die Zertifizierung der Cloud-KIS nach vorliegenden Zertifikaten/Katalogen (z.B. OH-KIS, B3S, oder die vertragliche Zusicherung des Providers der dort enthaltenen Anforderungen kann hier gut als Basis für Compliance der gesamten Lösung und stichprobenartige Revision herangezogen werden.

4.10.6 Datenübertragbarkeit

Cloud-Dienste müssen so gestaltet sein, dass der Cloud-Nutzer – hier ein Krankenhaus – seine Unternehmensdaten jederzeit aus der Cloud wieder exportieren kann und damit auch auf andere Systeme migrieren kann (damit kein vendor lock-in!). Der Export sollte dabei in einem selbstbeschreibenden und offenen Format erfolgen. Als Alternativen sind u.a. zu nennen

- Getrennte Export von Informationsschema (z.B. auf Basis des Datenmodellstandards ISO/IEC 11179 Metadata Registry (MDR) oder als XSD) und der Daten selbst (z.B. als EAV-Tripel). Mit den Informationen aus MDR und EAV-Tripeln können dann die Daten wieder in andere Systeme importiert (oder archiviert) werden. Denkbar wäre auch statt EAV ein CSV-Export bzw. als JSON-Strings.
- Export von Modellinformationen und Daten in einem Format, z.B. in Form von XML.
- Export der klinischen Daten wo möglich in Form von FHIR-Ressourcen (also in der Form, wie FHIR-Services Objekte zurückliefern.)
- Nutzung eines branchenspezifischen Standards wie z.B. den CEN ENV 13606 Electronic Healthcare Record Communication, ein teilgenerischer Ansatz, um Aktenstrukturen und Inhalte zwischen Systemen zu kommunizieren.
- Mischformen der o.a. Ansätze, d.h. Nutzung verschiedener Ansätze je nach Objekttypen oder Modul. So könnten für jene klinischen CMSM, denen die Struktur und Semantik

[415] Bundesamt für Sicherheit in der Informationstechnik, Informationssicherheitsrevision. 2018. S. 6.

von FHIR-Ressourcen zugrunde liegt auch FHIR-Service-Antworten z.B. im XML-Format exportieren, alle anderen Module entsprechend einer der anderen o.a. Ansätze.

Letztendlich ist in einer förderativen modularen Umgebung auch denkbar, dass jedes CMSM seine Exportbeschreibung elektronisch ausles- und verarbeitbar im Microservice-Repository mit ablegt und dadurch alle möglichen Ansätze genutzt werden können, wichtig ist nur eine Offenlegung und Basierung auf internationalen Standards. Letztendlich könnte auf Basis dieser Beschreibung ein generisches oder nach Standards modularisiertes Export-Modul implementiert werden, das auf Basis der Angaben im Modul-Repository die Daten aller CMSM-Datenhaltung und/oder der Daten-Services ausliest und in einem Einheitsformat exportiert. Eine Alternative wäre es, bei jeder Objektgenerierung oder -änderung entsprechende Einträge in eine fortgeschriebene EAV-Datenhaltung vorzunehmen, so würde ein Export im Prinzip permanent zur Verfügung stehen. In diesem Sinne können auch Log-Files als Export-Daten interpretiert werden, denn wenn die Logfiles in einem offenen Format zur Verfügung stehen, kann mit ihnen jederzeit der letzte Stand der Datenhaltung rekonstruiert werden.

4.10.7 Migration und Migrationsunterstützung

Für die Migration hin zu Cloud-KIS können zwei Szenarien angegeben werden:

1. Die Migration erfolgt stufenweise im Rahmen der Weiterentwicklung bzw. der Migration von Funktionalitäten des eingesetzten Legacysystems. Hier ist davon auszugehen, dass der Legacy-Hersteller auch im Rahmen der Updates entsprechende Datenmigrationsverfahren mit integriert hat. Der Vorgang wäre analog zu jenem, das heute bei Schemaänderungen der Datenbank üblich ist.
2. Das Krankenhaus wechselt insgesamt auf ein verfügbares Cloud-KIS. Dieses Szenario entspricht dem auch heute schon üblichen Vorgang des Wechsels des Legacy-Systems. Hier spielt dann erst einmal eine ganz wesentliche Rolle, inwieweit und in welcher Form der bisherige Anbieter bzw. seine Lösung einen transparenten Datenexport ermöglicht. Auf der Gegenseite wird es dann ebenso die Frage sein, in welcher Form das Cloud-KIS durch entsprechende Tools und Daten Konvertierungen ein Import von Bestandsdaten unterstützt. Insgesamt hängt eine solche Übernahme unabhängig von welchem System auf welches System gewechselt wird stark von den Schema-Missmatches der unter den Systemen liegenden Datenhaltungen ab.

Für ein cloud KIS bedeutet dies, dass neben einer offenen transparenten Export-Schnittstelle auch eine offene transparente Import-Schnittstelle vorhanden sein muss. Auch hierfür können die im vorangehenden Punkt genannten Alternativen zum Einsatz kommen.

4.10.8 Archivfunktion und Archive

Vor allem im medizinischen Teil eines KIS fallen viele Informationsobjekte an, die für sich gekapselte, in sich geschlossene und aus rechtlicher Sicht nicht mehr änderbare Objekte darstellen. Dies sind die von Medizintechnikgeräten generierten Dateien, die z.B. Biosignale oder aber morphologische Abbildung des Körperinneren repräsentieren, aber auch Fotos z.B. von Wunden, Hautveränderungen etc. und Videos von Sonographien bis hin zu Videos zur Ganganalyse oder aufgezeichnete Operationen und auch Audiodateien kommen vor. Aber auch Textdateien die Befunde repräsentieren, sind wichtige Informationsobjekte, deren unveränderbare Persistierung im KIS wichtig ist. Für alle diese Informationsobjekte sind offene Formate zu nutzen.

Für die medizintechnischen Objekte aber inzwischen auch darüber hinaus hat sich hier das DICOM-Format etabliert, das nicht nur für die Kommunikation und Speicherung von Bildern, sondern auch für Biosignale, Audiodateien aber auch Befunde genutzt werden kann. Neben den Originaldaten ermöglicht das Dicom-Informationsmodell auch integriert die Speicherung umfangreicher Metadaten zum Informationsobjekt in diesem selbst. Hierzu existiert auch ein umfangreiches Attribut-Verzeichnis.

Für Textbefunde und Formulare kann gut CDA genutzt werden oder wo das nicht möglich zumindest ein offenes Dokumentenformat.

Diese für Behandlungen wichtigen Informationsobjekte müssen auch langzeitarchiviert werden und es ist im Interesse der Krankenhäuser, dass die Dauer aus haftungsrechtlichen Gründen weit über die medizinisch verpflichtenden 10 Jahre hinausgeht. Damit ist es evident, dass als Teil bzw. Subsystem eines Cloud-KIS auch ein offenes herstellerneutrales Langzeitarchiv auf Basis von DICOM existiert, dass auch eine revisionssichere Speicherung ermöglicht. Hier gibt es inzwischen ein breites Angebot an DICOM-basierten Archivsystemen mit den entsprechenden Schnittstellen und zunehmend werden diese auch als Cloud-Lösungen angeboten, wobei z.B. Bilder direkt von den Modalitäten hineingeladen werden können oder von einem lokalen PACS aus. Da der Umgang mit DICOM-Objekten servicebasiert ist, können DICOM-Archivlösungen auch gut in die Cloud migriert werden.

Auch für das Langzeitarchiv ergeben sich alle Vorteile bei Cloud-Nutzung, denn Ressourcenallokation und Kosten sind adaptiv, ein Zugriff ist von überall und zu jeder Zeit via Webtechnologie möglich.

Für alle Systeme/Module eines Cloud-KIS, welche medizinische Informationen bzw. Informationsobjekte generieren, besteht daher die Anforderungen, dass diese versehen mit entsprechenden Meta-Informationen über den Storage-Service von DICOM an das Cloud-Archiv übertragen werden. Dabei muss auch in entsprechenden Compliance-Regeln festgelegt werden, welche Informationen und wann diese in das Langzeitarchiv kopiert werden. Mit Blick auf die CMSM, die sehr granulare und oft volatile Informationen verwalten, ist diese Festlegung von besonderer Bedeutung, da ein Zeitpunkt bzw. Event festgelegt werden muss, zu dem diese Informationen direkt oder via bestimmte Aggregationen (z.B. Arztbriefe, Verlaufsprotokolle) in das Archiv wandern.

An zwei Beispielen sei dies verdeutlicht:

- Das CMSM „Diagnosen" beinhaltet alle Algorithmen und die Datenspeicherung der Diagnosen eines stationären Patienten, implementiert also die Diagnosedokumentation. Sollen diese Informationen als justitiables Dokument in das Archiv, sollte dies erst geschehen, wenn keine Änderungen mehr erfolgen. Dies ist in der Regel nach Abschluss des stationären Falles der Fall. Über diese Eventinformation könnte dann das CMSM ein Diagnosedokument generieren (z.B. ein CDA-Dokument entsprechend dem Diagnoseleitfaden von HL7), das – ggf. systemsigniert – in das Archiv gestellt wird. Andererseits werden diese Diagnosen alle auch im Entlassbrief aufgelistet, sodass im Grunde bezüglich der Diagnosen die Archivierung des Entlassbriefes ausreichend sein könnte, zumindest wenn nach Entlassung keine Veränderungen mehr erfolgen. Je nach individueller

Compliance-Regel ist beides oder nur der Entlassbrief in das Langzeitarchiv zu überstellen.

- Für die Dokumentation des Medikationsverlaufes stellt sich dies schwieriger dar, da hier die Volatilität während des stationären Aufenthaltes viel höher ist als bei den Diagnosen. Hier stellt sich die Frage ob – bei gegebener Justitiabilität der Informationen im Cloud-KIS (siehe auch Kapitel 4.8.6) – Medikationsinformationen überhaupt in das Langzeitarchiv überführt werden sollen. Die Medikation bei Entlassung wird regelhaft auch im Entlassbrief stehen, ist also auch damit im Langzeitarchiv. Andererseits ist es aber auch von haftungsrechtlichem Interesse, den Verlauf der Medikation zu archivieren. Natürlich ist dieser über die Daten im Cloud-KIS vorhanden, es bleibt aber die Frage, was bei Migration auf ein anderes System geschieht oder bei Auslagerung und Archivierung der granularen Daten des KIS. Dann sind die haftungsrechtlich relevanten Informationen verteilt auf verschiedene Datenbestände. Wird eine Anforderung nach Archivierung der Medikationshistorie seitens des Krankenhauses formuliert, muss also das entsprechende CMSM in der Lage sein, ein entsprechendes Dokument zu erzeugen und nach Entlassung in das Archiv zu überstellen. Das Beispiel gilt für alle Datenkategorien, deren Historisierung aus Justitiabilitätsgründen von Bedeutung ist.

4.11 Potenziale und Chancen durch Cloud-KIS

4.11.1 Modularisierung und Best of Breed-Ansatz

mCloud-KIS bestehen auf fachlogischer Ebene wie in Kapitel 4.3 ausgeführt aus einer großen Menge von Microservice-Modulen des User Layers, die mittels Interoperabilität auf Serviceschnittstellen- bzw. API-Basis zusammenarbeiten und unter Nutzung von weiteren unterstützenden Softwarebausteinen aus den darunterliegenden Layern ein lauffähiges System ergeben. Ein wesentliches Ziel bei der Entwicklung hin zu mCloud-KIS sollte es sein, dass diese CMSM – zumindest die klinischen Microservice-Module – auf Basis internationaler Standards interoperabel sind und somit auch austauschbar. Gerade ein wesentlicher Aspekt ist es bei den Cloud Native Architekturen, dass durch die hohe Kohäsion und Lose Kopplung der mit anderen Modulen bzw. dem Gesamtsystem überdeckende Kontext minimal ist. Dies führt zu schlanken Schnittstellen und Unabhängigkeit der eigentlichen Funktionalität, die innerhalb von Modulen für den gleichen Zweck dann von Hersteller zu Hersteller differieren können. Im Grunde können die einzelnen CMSM als "KIS-Plugins" betrachtet werden.

Ganz im Sinne eines Best-of-Breed-Ansatzes – der mit Blick auf Kunden individuell ist – besteht damit für ein mCloud-KIS als SaaS die Möglichkeit, dass nicht nur in Bezug auf unterschiedliche Subsysteme aus Angeboten verschiedener Hersteller zurückgegriffen werden kann, sondern, dass sogar für bestimmte Module bzw. Modul-Bundles alternative Implementierung in der mCloud-KIS-SaaS-Umgebung verfügbar sind und bei Orchestrierung bzw. der Zusammenstellung des KIS für ein konkretes Krankenhaus dieses dann aus den bestehenden Alternativen des Cloud-Anbieters wählen kann. Dieser Ansatz kann auf MicroService-Ebene ebenfalls als Best-of-Breed bezeichnet werden. Die Möglichkeiten einer Best-of-Breed Strategie hat positive Auswirkungen auf passgenaue Funktionalität und positive Kosteneffekte.

4.11.2 Förderung von Innovation und Wettbewerb

In der Vergangenheit und auch heute ist es für Softwareunternehmen, die auf Basis spezialisierter Fachkompetenzen bestimmte Module für die Informationsverarbeitung im Krankenhaus herstellen schwierig, einen Marktzugang zu erhalten. Oftmals verursacht die Anbindung an ein Legacy-KIS höhere Kosten, als die Lizenzkosten eines solchen Moduls selbst. Dies reduziert dann die Motivation zur Beschaffung solcher Module bei den Verantwortlichen in Krankenhäusern doch sehr. Modularisierte und offene Architekturen bieten hier neue Perspektiven und Vorteile für Innovation und Wettbewerb:

- Eine CMSM-Architektur z.B. des Kernsystems ermöglicht einfach die Integration von Modulen von Drittanbietern.
- Ein Cloud-KIS selbst ist schon ein softwaretechnisches Öko-System, das so Heimat für viele Ideen, Innovationen und Bausteine sein kann.
- Krankenhäuser können zwischen verschiedenen alternativen Modulen wählen, gute Lösungen setzen sich durch.
- Kleine spezialisierte Unternehmen können innovative Beiträge leisten und haben einen einfacheren Marktzugang.
- Es entsteht Innovation und Wettbewerb in einem bisher ungeahnten Maße im KIS-Bereich.
- Innovationen und Software aber auch Content vor allem im Bereich des Wissensmanagements und der Wissensentwicklung können geteilt bzw. gemeinsam genutzt werden.

4.11.3 Wirtschaftliche Effekte

Die ökonomischen Vorteile von Cloud-Lösungen sind im Grunde Ursprung für die Cloud-Entwicklung. Zu Beginn waren es die Hersteller von großen Legacy-Systemen, die für Ihren weiteren Unternehmenserfolg eine Weiterentwicklung ihrer Produkte hin zu Web-fähigen Cloud-Lösungen aus den in Kapitel 4.2 genannten Gründern forcierten, dann entdeckten auch Bestandskunden dieser Unternehmen die Vorteile ebenso wie nun mögliche Neukunden, denen auch ohne umfangreichen und breiten Skill vor Ort nun die Nutzung von gesamtbetrieblichen integrierten Informationssystemen möglich wurde.

- Passgenauer Bezug von Softwarelandschaften, damit kein „Mitbezahlen" von nicht benötigter Funktionalität.
- Kosten nur für tatsächlich genutzte Module und diese nach Ressourcenverbrauchs- oder Wertschöpfungsmodellen, damit keine hohen Investitionskosten zu Beginn der Nutzung eines Informationssystems.
- Eine Community-Nutzung kann Kosten senken, Mengeneffekt skaliert über mehrere Kunden z.B. Krankenhäuser.
- Interoperabilitätsmodule können als Cloud-Lösung mandantenfähig in einer Community-Cloud betrieben werden, Aufwand für Anpassungen einmalig für alle Nutzer von einem Hersteller sinkt
- Durch responsive-Anwendungen entstehen keine Extra-Kosten mehr für mobile Lösungen, auch müssen diese nicht mehr aufwändig infrastrukturell eingebunden werden.
- Für in einer Community-Cloud gemeinsam genutzte Anwendungen entstehen ggf. auch nur einmalige Pflegekosten, die durch die nutzenden Krankenhäuser geteilt werden können.

- Das lokal vorzuhaltende spezialisierte systemtechnische Know-How kann minimiert werden bzw. wird nicht mehr notwendig.

4.12 Digitale Ökosysteme

Ein digitales Ökosystem ermöglicht es unabhängigen Unternehmen und Personen wie z.B. Kunden dieser Unternehmen aber auch Gruppen von Einzelpersonen unabhängig von Raum und Zeit zu kooperieren. Das Ziel ist dabei, gemeinsamen Nutzen bzw. Mehrwert und gemeinsame Potentiale zu heben und in dieser Kooperation damit besser gemeinsame Ziele zu erreichen und gemeinsame Aufgaben besser abarbeiten zu können. **Im Kern steht dabei eine digitale Plattform**, die mit ihren Funktionalitäten und Interoperabilitätsschnittstellen diese Zusammenarbeit ermöglicht. Solche Gemeinschaften (im Folgenden „Communities" genannt) können regionaler Art, nationaler Art oder sogar weltumspannend sein, man denke an Plattformen wie z.B. eBay, AirBnB, Facebook, Check24, XING, LinkedIn, ResearchGate, Spotify. Allen diesen ist gemeinsam, dass – selbst wenn sie nur von einem Anbieter technisch und verantwortlich als Geschäftsmodell betrieben werden – viele Akteure teilnehmen und wertschöpfend kooperieren. Im Grunde ist zum Großteil der disruptive Charakter von Informatiklösungen mit einhergehenden gesellschaftlichen und wirtschaftlichen Veränderungen durch solche digitalen Ökosysteme verursacht, die eben nicht nur „alte" bestehende Geschäftsmodelle digitale abbilden, sondern auch ganz neue schaffen.

Im Gesundheitswesen geht es dabei im Kern um die optimale Behandlung von Patienten, wobei Behandlungsprozesse sich selten nur in einer Gesundheitsversorgungseinrichtung abspielen, sondern einrichtungsübergreifend sind. In diesem Zusammenhang spielen Krankenhausbehandlungen, die oft eine komplexe Vor- und Nachgeschichte haben, für den Lebensverlauf eines Menschen eine besondere Rolle, denn hier werden Interventionen durchgeführt, die im ambulanten Bereich nicht möglich und die zumeist gravierender Art sind. Während es vor dem Internetzeitalter hieß „All business is local", gilt das zwar für das Geschäftsleben nicht mehr, aber für medizinische Behandlungen zum Großteil – mit Ausnahme ortunabhängig durchführbarer Zweitmeinungen und Konsile – immer noch, denn Patienten werden in einem regionalen Versorgungsnetz behandelt. **Cloud-KIS sind ein wesentlicher Baustein für regionale digitale Ökosysteme im Gesundheitswesen**.

Regionale Communities und regionale digitale Ökosysteme im Gesundheitswesen können daher einen großen Wertbeitrag für eine effektive und einrichtungsübergreifend abgestimmte und hochqualitative Versorgung leisten.

Wesentliche Ziele sind zum einen die Erhöhung der Wertschöpfung der überbetrieblichen Geschäfts- hier Behandlungsprozesse aber auch die Schaffung neuer Prozesse und Geschäftsmodelle und damit neuer Wertschöpfungen und Wertschöpfungsketten. Beispiele für letztgenannte Anwendungen sind die Teleüberwachung von Patienten z.B. nach Herzinfarkt bzw. -operation, spontane und bedarfsgerechte interdisziplinäre Telekonsile und Verfahren wie Teleradiologie, Telepathologie usw.

In vielen Einrichtungen des Gesundheitswesens wird heute digital dokumentiert, viele Arztpraxen führen heute schon keine Papierakte mehr bzw. archivieren in Papier eingegangene Originaldokumente, die aber vorher eingescannt und in die institutionelle elektronische Akte des Patienten eingefügt worden sind. Krankenhäuser sind auf dem Weg, papierlos zu werden. Hier

liegt eine große Chance und viel Potential, schon heute in den Aufbau und den Betrieb von digitalen Ökosystemen im Gesundheitswesen einzusteigen. Die Vorteile sind vielfältig und liegen zum einen in der besseren patientenbezogenen Zusammenarbeit der Einrichtungen, aber auch in der besseren Einbeziehbarkeit des Patienten und im nicht behandlungsbezogenen Bereich in der Ausschöpfung von Potentialen des Aufbaus und der inhaltlichen Pflege von Repositories, die heute jede Einrichtung für sich pflegt und im Krankenhaus oftmals sogar mehrfach im Kernsystem und in den verschiedenen Subsystemen. Ebenfalls von großer Bedeutung ist ein gemeinsames Wissensmanagement zur Pflege und Nutzung medizinscher Prozess- und Dokumentationsstandards und vieler anderer Wissensbausteine, die dann kontextsensitiv innerhalb der institutionellen Systeme genutzt werden können.

Kern eines solchen digitalen Ökosystems muss eine patientenzentrierte Behandlungsmanagementplattform sein auf Basis einer prozessorientierten Patientenakte. Der Anspruch einer optimalen Versorgung – einer multiinstitutionellen und multiprofessionellen „continuity of care" - kann durch das heute fraktionierte Gesundheitssystem mit vielen Spezialisten und Spezialinstitutionen nur wirklich dann auch eingelöst werden, wenn alle Mitglieder des Behandlungsteams eines Patienten zeitnah und sachgerecht wissen bzw. in Erfahrungen bringen können: Was war, was ist, was soll sein? Und wenn eine auch prospektive Behandlungssteuerung einrichtungsübergreifend möglich ist. Dies betrifft auch die Schnittstellen zwischen den Sektoren und zumindest können digitale Ökosysteme helfen, die Sektorengrenzen zu überwinden – ein seit 25 Jahren formuliertes, aber nie erreichtes politisches Ziel.

Eine solche Behandlungsmanagementplattform motivierende Kernaussagen sind z.B.[416]

Kernaussage 1:

Die derzeitige fraktionierte Organisationsform des Gesundheitswesens verhindert optimale Qualität, Wirtschaftlichkeit und Patientensicherheit.

Kernaussage 2:

Für die Qualität und Wirtschaftlichkeit der Versorgung z.B. von Langzeitkranken, Schwerkranken oder multimorbiden Patienten ist eine für die aktuelle Entscheidungs- und Behandlungssituation ausreichende Informationstransparenz der individuellen Situation des Patienten unabdingbar.

Kernaussage 9:

Alle Ansätze einer integrierten sektorübergreifenden Versorgung können ohne den Einsatz gemeinsamer IT-gestützte einrichtungsübergreifender EPA-Systeme nicht effektiv funktionieren.

Kernaussage 13:

Hauptziel einer eEPA ist es, dass es in einem fraktionierten Gesundheitssystem möglich ist, dass alle Behandler eines Patienten zu jeder Entscheidungs- und Behandlungssituation die notwendigen Informationen zu Vorgeschichte, Ist-Situation und geplanten Maßnahmen abrufen und

[416] Haas: Elektronische Patientenakten. Einrichtungsübergreifende Elektronische Patientenakten als Basis für integrierte patientenzentrierte Behandlungsmanagement-Plattformen.

eigene neue Informationen in die patientenbezogene Informationssammlung einstellen können.

Kernaussage 14:

eEPA-Systeme die nur Informationen verwalten, zielen zu kurz, sie müssen eine gesamtheitliche Unterstützung von Patienten und Behandlern ermöglichen – ggf. indikationsspezifisch ausgeprägt.

Kernaussage 13:

Hauptziel einer eEPA ist es, dass es in einem fraktionierten Gesundheitssystem möglich ist, dass alle Behandler eines Patienten zu jeder Entscheidungs- und Behandlungssituation die notwendigen Informationen zu Vorgeschichte, Ist-Situation und geplanten Maßnahmen abrufen und eigene neue Informationen in die patientenbezogene Informationssammlung einstellen können.

Wertebeiträge digitaler Ökosysteme im Gesundheitswesen sind z.B.:

- Zeitnahe und vollständig Patienten-Behandlungsinformationen für alle an konkreten Behandlungen beteiligte Einrichtungen.
- Verbesserung der multiprofessionellen Zusammenarbeit.
- Verbesserung der Patientensicherheit einrichtungsübergreifender Versorgungsprozesse.
- Vermeidung von Doppeluntersuchungen und unnötige Folgekosten.
- Einsatzmöglichkeit individualisierter klinischer Pfade für die einrichtungsübergreifende Versorgung.
- Möglichkeit der Patientenpartizipation und Stärkung der Patientensouveränität.
- Bruchlose Integration von Telemedizinverfahren.
- Bessere Rechtzeitigkeit und Angemessenheit von Interventionen.
- Die erleichterte Einholung von Zweitmeinungen.
- Je nach Patientenzustimmung Datennutzung für Forschung und neuen Wissensgewinn.
- Gemeinsames Wissensmanagement.
- Gemeinsame Pflege von Repositories.
- Gemeinsame Inanspruchnahme von Servicedienstleistern verschiedenster Art.
- Verbesserung von Bestell- und Lieferketten.

Dabei können für die gemeinsame Behandlungsmanagementplattform die gleichen API-Spezifikationen genutzt werden, wie intern für die Microservice-Module des Cloud-KIS, denn Einfügen und Abruf klinischer Daten ist unabhängig von der Lokalisierung und Nutzung der Daten

Eine bespielhafte fachlogische Ausprägung eines solchen Digitalen Ökosystems zeigt nachfolgende Abbildung.

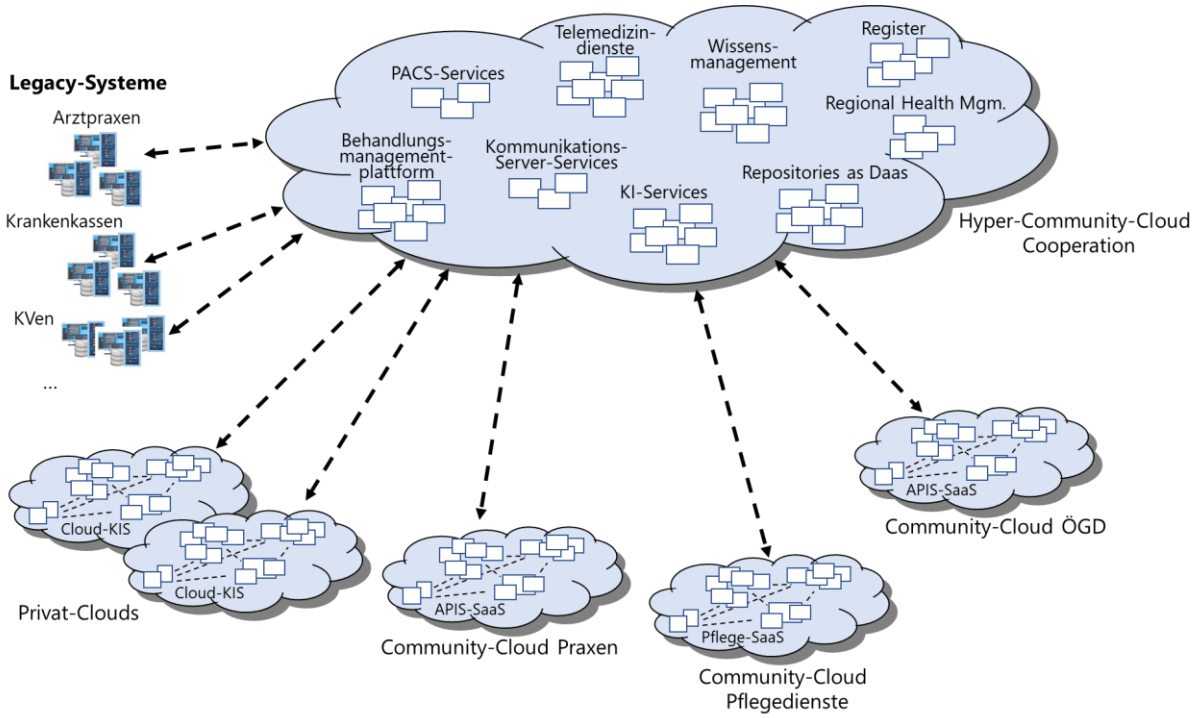

Abbildung 4-22: Digitales Ökosystem und Cloud-KIS

5 Vereinbarkeit von Recht und Technik

5.1 Einführung

Schon Hippokrates wusste um die Bedeutung der Geheimhaltung von medizinischen Informationen über Patienten, um diesen nicht zu schaden. Und schon zu jener Zeit wurden bereits – wenn auch nicht für die medizinische Dokumentation – Verfahren für die Geheimhaltung von Nachrichten und Aufzeichnungen vor allem für den politischen und militärischen Bereich entwickelt und eingesetzt. Beide Bemühungen wurden bis heute fortgesetzt und sind in der digitalen Welt aktueller denn je. Die Sicherstellung der ärztlichen Schweigepflicht und technisch-organisatorische Maßnahmen zum Schutz von Patientendaten vor unbefugter Einsichtnahme und Nutzung sind zentrale Themen der Medizinischen Informatik. Und so sollen heute einerseits die vielen positiven Effekte des Einsatzes digitaler Verfahren in der Medizin voll ausgeschöpft werden, andererseits darf dabei aber kein Schaden für Betroffene – auch nicht für den behandelnden Arzt – durch eine Offenlegung resultieren. In diesem Zusammenhang wird auch diskutiert, ob medizinische Daten nicht ebenso personenbezogene Daten über den Arzt sind, enthalten sie doch Informationen über sein Wissen und Können und sein Handeln.[417]

Unabhängig möglicher Lösungen ist die führende Größe immer das rechtlich Erlaubte und technische Maßnahmen müssen hier die Compliance sicherstellen. Wenn aber praktikable Lösungen zum Einsatz kommen sollen, führt dies immer zu der Frage nach der Vereinbarkeit von Recht und Technik, nicht nur, aber auch mit Blick auf die Benutzbarkeit der Anwendungssoftware. In einer Grenzwertbetrachtung gibt es fast immer eine technische Lösung, um das rechtlich Erlaubte umzusetzen. Das Konzept Datenschutz durch Technik wird geleitet durch den Gedanken: Wenn Datenschutzgefahren und -verletzungen faktisch nicht möglich sind, muss die Verarbeitung nicht rechtlich verboten werden bzw. ist erlaubt. Andererseits kann eine ausufernde technische Absicherung, die dann oft zu einer nicht mehr praktikablen Nutzbarkeit führt, eventuell durch vertragliche Reglungen und organisatorische Maßnahmen substituiert werden. So schreibt das Bundeswirtschaftsministerium in seiner Orientierungshilfe zum Gesundheitsdatenschutz: „Anders liegt die Sache, wenn sich ein Unternehmen bei der Verarbeitung von Gesundheitsdaten von spezialisierten (technischen) Dienstleistern unterstützen lässt. Das kann insbesondere der Fall bei der Nutzung von Cloud-Diensten sein. Für eine solche Datenverarbeitung durch Dienstleister sieht die DSGVO gewisse Privilegierungen und Ausnahmen von den strengen Voraussetzungen für den Austausch von Gesundheitsdaten mit anderen Unternehmen vor. Um in den Genuss dieser Erleichterungen zu kommen, muss der Dienstleister

[417] Soweit in den medizinischen Daten auch Ärzte genannt werden, bspw. als Urheber von Diagnosen o.Ä. (was im Sinne der Authentizität der Fall sein sollte), stellen diese auch personenbezogene Daten der Ärzte (oder anderen behandelnden Personals, das benannt wird) dar und sind grundsätzlich geschützt. Beim Schutzbedarf ist allerdings zu beachten, dass die Ärzte i.d.R. nicht in ihrer persönlichen Gesundheit von diesen Daten betroffen und damit nicht im gleichen Ausmaß wie die Patienten geschützt sind. Gerade die Patienten können auch über legitime Interessen an einer Offenlegung von Informationen über Wissen, Können und Handeln der Ärzte verfügen.

als weisungsgebundener Auftragsverarbeiter unter Beachtung bestimmter Vorgaben beauftragt werden."[418] Hier können also unter gewissen Umständen durch bestimmte Vertragsformen ansonsten notwendige sehr aufwändige technische Maßnahmen, die den Einsatz einer Lösung gegebenenfalls nicht praktikabel machen würden, entfallen.

Die Balancierung notwendiger, aus rechtlichen Rahmenbedingungen resultierenden technisch-organisatorischer Schutzmaßnahmen und der Benutzbarkeit der Anwendung bleibt in der modernen Informationsgesellschaft eine Herausforderung. Zum einen führen Schutzmechanismen im Extremfall den faktischen Einsatz einer Anwendung ad absurdum, wenn die technischen Maßnahmen letztendlich zu einem für den Anwender nicht mehr akzeptabel nutzbaren System führen. Zum anderen erfordern höhere Schutzmaßnahmen auch höhere Kosten, die oftmals durch das Management nicht genehmigt werden. An einem praktischen Beispiel der Benutzerauthentifikation – die im Grunde aus rechtlichen Gründen unabdingbar ist – sei dies verdeutlicht: Im klinischen Alltag und bei ubiquitärer Nutzung des KIS wird ein sehr häufiges Ein- und Ausloggen notwendig. Dieser Vorgang selbst dauert oft länger als der fachliche Vorgang, z.B. wenn nur der Blutdruck in das KIS eingetragen werden soll. Also bleibt oft einfach der erste Benutzer mit seinem am Morgen des Tages getätigten Login ohne Logout erhalten und alle können schnell und effektiv auf "Rechnung" dieses Benutzers das KIS benutzen; unter einer Kennung, die tagsüber keiner mehr wahrnimmt oder ändert. Zurechenbarkeit und Berechtigungsprüfung sind faktisch außer Kraft gesetzt. Oder es wird gleich mit sogenannten Gruppenkennungen gearbeitet, was für die Justitiabilität und vor allem Zurechenbarkeit noch problematischer ist, denn sie ist praktisch nicht mehr gegeben. Als Maßnahme könnte ein automatischer Logout erfolgen, wobei das Zeitfenster klein genug sein muss, damit nicht der Nächste noch unter der vorigen Kennung weiterarbeitet. Also wird z.B. nach 30 Sekunden der Nichttätigkeit ausgeloggt. Auch das wäre für die Arbeit mit dem System in der Regel kontraproduktiv. Nun könnte man ergänzend noch eine 2-Faktor-Authentifikaiton einführen. Dann wäre das Erzwingen einer sicheren Authentifikation in Verbindung mit automatischem Logout vermutlich am sichersten. Jeder der den Betrieb auf einer Pflegestation kennt, wird an einer Durchsetzbarkeit zweifeln. So zeigt sich, dass zwar ausreichende technische Mechanismen vorhanden sind, diese aber nicht alltagstauglich und zu personalkostenintensiv sind. Andere Verfahren wie sensorgestützte Benutzererkennung oder biometrische Verfahren oder Kombinationen sind ebenfalls denkbar, aber jedenfalls von der Erstinvestition her kostenintensiv und müssten in die KIS-Anwendung so integriert werden, dass Login-/Logout damit auf Anwendungsebene möglich ist.

5.2 Rechtliche Anforderungen und Herausforderungen

Die rechtlichen Anforderungen und daraus resultierende Herausforderungen für Cloud-basierte KIS in Deutschland ergeben sich primär aus den in Kapitel 3 dargestellten europäischen und nationalen Datenschutzvorschriften sowie der ärztlichen Schweigepflicht.

[418] BMWi, Orientierungshilfe zum Gesundheitsdatenschutz. 2018. S. 3.

5.2.1 Herausforderungen durch unterschiedliche Anforderungen der Landeskrankenhausgesetze

Wie in Kapitel 3 bereits umfangreich ausgeführt, ergibt sich bei der Betrachtung der relevanten Datenschutzvorschriften für Krankenhäuser in Deutschland ein stark heterogenes Bild. Neben den direkt oder subsidiär anwendbaren Bestimmungen der DSGVO und des BDSG bzgl. des Umgangs mit personenbezogenen Daten im Allgemeinen und Patientendaten als besonders schutzbedürftigen Daten im Besonderen, treffen die LKHG und LDSG der Bundesländer vielfach – im Rahmen der Öffnungsklauseln der DSGVO – vorrangig anzuwendende, strengere Regelungen. Dies gilt insbesondere auch für die Verarbeitung solcher Daten im Auftrag, also das Outsourcing der Datenverarbeitung an Dienstleister wie etwa Cloud-Anbieter.

Inwieweit und unter welchen Voraussetzungen die Verarbeitung von Patientendaten outgesourct werden darf, geht dabei bundeslandspezifisch weit auseinander von praktisch überhaupt nicht bis hin zur „bloßen" Geltung der Anforderungen der DSGVO. Letzteres trifft zum Beispiel auf Hamburg zu. In Bayern ist dagegen die Verarbeitung von Patientendaten zu medizinischen Zwecken grundsätzlich nur im Krankenhaus selbst oder aber durch ein anderes Krankenhaus im Auftrag erlaubt. Damit ist insoweit der Einsatz eines spezialisierten Cloud-Anbieters als Auftragsverarbeiter des Krankenhauses in diesem Bundesland ausgeschlossen. Von dieser strengen Regelung ausgenommen sind lediglich solche Verarbeitungsvorgänge bzw. Patientendaten, die zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten (insbes. Abrechnung) erforderlich sind. Diese Ausnahme kann jedenfalls nicht alle denkbaren Module oder Subsysteme eines KIS abdecken, sondern lediglich Aspekte der administrativen Kernsysteme.

Eine komprimierte Aufstellung der unterschiedlichen Anforderungen der Bundesländer findet sich in Tabelle 3-2, eine erste grafische Übersicht in Abbildung 3-2.[419]

Solche teils sehr restriktiven länderspezifischen Vorschriften schließen nach heutigem rechtlichem und technischem Stand die Einschaltung eines Cloud-Anbieters für die krankenhausexterne Verarbeitung von Patientendaten in manchen Bundesländern aus. Darüber hinaus wird die bundeslandübergreifende Umsetzung von Krankenhaus-IT-Strategien und die Vernetzung von Krankenhäusern – was insbesondere im wirtschaftlichen Interesse von Krankenhausketten liegt – in verschiedenen Bundesländern durch den regulatorischen „Flickenteppich" stark erschwert.

Wenn jedoch vermieden wird, dass die outgesourcten Patientendaten für den Auftragsverarbeiter personenbezogen sind, zum Beispiel durch eine effektive Ende-zu-Ende-Verschlüsselung oder Pseudonymisierung im Krankenhaus, dann ist es vertretbar diese besonderen Vorschriften zur Auftragsverarbeitung nicht anzuwenden.[420] Es blieben auch dann zwar Restrisiken für den Datenschutz bestehen, nämlich durch die praktisch immer denkbare Möglichkeit verschlüsselte Daten auch ohne Schlüssel über kryptoanalytische Angriffe zu entschlüsseln oder pseudonymisierte Daten durch Abgleich mit anderen Datenbeständen zu reidentifizieren. Diesen müsste zumindest nach Art. 32 DSGVO durch andere technische und organisatorische

[419] Siehe vorne Kap. 3.4.18, S. 158 ff.

[420] Die Relativität des Personenbezuges vorausgesetzt.

Maßnahmen einschließlich vertraglicher Verpflichtungen des Auftragnehmers begegnet werden, ohne dass dies zwingend als Auftragsverarbeitung eingeordnet werden müsste.[421]

In vielen Bundesländern mit Ausnahme der in der Übersichtsgrafik 3-2 mit roter Ampel markierten Länder (Bayern, Mecklenburg-Vorpommern, Nordrhein-Westfalen und Saarland) wird man jedoch auch ohne solche sehr weitgehenden technischen Maßnahmen zum Ausschluss des Personenbezuges mit den ansonsten für die Verarbeitung von Patientendaten in der Cloud risikoangemessenen technischen und organisatorischen Maßnahmen grundsätzlich ein Cloud-KIS betreiben können. Dabei sind in vielen Bundesländer jedoch gewisse Zusatzvoraussetzungen zu erfüllen, wie beispielsweise die Genehmigung durch die Aufsichtsbehörde oder zumindest eine Anzeige an diese, was im Einzelfall zu prüfen ist, aber die Nutzung von Cloud-KIS nicht generell unmöglich macht.

5.2.2 Herausforderungen durch zusätzliche Anforderungen bei einem Bezug der Auftragsverarbeitung zu unsicheren Drittstaaten

Ein Blick auf den internationalen Cloud-Markt zeigt, dass die größten Anbieter in diesem Bereich Stand heute US-amerikanische Unternehmen sind. Aus datenschutzrechtlicher Sicht bringt dies Probleme mit sich.

So bestehen bereits nach der DSGVO besondere Anforderungen an die Übermittlung personenbezogener Daten in Länder außerhalb des Anwendungsbereichs der Verordnung, also außerhalb des EWR. Dabei ist neben der stets erforderlichen Rechtsgrundlage für die eigentliche Verarbeitungshandlung zusätzlich die Sicherstellung eines angemessenen Schutzniveaus für die personenbezogenen Daten in dem Land, in das sie übermittelt werden sollen, erforderlich. Weitgehend unproblematisch ist dies für diejenigen Länder, für die ein sog. Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 DSGVO besteht.

Bis zum 16. Juli 2020 bestand mit dem EU-US Privacy Shield in Teilen auch ein solcher Angemessenheitsbeschluss für die USA, nämlich für diejenigen Unternehmen in den USA, die sich freiwillig selbst zur Einhaltung der in diesem Beschluss genannten Bedingungen verpflichtet haben, sowie sich in ein entsprechendes Verzeichnis beim US-Handelsministerium haben eintragen lassen. Diesen Beschluss hat der EuGH in seiner "Schrems II"-Entscheidung jedoch mit sofortiger Wirkung für ungültig erklärt. Begründet wurde dies in erster Linie mit aus europäischer Sicht zu weitgehenden und rechtsstaatlich zu wenig kontrollierbaren Zugriffsbefugnissen der US-Behörden, insbesondere der dortigen Geheimdienste. Alle auf das Privacy Shield gestützten Datenübermittlungen in die USA sind somit seit Mitte Juli rechtswidrig. Das allein hätte wohl eine überschaubarere Tragweite, da ein Großteil der betroffenen Unternehmen seine Datentransfers in die USA nicht (allein) durch das Privacy Shield, sondern durch EU-Standardvertragsklauseln (Standard Contractual Clauses – SCC) zur Auftragsverarbeitung nach Art. 46 Abs. 2 Buchst. c DSGVO abgesichert hat oder dies jedenfalls könnte.

Jedoch hat "Schrems II" auch Auswirkungen auf die Verwendung der Standardvertragsklauseln. So hat der EuGH in seiner Entscheidung klargestellt, dass diese Klauseln zwar grundsätzlich

[421] Auch in diesen Fällen bietet sich aber der vorsorgliche Abschluss einer Vereinbarung über die Auftragsverarbeitung an, auch wenn nicht unbedingt alle ergänzenden landesrechtlichen Zulässigkeitsvoraussetzungen für eine solche Auftragsverarbeitung erfüllt sein müssen.

ihre Gültigkeit behalten, diese allein aber nicht zwingend zur Sicherstellung eines angemessenen Datenschutzniveaus beim Empfänger im Drittland ausreichen, gerade wenn das Datenschutzniveau aufgrund staatlicher Zugriffsbefugnisse dort aus EU-Sicht nicht ausreichend ist. Vielmehr muss das übermittelnde Unternehmen für jeden seiner Auftragsverarbeiter in einem unsicheren Drittland prüfen und ggf. durch zusätzliche Maßnahmen sicherstellen, dass ein angemessenes Schutzniveau besteht.

Nach Auffassung des Europäischen Datenschutzausschusses (EDSA) können die zu ergreifenden Maßnahmen technischer, vertraglicher und organisatorischer Art sein. Der EDSA stellt jedoch auch fest, dass vertragliche oder organisatorische Maßnahmen nicht ausreichen, wenn das Datenschutzniveau im Drittland deshalb nicht angemessen ist, weil für staatliche Behörden dort aus europäischer Sicht zu weitgehende Zugriffsbefugnisse gewährt werden. Denn diese Behörden wären nicht an Verträge zwischen Auftraggeber (wie einem Krankenhaus) und Auftragsverarbeiter gebunden und könnten organisatorische Sicherung bei Letzterem auch umgehen. In diesen Fällen seien vorab in der Hand des Auftraggebers liegende technische Maßnahmen wie bspw. die Pseudonymisierung oder Verschlüsselung anzuwenden[422]. Dadurch ließe sich, zumindest für gewisse Anwendungssituationen ein angemessenes Datenschutzniveau gewährleisten und ein Zugriff durch Behörden im Drittland effektiv vermeiden. Der EDSA stellt allerdings auch klar, dass für andere Konstellationen nach heutigem rechtlichem und technischem Stand keine ausreichenden zusätzlichen Maßnahmen getroffen werden könnten, um einen DSGVO-konformen Datentransfer zu ermöglichen[423]. Dies sei insbesondere dann der Fall, wenn der Auftragsverarbeiter zur Erfüllung seiner Aufgaben Zugriff auf Klartextdaten benötigt.

Der EDSA hat zu einer offiziellen Kommentierung seiner Empfehlungen aufgerufen, welche bis Ende November 2020 möglich war. In den Stellungnahmen wurde deutliche Kritik unter anderem dahingehend vorgetragen, dass die strikte Haltung des EDSA im Hinblick auf unsichere Drittstaaten wie die USA mit der Notwendigkeit im Grunde genommen durch technische Maßnahmen den Personenbezug auszuschließen oder massiv zu reduzieren, keineswegs in allen Fällen risikoadäquat sei. Ob der EDSA dieser Kritik zumindest teilweise entgegenkommt, kann derzeit nicht prognostiziert werden. Vor diesem Hintergrund ist es der rechtlich sicherste Weg, sich an diese Empfehlungen zu halten. Gerade bei Patientendaten, die nach deutschem Recht einem besonderen Beschlagnahmeschutz unterliegen, der auch deren Schutzbedarf definiert, wird eine abweichende Auffassung schwer zu vertreten sein. Insofern müsste auch insoweit auf eine vom Krankenhaus vorgenommenen Ende-zu-Ende-Verschlüsselung oder eine effektive Pseudonymisierung im Krankenhaus vor Export gesetzt werden. Alternativ oder ergänzend kann man auch an Methoden der Secure Multi Party Computation denken, welche ebenfalls verhindern müssten, dass Patientendaten im Klartext in unsichere Drittstaaten gelangen.

Um eine Datenübermittlung in unsichere Drittstaaten und insbesondere die USA zu vermeiden, bieten viele Cloud-Anbieter bereits eigene, in der EU lokalisierte Server an. Auch wenn eine solche Lokalisierung der zu verarbeitenden personenbezogenen Daten vorliegend jedenfalls gegenüber einer Drittlandübermittlung zu bevorzugen ist, kann sie datenschutzrechtliche Bedenken nach strenger Auslegung nicht gänzlich ausräumen.

[422] EDSA Recommendations 01/2020 S. 22 f.

[423] EDSA Recommendations 01/2020 S. 26 f.

Wie bereits ausgeführt, spielen US-amerikanische Unternehmen im Cloud-Bereich eine überragend wichtige Rolle. Diese Unternehmen sowie auch mit ihnen verbundene Unternehmen, auch solche mit Sitz in der EU, unterfallen in der Regel zumindest auch US-amerikanischem Recht und damit dem U.S. CLOUD-Act. Dieses Gesetz ermächtigt US-Behörden, von Unternehmen mit US-Bezug die Offenlegung von bei ihnen gespeicherten Daten zu verlangen, unabhängig davon, wo diese Daten gespeichert werden. Dadurch sind auch auf in der EU lokalisierten Servern gespeicherte personenbezogene Daten nicht zwangsläufig ausreichend vor einem Zugriff durch US-Behörden geschützt. Die betroffenen Unternehmen befinden sich in einem Spannungsfeld zwischen der Einhaltung von US-Vorschriften auf der einen Seite und von DSGVO sowie Vorschriften der EU-Mitgliedstaaten auf der anderen Seite. Es ist deshalb auch in diesem Fall zumindest zu empfehlen, wenn nicht gar erforderlich, auch bei der Verwendung von EU-Servern solcher Anbieter zusätzliche technische Sicherungsmaßnahmen zu ergreifen.

Eine Lösung des genannten Konflikts kann gegebenenfalls durch ein Treuhandmodell erreicht werden, bei dem neben einem US-Cloud-Anbieter ein EU-Unternehmen als Datentreuhänder eingesetzt wird.[424]

5.2.3 Herausforderungen durch die Schweigepflicht der Heilberufe

Neben den genannten datenschutzrechtlichen Herausforderungen kann die Übermittlung von Patientendaten auch eine Verletzung der ärztlichen Schweigepflicht bzw. von Privatgeheimnissen nach § 203 StGB darstellen und somit strafrechtliche Relevanz haben. Auch an dieser Stelle ergeben sich also Herausforderungen für den Betrieb eines Cloud-KIS.

Ähnlich der datenschutzrechtlichen Erlaubnistatbestände nach Art. 6 Abs. 1 und Art. 9 Abs. 2 DSGVO bedarf es bzgl. der Schweigepflicht einer Befugnis zum Offenbaren von Patientendaten, denn unbefugtes Offenbaren ist strafbar. Eine Befugnis durch die freiwillige Entbindung von der Schweigepflicht seitens der Patienten scheidet im Rahmen eines Cloud-KIS mangels Praktikabilität aus. Einige Landeskrankenhausgesetze enthalten eine gesetzliche Offenbarungsbefugnis, womit sich die Voraussetzungen auch im Hinblick auf die Schweigepflicht primär nach diesen richten.

Soweit, wie beispielsweise in Hamburg, im LKHG jedoch keine Regelung zur Auftragsverarbeitung und damit keine Offenbarungsbefugnis enthalten ist, muss auf die Befugnis zum Offenbaren gegenüber sonstigen mitwirkenden Personen nach § 203 Abs. 3 Satz 2 StGB zurückgegriffen werden. Auch Cloud-Anbieter können unter den Begriff der sonstigen mitwirkenden Personen gefasst werden. Die eben genannte Befugnis setzt jedoch voraus, dass ein Offenbaren nur insoweit erfolgt, als es für die Tätigkeit dieser mitwirkenden Person erforderlich ist, die Mitwirkung also ohne ein Offenbaren nicht möglich wäre. Nach der hier vertretenen Auffassung ist dabei auf den Maßstab der „relativen Unmöglichkeit" bzw. groben Unverhältnismäßigkeit abzustellen, der neben technischen in gewissem Rahmen auch wirtschaftliche Aspekte berücksichtigt. Soweit möglich und praktikabel, wenn auch mit einigem, aber nicht vollkommen unvertretbarem Aufwand, muss vor diesem Hintergrund gleichwohl eine Ende-zu-Ende-Verschlüsselung und/oder effektive Pseudonymisierung erfolgen.[425] Bei einzelnen KIS-Modulen

[424] Näheres siehe dazu unten Kap. 6.3.2, S. 289 f.

[425] Zu diesem Maßstab der „relativen Unmöglichkeit" bzw. groben Unverhältnismäßigkeit s. oben S. 73, Fn. 154.

bzw. -Add-ons in der Cloud dürfte dies häufig praktikabel sein, wie beispielsweise für die radiologische Bildarchivierung (PACS), wo Ende-zu-Ende-Verschlüsselung eingesetzt werden kann und eingesetzt wird, oder auch Hilfen bei der Erstellung von Befundtexten, wo Pseudonymisierung möglich und praktikabel ist. Bei einem Cloud-native-KIS wären diese technischen Maßnahmen jedoch nicht möglich, damit aber auch trotz verschärfter Erforderlichkeitsprüfung wohl nicht notwendig, wenn sich ein Krankenhaus dazu entscheidet die kompletten Tätigkeiten rund um Betrieb und Wartung eines KIS in die Cloud auszulagern und vor Ort nur noch Browser als Thin Clients einsetzen möchte. Des Weiteren muss die mitwirkende Person gemäß § 203 Abs. 4 StGB zur strafbewährten Verschwiegenheit verpflichtet werden, was rechtsgeschäftlich zu bewerkstelligen ist, somit praktikabel erscheint und jedenfalls in Deutschland auch strafrechtliche Wirkung entfaltet.

5.2.4 Herausforderungen bzgl. der Übermittlung von Leistungsdaten nach dem SGB V

Die Übermittlung von Patientendaten durch ein Krankenhaus an einen Cloud-Anbieter unterfällt zudem dem Schutz von Leistungsdaten nach dem SGB V. Anders als in den SGB I und X, die bzgl. des Schutzes von Sozialdaten nur Leistungsträger adressieren, sind von den Regelungen des SGB V auch Krankenhäuser als Leistungserbringer erfasst. Allerdings erscheinen die Regelungen des SGB V bzgl. der Auftragsverarbeitung unsystematisch und unvollständig. So sind in den §§ 295a ff. des Gesetzes verschiedene Abrechnungsszenarien und die Zuhilfenahme von Rechenzentren durch bestimmte Leistungserbringer erfasst. Jedoch enthält § 301 SGB V, der die Abrechnung durch Krankenhäuser regelt, gerade keine Ausführungen zur Auftragsverarbeitung. Daher liegt es im Umkehrschluss nicht ganz fern, dass sich Krankenhäuser bei der Abrechnung keiner Auftragsverarbeiter bedienen dürfen. Dem lässt sich zwar das Argument entgegenhalten, dass die vollständige Auslagerung eines KIS in die Cloud nicht gezielt und allein der Übermittlung von Leistungsdaten in die Cloud dient und es sich somit nicht um eine reine Abrechnungsstelle handelt. In rechtspolitischer Hinsicht bietet sich insoweit jedoch zumindest eine Klarstellung bzw. eine klare Regelung an, welche die Einschaltung von Auftragsverarbeitern auch insoweit, wenn auch gegebenenfalls unter Bedingungen, erlaubt.[426]

5.3 Resultierende technische Herausforderungen und Umsetzungsmöglichkeiten

5.3.1 Anonymisierung, Pseudonymisierung oder Verschlüsselung

Die Verarbeitung von personenbezogenen Daten durch ein Cloud-KIS insgesamt oder in Teilen setzt zuerst einmal Voraus, dass ein Erlaubnistatbestand für die Verarbeitung existiert. Dies dürfte für ein KIS, wie es heute oft vor Ort betrieben wird der Fall sein, entsprechende Zustimmungsklauseln sind in jedem Krankenhaus-Aufnahme- und Behandlungsvertrag enthalten. Die Formulierungen zielen hier jedoch nur auf die prinzipielle Verarbeitung und die Weitergabe zu Zwecken der Abrechnung oder Mitbehandlung ab, z.B. wenn externe Labore oder Radiologieinstitute mitgenutzt werden. Die Besonderheit des Cloud-KIS liegt also in dessen Betrieb in einer externen skalierbaren Infrastruktur eines Cloud-Betreibers.

[426] Siehe dazu unten Kap. 6.1.2, S. 282.

Die Verarbeitung personenbezogener Daten bei einem Cloud-Betreiber setzt zumindest unabhängig weiterer Betrachtungen voraus, dass die Verarbeitung in einem DSGVO-konformen Rechenzentrum erfolgt, welches die erforderlichen Absicherungen und technischen Möglichkeiten der Cybersicherheit auf dem Stand der Technik einsetzt und natürlich auch die Kommunikationsverbindungen verschlüsselt sind.

Hier können Zertifikate der Rechenzentren im Hinblick auf Datenschutz und IT-Sicherheit den Krankenhäusern auch mehr rechtliche Sicherheit bieten. Zwar ist derzeit noch keine Zertifizierung nach Art. 42 DSGVO verfügbar, doch gibt es Zertifikate zum Beispiel im Hinblick auf das Informationssicherheitsmanagement nach ISO 27001, die Sicherheit von Cloud-Dienstleistungen nach ISO 27017 oder einem technischen Datenschutzstandard für Cloud-Dienste nach ISO 27018. Diese Zertifikate zeigen zwar lediglich, dass für die zertifizierten Dienste ein System zum Management von Risiken für die Informationssicherheit bzw. den Datenschutz existiert, das den Audits der Zertifizierungsstellen standgehalten hat, die praktisch immer nur Plausibilitäts- oder Stichprobenprüfungen darstellen. Damit garantieren sie zwar keine Datenschutz-Compliance und können auch keine Prüfung eventuell bestehender besonderer rechtlicher Voraussetzungen für ein Outsourcing ersetzen. Sie bieten aber doch gewisse Indizien für einen materielles Schutzniveau durch technische sowie organisatorische Sicherheitsmaßnahmen und können so den Krankenhäusern die sorgfältige Auswahl eines Auftragsverarbeiters erleichtern.

Ebenso sollte das Cloud-KIS selbst zertifiziert sein oder es sollte zumindest für Krankenhäuser transparent sein, welche Anforderungen aus welchen Anforderungskatalogen erfüllt werden. In diesem Sinne sollten sich Krankenhäuser mit gängigen Anforderungskatalogen[427] vertraut machen und die für sie oder allgemein wesentlichen Anforderungen daraus in die Auftragsdatenverarbeitungsverträge mit aufnehmen. Zu nennen sind hier u.a. die vom BMWi genannten Standards und Zertifizierungen[428] und der Kriterienkatalog Cloud Computing C5 des BSI[429], aber auch die Anforderungen aus der Orientierungshilfe KIS[430], dem BSI-Leitfaden[431] und dem branchenspezifischen Sicherheitsstandard der DKG[432]. Die Europäische Agentur für Cybersicherheit (enisa – EUROPEAN UNION AGENCY FOR CYBERSECURITY) publiziert auf ihrer Website eine Liste von 13 Zertifizierungs-Schemata und der zugehörigen Zertifikate und Organisationen[433].

Details zu technischen Anforderungen sollen hier im Folgenden nicht weiter betrachtet werden, finden sich doch ausführliche Empfehlungen und Anforderungskataloge in den vorgenannten Leitfäden und in Kapitel 4.

---

[427] Siehe auch oben Kapitel 4.5, S. 219 ff.

[428] BMWi, Cloud-Standards und Zertifizierungen im Überblick – Was Cloud-spezifisch betrachtet werden sollte. Version 1.0. 2016.

[429] Bundesamt für Sicherheit in der Informationstechnik, Kriterienkatalog Cloud Computing C5:2020.

[430] Arbeitskreise „Gesundheit und Soziales" sowie „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2014): Orientierungshilfe Krankenhausinformationssysteme.

[431] Bundesamt für Sicherheit in der Informationstechnik, Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. 2013.

[432] Deutsche Krankenhausgesellschaft: Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus. 2019.

[433] Siehe unter https://resilience.enisa.europa.eu/cloud-computing-certification.

Zum Zweiten muss eine solche Verarbeitung im Cloud-KIS außerhalb des Krankenhauses entsprechend ebenfalls durch einen Erlaubnistatbestand gedeckt sein, und je nach Erlaubnistatbestand so abgesichert sein, dass keinerlei Kenntnisnahme von Geheimnissen durch den Cloud-Betreiber erfolgen können.

Als stärkste Form der Geheimhaltung kann die Verschlüsselung von Daten angesehen werden. Kryptographische Verfahren sind heute ausgereift und werden ständig weiterentwickelt, z.B. um den immer leistungsfähigeren Rechnern und dem Brechen von Schlüsseln entgegenzutreten. Eine erste Form der Nutzdatengeheimhaltung ist die Plattenverschlüsselung, die vor allem eingesetzt wird, um den unberechtigten Zugriff auf Sicherungskopien oder durch Wartungspersonal auszuschließen. Immerhin stehen die Nutzdaten unverschlüsselt zur Laufzeit der Verarbeitung im Hauptspeicher, so dass prinzipiell unbefugte Kenntnisnahme möglich ist, aber nur unter sehr erschwerten Bedingungen und mit krimineller Energie von RZ-Insidern. Aus Praktikabilitätsgründen ist der Schlüssel in der Regel ausgewählten Mitarbeitern des Betreibers bekannt, da er bei jedem Neustart eingegeben werden muss. Eine Plattenverschlüsselung ist für Cloud-KIS zwar unabdingbar, garantiert aber nicht vollständig, dass der Betreiber in die Daten Einsicht nehmen kann. Dies sicherste Form ist daher eine Ende-zu-Ende-Verschlüsselung, die zum Teil für medizinische Verfahren gefordert wird. Diese wird in der Regel durch die Anwendung selbst oder dieser zugegebenen Komponenten durchgeführt. Im Falle von Cloud-KIS sind die Endpunkte hierbei der Persistenzspeicher in der Cloud und das Anzeigegerät des Benutzers. Neben einem komplexen Schlüsselmanagement ist hier unabdingbar, dass die Verarbeitung der Daten – zumindest die Entschlüsselung – direkt im Client erfolgt.

Genau ein wesentliches Ziel aber von Cloud-Anwendungen ist es, mittels Webanwendungen jegliche Vor-Ort-Installation unnötig zu machen und die Anwendungen nur über einen Browser zu bedienen. Verarbeitung und Oberflächengenerierung erfolgen im Webserver, der lediglich dynamische Seiten an den Browser gibt. Damit scheidet eine Entschlüsselung von Nutzdaten auf einem nativen Browser-Client aus. Eine Möglichkeit bestünde zumindest beim Einsatz einer Rich Internet Application (RIA), bei der z.B. umfangreiches JAVA Script im Browser ausgeführt wir, eventuell in der Nutzung eines lokal gespeicherten Schlüssels der via z.B. Cookie der Verarbeitung im Browser untergeschoben wird und so eine Entschlüsselung der Nutzdaten ermöglicht. Dies würde aber einen Angriffspunkt für Hacker darstellen. Auch wäre hier dann nur eine symmetrische Verschlüsselung möglich und der Schlüssel (z.B. ein institutionsweit gültiger oder je Anwendungssystem) müsste physisch auf jedem die Webanwendung nutzenden Endgerät vorhanden sein. Alternativ ist denkbar, dass der Benutzer selbst den Schlüssel eingibt, was aber im Alltagsbetrieb nicht als praktikabel angesehen werden kann. Einige weitere Varianten sind denkbar (entfernter Key Store, Nutzung von Kontextinformationen etc.), hier besteht aber weiterer Forschungsbedarf. Die Tatsache, dass inzwischen auch auf verschlüsselten Daten gesucht werden kann, schafft für das geschilderte Problem keine Abhilfe, da für die Visualisierung und Nutzung durch den Benutzer immer lokal eine Entschlüsselung notwendig wird. Immerhin kann durch Suchen auf verschlüsselten Daten die Performance solcher Lösungsansätze sehr verbessert werden, da nicht die Gesamtmenge der zu durchsuchenden Objekte erst in den Client geladen, entschlüsselt und dann die Suchoperation gestartet werden muss.

Sollen oder müssen Informationen zwar im Klartext, aber nicht zuordenbar verarbeitet werden, bietet sich als stärkste Form die Anonymisierung gegenüber dem Cloud-Anbieter durch Pseudonymisierung bereits im Krankenhaus an.[434] Entsprechend Erwägungsgrund 26 DS-GVO sollen die Vorgaben der DS-GVO nicht für anonyme Daten gelten. Jedoch muss der Verantwortliche u. a. der Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO folgend, zu jedem Zeitpunkt der Verarbeitung (und damit insbesondere auch während der gesamten Speicherdauer) nachweisen können, dass es sich um anonyme Daten handelt".[435] Eine faktische Deanonymisierung muss also auf jeden Fall ausgeschossen werden können.

Wie bereits in Kapitel 4.4.3 dargestellt, handelt es sich bei einem Cloud-KIS um eine weitegehend modularisierte Anwendung, deren Teile auch auf verschiedenen Rechnern oder in verschiedenen Clouds laufen können. Die technische Zerteilung gibt in manchen Fällen – nämlich dort, wo Aufgaben, für die die genauen Kenntnisse des Patienten nicht notwendig sind – auch die Möglichkeit, entsprechend anonymisiert zu verarbeiten. Dies dürfe immer dann der Fall sein, wenn gewisse medizinische Informationen über den Patienten zwar zu verarbeiten bzw. als Kontext zu nutzen sind, aber eine Zuordnung zur Person für den Vorgang selbst beim Verarbeiter nicht erforderlich ist. Beispiel sind hier die AMTS-Prüfung, die Auswertung von Biosignalen und Bildern, die kontextsensitive Wissensrecherche oder die Anforderung einer Zweitmeinung oder die Durchführung einer Erstbefundung ausschließlich auf Basis medizinischer Daten oder Bilder. Für die beiden Erstgenannten Beispiele können "Function-as-a-Servcie" eingesetzt werden und wenn notwendig (z.B. bei AMTS) erfolgt die Nutzung oder Zuordnung der vom angefragten Dienst rückgelieferten Ergebnisse in der anfragenden Anwendung manuell durch den Benutzer. In diesem Fall stellt die Schutzmaßnahmen "anonyme Nutzung" auch keine Einschränkung der Funktionalität oder Benutzbarkeit des KIS dar. Solche Dienste aus der Cloud können auch schon heute in Legacy-KIS integriert werden. Bei einer Erst- oder Zweitbefundung von medizinischen Daten und Informationsobjekten stellt sich die Ausgangssituation etwas komplexer dar, denn die Ordnungsmäßigkeit der Medizinischen Dokumentation erfordert eine gesicherte Einheit aus Angaben zum Patienten und Befund, was auch für die Patientensicherheit wichtig ist. Es muss also zweifelsfrei eine Zuordnung möglich sein, sodass im Grunde - auch wenn der Befunder scheinbar anonyme Daten erhält - diese Verfahren faktisch schon unter ein pseudonymisiertes Verfahren fallen. Holst et. al sehen im Sinne des Art. 4 Nr. 2 DSGVO auch schon die anonymisierte Verarbeitung als Verarbeitung nach Art. 6 und Art. 9 der DSGVO an und halten auch diese für zustimmungspflichtig.

Bei der Pseudonymisierung wird eine Trennung der Nutzdaten und der identifizierenden Daten vorgenommen. In der DSGVO heißt es hierzu im Erwägungsgrund 26 "Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine

[434] Für das verantwortliche Krankenhaus muss eine Deanonymisierung dagegen für die üblichen Anwendungsszenarien eine KIS immer möglich sein. Eine Anonymisierung für den Cloud-Anbieter ist daher nur unter Zugrundelegung des relativen Ansatzes des Personenbezuges möglich, der jedoch auch nach EuGH, Urteil v. 19.10.2016, Az. C-582/14, zum Personenbezug von dynamischen IP-Adressen zumindest in einer verschärften Form noch vertretbar ist. Das würde jedoch bedingen, dass die Anonymisierung für den Cloud-Anbieter bereits im Krankenhaus erfolgt und für das Krankenhaus lediglich eine Pseudonymisierung vorliegt.

[435] Holst/Schütze/Sypra, Arbeitshilfe zur Pseudonymisierung/Anonymisierung. 2018. S. 9.

identifizierbare natürliche Person betrachtet werden." Die Reichweite dieser Aussage ist umstritten. Pseudonyme Daten sind für die Stelle, hier insbesondere das verantwortliche Krankenhaus, welches über die Zuordnung zur Person verfügt, definitiv noch personenbezogen. Für sonstige Stelle, zum Beispiel für Cloud-Anbieter, die nicht über die Zuordnung verfügen, ist dies jedoch umstritten.[436] In jedem Fall kann die Pseudonymisierung ein effektives Mittel des technisch-organisatorischen Datenschutzes sein und deren Einsatz daher, je nach den Umständen, auch geboten sein. So kann die Pseudonymisierung noch im Krankenhaus beispielsweise auch die Nutzung von Cloud-Diensten aus „unsicheren" Drittstaaten wie den USA rechtlich möglich machen.[437]

Prinzipiell können fast alle medizinischen Microservice-Module auf pseudonymisierter Basis betrieben werden. Auch schon bei einem regelhaften Datenbankentwurf sind die Angaben zur Personen immer getrennt von den medizinischen Daten und z.B. in FHIR sind diese auch nicht in den Ressourcen inkludiert, sondern es erfolgt nur ein Verweis ("Reference") auf die Ressource "Person". Andererseits müssen für eine justitiable Archivierung bzw. bei Signatur von Befunden und anderen Feststellungen die Einheiten aus Personenangaben und Inhalten en block archiviert und wo Signieren eingesetzt wird auch en block signiert werden. Damit muss es immer zu einem Zeitpunkt für kurze Zeit an einem Ort – sprich in einer IT-Anwendung – eine Zusammenführung geben. Ein Ansatz zu physischen Trennung von medizinischen bzw. personenbezogenen Nutzdaten und Patientenstammdaten ist in Abbildung 4-20 dargestellt.

Insgesamt kann festgestellt werden, dass einerseits der Aufwand für Verbergen von Patientendaten vor dem Cloud-KIS-Betreiber durch Kombination verschiedenster Ansätze sehr hoch ist und für wirklich effektive Webanwendungen hierzu noch Forschungsbedarf besteht.

5.3.2 Bare-Metal-Server

Wie unter 3.3 bereits ausgeführt, stellt die Einschaltung von Cloud-Anbietern i.d.R. eine Auftragsverarbeitung nach Art. 28 DSGVO dar. Diese Einordnung bringt nach Unionsrecht bereits Restriktionen für das Outsourcing mit sich, die insbesondere durch noch restriktivere Datenschutzanforderungen auf Landesebene verschärft werden. Der datenschutzkonforme Betrieb eines vollumfänglichen KIS-as-a-Service auf Basis einer Auftragsverarbeitung ist nach geltendem Recht nicht in allen Bundesländern möglich.

Die Verwendung sogenannter Bare-Metal-Server könnte unter bestimmten Voraussetzungen eine Lösung dieses Problems darstellen.

Bare-Metal-Server sind Hardwarestrukturen, auf denen Anwendungen ohne zwischengeschaltete Virtualisierung direkt ausgeführt werden. Bare-Metal-Server können im eigenen Rechenzentrum betrieben oder aber auch bei Hosting-Anbietern gemietet werden. Häufig werden solche Server als dedizierte Single-Tenant-Lösungen angeboten. Die Hardware eines Servers steht also dediziert nur einem einzigen Kunden zur Verfügung, was eine physische Trennung der auf der Hardware gespeicherten und verarbeiteten Daten von den Daten anderer Kunden mit sich bringt.

---

[436] Zur Debatte um den absoluten oder den relativen Ansatz des Personenbezuges siehe EuGH, Urteil v. 19.10.2016, Az. C-582/14, und Schneider, Sekundärnutzung klinischer Daten, S. 11 ff.

[437] Siehe dazu oben den Use Case 2 des EDSA zur Drittlandübermittlung auf S. 57.

Damit scheidet aber eine Skalierung über Ressourcen vieler Kunden - was die Potenz von Cloud Computing ausmacht - aus, sodass das Bare-Metal-Model eher dem klassischen RZ-Betrieb entspricht bzw. einem PaaS-Ansatz.

Je nach Ausgestaltung des Service-Modells kann die Bereitstellung eines Bare-Metal-Servers gewisse administrative Aufgaben, wie z.B. die Installation und Wartung eines Betriebssystems, durch den Anbieter vorsehen. Möglich ist aber auch die reine Hardware-Bereitstellung, wobei der Kunde selbst die Installation, Konfiguration und Wartung von Betriebssystem sowie Soft- und Middleware übernimmt. Im zuletzt dargestellten Modell hat der Kunde somit vollumfänglichen Root-Zugriff und sämtliche Administrationsrechte. Unter zusätzlicher Zuhilfenahme einer Festplattenverschlüsselung ist es dann möglich, einen Zugriff des Anbieters sowie anderer Kunden auf Daten, die auf dem Server gespeichert und verarbeitet werden, nahezu vollständig auszuschließen, Kenntnis von Daten kann nur noch erlangt werden, wenn zur Laufzeit des Systems der Hauptspeicher ausgelesen wird, was im Grunde nur möglich ist, wenn der Service-Dienstleister für seine Infrastruktur so gut wie keine technisch-organisatorischen Maßnahmen trifft bzw. einhält.

Da der Anbieter unter den genannten Voraussetzungen keinen direkten Zugriff auf die auf dem Server gespeicherten und verarbeiteten personenbezogenen Klartext-Daten hat, ist zumindest fraglich, ob in einem solchen Fall überhaupt noch eine Auftragsverarbeitung vorliegt. Das muss wohl verneint werden. Rechtlich wäre eher von einem Mietverhältnis bzgl. der Hardwarestruktur bzw. Infrastruktur als von einer Auftragsverarbeitung auszugehen. Die bzgl. dem Outsourcing bestehenden restriktiven Datenschutzvorschriften wären somit nicht einschlägig.

Neben den genannten Vorteilen sprechen auch weitere Gründe, wie eine höhere Performance und gesteigerte Zuverlässigkeit sowie die Vermeidung von Störungen durch andere Kunden (sog. Noisy Neighbor Effekt), für den Einsatz eines Bare-Metal-Servers für das Cloud-Computing[438].

Dem stehen allerdings auch einige Nachteile gegenüber. Zunächst sind entsprechende Angebote gegenüber herkömmlichem Cloud-Hosting meist teurer, da die verwendete Hardware statt einer Vielzahl von Kunden nur einem einzigen Kunden zur Verfügung gestellt wird. Außerdem ist bei herkömmlichen Cloud-Hosting-Angeboten i. d. R. größere Skalierbarkeit bzw. Elastizität als auch Ausfallsicherheit gegeben. Zudem erfordern die Einrichtung und Pflege eines solchen Systems viel technisches Know-how und bringt enormen Aufwand für die IT-Abteilung des Nutzers mit sich analog zum Aufwand beim Betrieb eines lokalen Systems.

Letztendlich können aber in diesem Modell die Vorteile von Cloud-KIS hinsichtlich Softwarearchitektur, Modularität und Offenheit sowie Orchestrierbarkeit und dynamisches Deployment sowie der Betrieb als Webanwendung und damit kein Aufwand für das Client-Management vollumfänglich ausgeschöpft werden. Vor dem Hintergrund der Tatsache, dass die Skalierbarkeit aufgrund des relativ stabilen und bekannten Lastprofils eines Krankenhauses nicht das entscheidende Argument für Cloud-KIS ist, scheint das Bare-Metal-Modell einen interessanten Kompromiss zwischen Nutzung moderner Cloud-Technologien und Sicherstellung der Vertraulichkeit darzustellen.

[438] IONOS: Bare-Metal-Server – dedizierte Hardware für anspruchsvolle Webprojekte; 07.02.2020.

In diesem Sinne wäre denkbar, dass ein Cloud-KIS-SaaS-Angebot als vorgefertigte KIS-Umgebung bei einem Betreiber vorgehalten wird, die dann für Neukunden – nach voriger Orchestrierung der Funktionalitäten – physisch in den Bare-Metal-Server kopiert wird inklusive aller Mechanismen für die Betriebssystem-, Middleware- und Anwendungssoftwareaktualisierungen.

5.4 Bewertung der Vereinbarkeit der Anforderungen für den Krankenhaus-Bereich

5.4.1 Basisanforderungen nach Art. 28 DSGVO

Nach den Basisanforderung zur Auftragsverarbeitung in Art. 28 DSGVO kann ein entsprechend vertraglich eingebundener Cloud-Anbieter als "trusted person" angesehen werden, die bei Bedarf (z.B. zur Fehleranalyse) auch Kenntnis von personenbezogenen Daten nehmen darf und jedenfalls die Möglichkeit dazu haben darf. Eine Vertraulichkeit gegenüber dem Provider (vgl. 4.7.3, Abb. 4-20) ist hier nicht generell vorgeschrieben. Der Cloud-Anbieter muss als Auftragsverarbeiter aber die Patientendaten selbstverständlich gegenüber dem unbefugten Zugriff Dritter schützen und muss insoweit risikoadäquat vorhandene technischen und organisatorischen Maßnahmen nach dem Stand der Technik einsetzen. Insofern sind diese datenschutzrechtlichen Anforderungen ohne Weiteres mit den technischen Möglichkeiten und dem Betrieb eines Cloud-KIS, selbst eines Cloud-native-KIS vereinbar.

5.4.2 Verschärfte Erforderlichkeitsprüfung gemäß der Schweigepflicht (§ 203 StGB)

Die ärztliche Schweigepflicht nach deutschem Recht (§ 203 StGB) verschärfte die Anforderungen an die Prüfung der Erforderlichkeit von technischen Maßnahmen gegenüber der allgemeinen datenschutzrechtlichen Lage nach Art. 28, 32 DSGVO. Denn soweit eine ausgelagerte Tätigkeit technisch ohne Offenbaren von Privatgeheimnissen (wie solchen des Patienten) möglich ist, wird es hier als erforderlich angesehen, diese Geheimisse nicht zu offenbaren, was dann ggf. eine Ende-zu-Ende-Verschlüsselung oder eine effektive Pseudonymisierung nötig macht. Eine Vereinbarung über die Auftragsverarbeitung nach Art. 28 DSGVO und auch eine Schweigeverpflichtung nach § 203 Abs. 4 StGB allein, genügen nicht um ein Offenbaren befugt zu machen. Es erscheint jedoch vertretbar, auch in diese verschärfte Erforderlichkeitsprüfung gewisse Performancegesichtspunkte einzubeziehen, so dass auch die Schweigepflicht letztlich nichts fordert, was technisch nicht möglich ist oder praktisch ein effektives Outsourcing verhindern würde. Allerdings muss doch geprüft werden, ob nicht sehr fortgeschrittene, über den üblichen Standard hinausgehende technische Methoden zum Einsatz kommen können, um einen Patientenbezug zu vermeiden.

Soweit sich eine Befugnis zur Durchbrechung der Schweigepflicht auch außerhalb von § 203 Abs. 3 StGB findet, ist eine solche verschärfte Erforderlichkeitsprüfung, also die Prüfung, ob eine Offenlegung von Patientendaten überhaupt erforderlich ist, jedoch nur nötig, wenn diese separate Befugnisnorm dies vorsieht. Dies ist nach dem meisten LKHG nicht der Fall, deren Regelungen zur Auftragsverarbeitung von Patientendaten gerade vorsehen, dass diese ausgelagert, also offenbar werden dürfen und in Zusammenhang damit eben unter anderem die zum Schutz der Daten beim Auftragnehmer, also in der Cloud, erforderlichen technischen und organisatorischen Maßnahmen fordern.

5.4.3 Unsichere Drittstaaten und schwierige Bundesländer

In Bezug auf Drittstaaten, deren Datenschutzniveau aus EU-Sicht wegen zu weiten Zugriffsbefugnissen von dortigen Behörden unangemessen ist, gelten allerdings noch weiter verschärfte Restriktionen. Hier fordert der Europäische Datenschutzausschuss, dass überhaupt keine personenbezogenen Daten im Klartext an Auftragnehmer in diesen Staaten übermittelt werden dürfen, sondern dass der Personenbezug für den Auftragnehmer praktisch durch technische Maßnahmen wie Ende-zu-Ende-Verschlüsselung, effektive Pseudonymisierung oder Secure Multi Party Computation ausgeschlossen wird. Einen Vorbehalt wie bei der Erforderlichkeit des Offenbarens nach der deutschen Schweigepflicht dahingehend, dass die Auslagerung einer Tätigkeit dadurch nicht unmöglich gemacht werden darf, kennt der EDSA nicht. Dies mag man in dieser Allgemeinheit durchaus kritisieren können. Im Hinblick auf Patientendaten aus Krankenhäusern, die nach deutschem Recht - aber eben in der Regel nicht nach dem Recht von unsicheren Drittstaaten - einem Beschlagnahmeschutz unterliegen, erscheint dies jedoch gut nachvollziehbar. Bevor in Deutschland der rechtliche Beschlagnahmeschutz auf sonstige mitwirkende Personen bzw. Auftragsverarbeiter ausgedehnt wurde, war auch hier häufig angenommen worden, dass es eines technischen Beschlagnahmeschutzes bedürfe, welcher den Anforderungen des EDSA für technische Lösungen in unsicheren Drittstaaten entspricht.

Im Sinne der Rechtssicherheit empfiehlt sich eine solche Lösung des "technischen Beschlagnahmeschutzes" auch, wenn in Deutschland oder der EU lokalisierte Cloud-Angebote von US-Dienstleistern genutzt werden, da diese nach dem U.S. CLOUD Act - ungeachtet der Lokalisierung der Daten - dazu gezwungen werden könnten, diese Daten an öffentliche Stellen in den USA herauszugeben - und dies derzeit ohne Rechtsschutzmöglichkeiten für Betroffene, die weder Bürger der USA noch dort wohnhaft sind.

Auch manche Bundesländer innerhalb der BRD verbieten teils das Outsourcing von Patientendaten. So erlaubt z.B. das LKHG BY nur die Auslagerung administrativer KIS-Module an spezialisierte (Cloud-)Anbieter, was aber wiederum im SGB V jedenfalls für Abrechnungsdaten von Krankenhäusern nicht vorgesehen ist. Medizinische KIS-Module dürfen von Krankenhäusern in Bayern nur an andere Krankenhäuser im Wege der Auftragsverarbeitung ausgelagert werden. Dies würde dazu führen, dass bei der Auslagerung solcher Module auf spezialisierte Cloud-Anbieter, selbst innerhalb der EU oder in Deutschland, Maßnahmen wie eine Ende-zu-Ende-Verschlüsselung zur Verschleierung des Patientenbezuges ergriffen werden müssten, wie sie sonst nur gegenüber unsicheren Drittstaaten angezeigt sind. Im Gegensatz zur Skepsis der EU bzw. des EuGH gegenüber unsicheren Drittstaaten erscheint diese Zurückhaltung gerade in rechtspolitischer Hinsicht wenig nachvollziehbar.

Denn angezeigte Lösungen wie eine Ende-zu-Ende-Verschlüsselung würden beispielsweise ein Cloud-Native-KIS nicht möglich machen, weshalb insoweit nach dem Stand der Technik rechtliche und technische Anforderungen unvereinbar nebeneinander stünden. Im Zuge einer Weiterentwicklung des Standes der Technik, insbesondere wenn Krypto-Mechanismen für die Ende-zu-Ende-Verschlüsselung in Browsern untergebracht werden können (zur Ver- und Entschlüsselung nur im Browser bei persistenter Verschlüsselung in der Cloud), könnte sich dies jedoch ändern.

Im Übrigen kämen im Hinblick auf die Verarbeitung durch US-Cloud-Anbieter bzw. mit deren Technologie in Europa und insbesondere Deutschland auch Datentreuhandlösungen in Betracht, wie sie in Kapitel 6 vorgestellt werden und die CLOUD-Act-Problematik entschärfen.

6 Lösungsvorschläge

6.1 Vorschläge für Schaffung einer einheitlicheren und Cloud-freundlicheren Rechtslage

6.1.1 Angleichung der Regeln zur Auftragsverarbeitung in den Landeskrankenhausgesetzen

Die in den Landeskrankenhausgesetzen enthaltenen, stark heterogenen Regelungen zum Datenschutz im Allgemeinen und zur Auftragsverarbeitung im Besonderen stellen ein erhebliches Hemmnis für die Entwicklung, Einrichtung und den Betrieb Cloud-basierter KIS dar. Nicht nur ist Krankenhäusern nach der aktuellen Rechtslage in mehreren Bundesländern die Auftragsverarbeitung durch Cloud-Anbieter weitgehend untersagt. Vielmehr sind dadurch auch länderübergreifende Strukturen und der Aufbau regionaler digitaler Ökosysteme erheblich erschwert und ein einheitlicher KIS-Markt kann nicht entstehen, was die Attraktivität des Standorts Deutschland für Anbieter negativ beeinflusst. Das verhindert auch das Entstehen europäischer Cloudlösungen als Alternative zu Anbietern im Ausland ohne Angemessenheitsbeschluss nach DSGVO.

Dieser regulatorische Flickenteppich kann nur durch eine Angleichung und Vereinheitlichung der entsprechenden Regelungen in den Landeskrankenhausgesetzen aufgelöst werden. Der Maßstab für eine Vereinheitlichung sollten dabei aber nicht diejenigen Länder sein, in denen besonders restriktive Regelungen gelten. Vielmehr sollte im Zuge der Angleichung auch eine gewisse Liberalisierung erfolgen, bei der sich die länderspezifischen Regelungen eher den Anforderungen der DSGVO annähern.

Die entsprechenden Regelungen sollten dabei die Inanspruchnahme externer Dienstleister für bestimmte Aufgaben ausdrücklich gestatten, ähnlich der Regelungen des § 43e Bundesrechtsanwaltsordnung (BRAO). Die in der Begründung zur Einführung dieser Vorschrift aufgeführten Argumente lassen sich zum Teil auch auf die Inanspruchnahme von Dienstleistern durch ein Krankenhaus übertragen. Demnach machten es "[m]oderne arbeitsteilige Strukturen und das Erfordernis der Nutzung elektronischer Datenverarbeitung [...] heutzutage in vielen Fällen nicht mehr möglich, alle Arbeiten, die mit der Berufsausübung des Rechtsanwalts zusammenhängen, von Personen ausüben zu lassen, die bei diesem beschäftigt sind".[439] Als Beispiel für solche Fälle nennt der Entwurf die Heranziehung externer IT-Dienstleister für die elektronische Datenverarbeitung. Dies lässt sich sicherlich auch auf Krankenhäuser übertragen, deren IT-Abteilungen durch den vermehrten Einsatz externer Dienstleister und insbesondere Cloud-Anbieter deutlich entlastet werden könnten.

§ 43e Abs. 4 BRAO geht noch einen Schritt weiter und erlaubt Rechtsanwälten ausdrücklich die Inanspruchnahme von Dienstleistungen, die im Ausland erbracht werden, sofern „der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist, es sei denn, dass der Schutz der Geheimnisse dies nicht gebietet." In der Gesetzesbegründung wird dazu – wenn

[439] Begründung zum Regierungsentwurf des Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen, Bundestags-Drucksache 18/11936, S. 32.

auch ohne nähere Angaben – weiter ausgeführt, dass „[f]ür die anderen Mitgliedstaaten der Europäischen Union [...] in der Regel von einem solchen Schutz ausgegangen werden" kann.[440] Eine solche Regelung wäre auch für die Verarbeitung von Patientendaten durch Cloud-Dienstleister im Auftrag eines Krankenhauses zu erwägen und käme den Anforderungen der DSGVO recht nahe. Im Hinblick auf die Vergleichbarkeit des Geheimnisschutzes für Patientendaten in anderen Mitgliedstaaten sollten allerdings genauere Untersuchungen angestellt werden.[441] Jedenfalls die Bedenken im Hinblick auf „unsichere" Drittstaaten wie die USA blieben aber auch mit einer solchen Regelung bestehen.

Eine Vereinheitlichung und Liberalisierung der landesrechtlichen Vorschriften zu Datenschutz und Auftragsverarbeitung im Krankenhaus, beispielsweise orientiert am Vorbild der Geheimnisschutzvorschriften der BRAO, würde die Entwicklung hin zu mehr Cloud-Computing im Gesundheitsbereich begünstigen und die damit verbundenen vorangehend beschriebenen Vorteile schöpfen lassen. Die entsprechenden Vorschriften müssten dabei aber selbstverständlich so ausgestaltet sein, dass der gebotene Schutz besonders schutzbedürftiger Patientendaten keinesfalls hinter demjenigen nach der DSGVO zurückbleibt.

6.1.2 Vereinheitlichung der Regeln zur Auftragsverarbeitung im SGB V

Die Regelungen zur Auftragsverarbeitung im Rahmen der Übermittlung von Leistungsdaten durch Leistungserbringer in der GKV an die Krankenkassen oder Kassenärztlichen Vereinigungen sollten nicht wie bislang nur partiell und uneinheitlich im SGB V geregelt werden (was möglicherweise zu Umkehrschlüssen dahingehend führt, dass dies für die Abrechnung durch Krankenhäuser nicht zulässig ist).

Eine einheitliche Regelung für alle Leistungserbringer in der GKV würde daher Sinn machen. Eine Gesetzgebungskompetenz des Bundes läge hierfür mit Art. 74 Abs. 1 Nr. 12 des Grundgesetzes vor, da die Abrechnung mit der GKV als Sozialversicherung geregelt würde.

Diese einheitliche Vorschrift könnte sich gegebenenfalls an der Regelung für Sozialleistungsträger in § 80 SGB X orientieren. Diese Norm ist nicht unmittelbar auf Leistungserbringer anwendbar, könnte aber für entsprechend anwendbar erklärt werden.

Alternativ könnte man auch gesetzgeberisch klarstellen, dass ein Rückgriff auf die allgemeinen datenschutzrechtlichen Regelungen überall dort möglich bleiben soll, wo das SGB V keine speziellen Vorschriften enthält. Dann könnte mangels spezifischer Offenbarungsbefugnis jedoch auch strengere Erforderlichkeitsprüfung gemäß § 203 Abs. 3 StGB zur Anwendung kommen.

6.1.3 Abschaffung von Öffnungsklauseln für Sonderregelungen der Kirchen

Um zur Reduzierung der insbesondere in Kapitel 3 aufgezeigten rechtlichen Komplexität beizutragen, sollten auch die in den LKHG und LDSG bisher enthaltenen Öffnungsklauseln für Sonderregelungen der Kirchen gestrichen werden. Nach der hier vertretenen Auffassung ist es nicht zwingend, dass der Staat solche Sonderregelungen zulässt bzw. vorsieht.

---

[440] Begründung zum Regierungsentwurf des Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen, Bundestags-Drucksache 18/11936, S. 35.

[441] Skeptisch insoweit z.T. auch Cornelius, NJW 2017, 3751, 3754.

6.1.4 Rechtliche Vorgaben zur Interoperabilität von KIS und KIS-Modulen

Gesundheitsversorgung erfolgt mehr denn je nicht mehr isoliert in einer Einrichtung, sondern in einem verteilten System von Versorgungseinrichtungen, wobei die einzelnen Einrichtungen für die Erbringung ihrer anteiligen Behandlungsleistungen erheblich auf die Informationen anderer Versorger zum Patienten angewiesen sind. Dies gilt im Besonderen für Krankenhausbehandlungen hinsichtlich Vorinformationen aus dem ambulanten Bereich als auch für die Nachversorgung wiederrum im ambulanten Bereich für die Informationen aus dem stationären Bereich. Die Fähigkeit eines KIS zum adäquaten Austausch wichtiger Behandlungsinformationen sollte daher nicht nur Sache und im Obliegen eines Softwareherstellers sein, sondern ist ein gesamtgesellschaftliches Anliegen. Auch hier können cloudbasierte regionale digitale Ökosysteme mit integrierten Cloud-KIS einen erheblichen Beitrag für mehr Behandlungseffektivität und -sicherheit leisten.

Für die Zukunft sollte eine semantische Interoperabilität von Informationssystemen im Gesundheitswesen über ein message-basiertes Verfahren mit Minimaldatensätzen wie es heute üblich ist hinausgehen. Für eine offene verteilte Infrastruktur wird eine konsequente Serviceorientierung notwendig, für deren Betrieb die notwendige Hochverfügbarkeit heute technisch problemlos durch Cloud-Betreiber gewährleistet werden kann. Servicebasierte Interoperabilität und Cloud-Lösungen können auch Grundlage sein für den Aufbau und den Betrieb regionaler digitaler Ökosysteme für die einrichtungs- und sektorübergreifende Zusammenarbeit im Rahmen von Behandlungsprozessen. Darüber hinaus wird auch gemeinsame Wissensentwicklung und Wissensnutzung unterstützt. Ein Vorteil hier ist, dass mit FHIR von HL7 inzwischen umfangreiche Servicespezifikationen für medizinische Informationsobjekte vorliegen.

Ähnlich wie es heute für die Durchführung klinischer Maßnahmen – meist spezifiziert durch die medizinischen Fachgesellschaften - einzuhaltende Standards gibt, sollte zukünftig der Einsatz von entsprechenden informationstechnologischen Verfahren – die ja auch finanziert werden mit öffentlichen bzw. Krankenversichertengeldern – zur Dokumentation solcher medizinischen Maßnahmen ebenfalls einer Standardisierung unterliegen, zumindest bezüglich der fachlichen Kerndaten und der Kernfunktionalität, was erheblich zur Kompatibilität von Systemen für den Informationsaustausch bzw. die semantische Interoperabilität beitragen würde, da keine Schema- und Semantic-Missmatches mehr auftreten würden.

Es ist nicht einzusehen, dass wichtige klinische Konzepte wie ärztliche und pflegerische Diagnosen, Symptome, Medikationen und Maßnahmen in jedem System verschieden abgebildet und gehandhabt werden. Warum sollten Wunden und deren Versorgung, die ja auch medizinisch/pflegerisch einem Standard folgen muss, informationstechnisch so unterschiedlich abgebildet und dokumentiert werden, wie dies heute der Fall ist? Natürlich kann und soll jeder Hersteller weiterhin individuelle Implementierungen mit individueller Benutzeroberfläche und Zusatzfunktionalitäten anfertigen können, aber eben auf Basis bestimmter vereinbarter Branchenstandards zu den Kerninhalten von zentralen Informationsobjekten. In vielen Bereichen des täglichen Lebens ist das heute bereits so umgesetzt, vom grundsätzlichen Aufbau von Steckdosen bis zu den Sicherheitsmerkmalen eines Toasters, in der Fahrzeug- und Gebäudetechnik bis hin zu Produkten der Lebensmittelindustrie oder Pharmakologie oder beim Datenverkehr in der Logistikbranche. Daher scheint es nur angebracht, für einen der größten Wirtschaftsbereiche in Deutschland - das Gesundheitswesen - auch für den Einsatz von

Informationstechnologie eine gewisse Regulierung für Datenaustausch, Interoperabilität und Produktfunktionalität vorzunehmen. Immerhin wurden mit dem Bundesmedikationsplan und dem Notfalldatensatz erste wichtige Schritte in diese Richtung unternommen, ebenso zeigen die entsprechenden Regelungen in den Förderbedingungen zum KHZG deutlich in diese Richtung. Auch die von der KBV spezifizierten und noch zu spezifizierenden Medizinischen Informationsobjekte (MIO) sind normativ und enthalten granulare Spezifikationen zu bestimmten medizinischen Daten.

Festlegungen zu Kerneigenschaften zu bestimmten in allen Versorgungsbereichen und -situation wichtigen Informationsobjekten betreffen sowohl die Struktur als auch die verwendete Semantik für die Wertebereiche bestimmter Attribute, aber auch der Grundaufbau bestimmter Dokumente wie z.B. Entlassbriefe, Befundberichte u.ä. Für alles dies existieren heute weitgehend ausdifferenzierte Standards, und wo diese an ihre Grenzen stoßen, ist eine stärkere und finanzierte institutionalisierte nationale Mitarbeit bei der internationalen Health IT-Standardisierung wünschenswert.

Lösungsvorschläge im Einzelnen:

- Ausarbeitung von Kerndaten und Kernfunktionalitäten für Kern-Informationsobjekte der Gesundheitsversorgung auf Basis von FHIR, dabei auch Prüfung und Identifizierung von strukturellen oder semantischen Schwachstellen der Standards, auf nationaler Ebene und als Teil der nationalen eHealth-Strategie. Hier prioritär für die o.a. Behandlungsphänomene und Austauschdokumente.
- Mitaufnahme des Kriteriums Offenheit bzw. offene Service-Schnittstellen und Aufrufpunkte in Legacy-KIS in die Förderkriterien von Förderprogrammen, die sich auf die Erweiterung von KIS beziehen.
- Förderung des Aufbaus und Betriebs von Cloud-basierten Repositories gemäß Abbildung 4-16 und regionaler Cloud-basierter Ökosysteme unter Berücksichtigung bestehender Standards. Dabei auch Berücksichtigung der Möglichkeiten der Einbeziehung von Patienten in die Dokumentation und Prozessabwicklung.
- Schaffung von Rahmenbedingungen für den diskriminierungsfreien Marktzugang von Spezialanbietern und Spin Offs/Neugründungen, die heute oftmals an der Festungsstrategie der Legacy-KIS scheitern.
- Schaffung von Regelungen für die Zulassung oder zumindest Registrierung von medizinischen Cloud-Microservice-Modulen (CMSM) – z.B. analog zu dem DiGA-Verfahren – zum Aufbau eines "Cloud-KIS Plugin-Verzeichnisses" bzw. "Plugin-Stores". Denkbar auch Delegation an Selbstverwaltungsorgane, ähnlich wie dies im ambulanten Bereich für Softwarezulassungen der Fall ist. So könnten gewisse Anforderungen an CMSM spezifiziert werden, die ähnlich den DIGA-Anforderungen gegliedert sein könnten, ebenso ein Satz an beschreibenden Metadaten wie Ziele, Verwendungszeck aber auch Offenlegung der Serviceschnittstelle(n) des CMSM. Anhand eines solche Registers könnten sich Krankenhäuser über vorhandene in ihr KIS integrierbare CMSM informieren und es würde eine große Angebotstransparenz resultieren.

Normative Ansatzpunkte zur Vorgabe dieser Standards finden sich für Leistungserbringer in der GKV und damit auch alle Krankenhäuser außer reine Privatkliniken bereits im SGB V, so z.B. zum bundeseinheitlichen elektronischen Medikationsplan nach § 31a, § 334 Abs. 1 Nr. 4, § 355 Abs. 3, § 358 SGB V. Dieser Ansatz könnte über die Bundeskompetenz für die Sozialversicherung weiter ausgebaut werden. Neben solchen zwingenden Regularien ist auch an eine an Interoperabilitätskriterien geknüpfte Förderung wie nach dem KHZG zu denken, die mit der Zeit auch in eine entsprechende Forderung übergeht, die erfüllt werden muss, wenn Vergütungsabschläge vermieden werden sollen.

6.1.5 Stimulierung der Cloudifizierung von KIS

Als "Cloudifizierung" wird hier die Migration oder schrittweise Umstellung bestehender Legacy-Systeme auf Cloud Native Anwendungen verstanden. Wie in Kapitel 4.4.3 dargestellt, handelt es sich bei feingranularen mCloud-KIS um die Summe aller cloudbasierten MicroService-Module, die für den operativen Betrieb und die Steuerung sowie für das taktische und strategische Krankenhausmanagement notwendig sind. Aufgrund des modularen Charakters können diese Module auch von verschiedenen Herstellern stammen, sodass auch von einem modularen multivendorfähigem Cloud-KIS gesprochen werden kann. Trotzdem benötigt ein solcher Lösungsansatz wie in Abbildung 4-4 gezeigt ein gewisses minimales Kernsystem, in das dann Zusatzmodule in Form von "KIS-PlugIns" einbezogen/eingeklinkt werden können. Und eben für dieses "Einklinken" sind verbindliche standardisierte offengelegte Service- und Aufrufschnittstellen zur Einbindung an der Benutzeroberfläche notwendig.

Der Einsatz von Cloud-KIS hat für Krankenhäuser eine Reihe von Vorteilen, die allgemein für Cloud-Einsatz angegeben werden. Hierzu zählen u.a. die Hochverfügbarkeit, das hohe Sicherheitsniveau, die passgenau Orchestrierung der Anwendungsumgebung, ressourcennutzungs- oder wertschöpfungsorientierte Kostenmodelle, die sukzessive Hinzunahme von Funktionalitäten, die Möglichkeit aus verschiedenen alternativen Modulen zu wählen, die Schaffung von Freiräumen für das Vor-Ort-IT-Personal für die Konzentration auf fachliche und strategische Belange der IT im Krankenhaus, Abbau von Herstellerabhängigkeit, keine Notwendigkeit mehr von Client-Installationen und Client-Management, Integration von "Fremdsoftware" und Eigenentwicklungen. Die Verfügbarkeit von mCLoud-KIS muss daher auch ein großes Anliegen der Krankenhäuser sein. Selbst der Betrieb entsprechender Lösungen On-Premises hat viele Vorteile.

Legacy-Hersteller haben stabile langjährig entwickelte Software und in der Regel wenig Motivation, ökonomischen Erfolg durch Neuentwicklungen zu reduzieren, denn: Je länger die Betriebslaufzeit, desto größer der unternehmerische Wertebeitrag. Auch wenn technologische Modernität, Flexibilität und Plug-In-Fähigkeit eines KIS Wettbewerbsfaktoren sind, schlägt sich dies im Wettbewerb nur nieder, wenn in einer Branche auch eine Nachfrage nach solchen innovativen Lösungen besteht. Wenn Anbieter und Kunden gemeinsam in der Nische der technologischen Vergangenheit verharren, entstehen auch keine innovativen neuen Lösungen.

Es sind daher nationale Strategien und Anstrengungen zu entwickeln, die die Weiterentwicklung für den Krankenhausbereich in Richtung Cloud Native Anwendungen stimulieren. Erster Anreiz und Stimulierung könnte hier der §19 Abs 1 Nr 7 des KHZG sein, in dem explizit Cloud-Computing als förderfähige Vorhaben für die Abstimmung des Leistungsangebotes mehrerer

Krankenhäuser oder die Bereitstellung sicherer Systeme ohne lokale Server benennt. Auch heißt es in den Richtlinien unter Zielsetzung dazu: "Eine einrichtungsübergreifende Kooperation zur Abstimmung des Leistungsangebots ist insbesondere bei Digitalisierungsvorhaben der Fördertatbestände 2-6 sowie 8-10 möglich". Krankenhäuser sollten also bei Beantragungen prüfen, ob sie mit ihren Partnern und ggf. auch im Verbund mit anderen Krankenhäusern Lösungserweiterungen als Cloud-Lösungen umsetzen lassen.

Daneben können auch die Krankenhäuser die Entwicklung stimulieren, indem sie bei anderen Ausschreibungen und Neubeschaffungen neben der Offenheit auf Basis von HL7-Nachrichten wie das heute üblich ist auch eine Offenheit in Bezug auf servicebasierte Interoperabilität - wo möglich auf Basis von FHIR – und Cloud-Perspektiven einfordern. Ebenso sollten Aufrufpunkte im Legacy-System – ggf. parametrierbar durch das Krankenhaus – zum Aufruf von Cloud-Modulen eingefordert werden; auch von Drittanbietern. Dies würde zunehmend eine Vielfalt von "KIS-Plugins" ermöglichen und Spezialfunktionalitäten, die so von den Legacy-Herstellern nicht geliefert oder nicht wirtschaftlich akzeptabel geliefert werden können, verfügbar machen.

6.2 Vorschläge zur Ausrichtung der technischen KIS-Architekturen auf die Cloud

Viele der heute kommerziell verfügbaren KIS-Lösungen bzw. der Subsysteme sind noch keine Cloud-Lösungen. Zumeist handelt es sich bei Legacy-KIS um klassische Client-Server-Anwendungen. Bei RZ-Betrieb erfolgt die Verarbeitung der „fetten Clients“ auch im Rechenzentrum und die Benutzung wird mittels Terminalserver bzw. virtualisiertem Desktop auf die Arbeitsrechner gebracht. Im weitesten Sinne ist der Betrieb von Legacy-KIS des alten Stils auf skalierbaren Infrastrukturen oder Plattformen auch schon Cloud-Computing, aber diese Systeme können die skalierenden Infrastruktur- und Plattform-Potenziale des Cloud-Computing nur in gewissem Maße ausschöpfen. Angebote in Form von Software-as-a-Service sind ebenfalls damit nicht am Markt platzierbar. Aber auch softwaretechnisch wird es immer schwieriger, diese zum Teil vor 25 Jahren entstandenen Software-Systeme an neue Anforderungen und Herausforderungen anzupassen. Aufgrund des technologischen Wandels und der Nichtmehrverfügbarkeit alter zugrunde liegender Basis-Technologien sind Legacy-KIS dabei, zunehmend zu verrotten.

In vielen anderen Branchen haben bereits vor Jahren Hersteller damit begonnen, ihre Legacy-Systeme auf Cloud-fähig umzustellen bzw. neu zu entwickeln. Eine reine Code-Migration scheint wenig praktikabel und sinnvoll, da heutige Tools und Technologien sowie der für Cloud Native Anwendungen notwendige Architekturzuschnitt anderen Paradigma gehorchen als vor 20-30 Jahren. Auch lassen die heutigen Technologien und Werkzeuge eine weitaus effektivere Softwareentwicklung zu, sodass eine Code-Migration aufwändiger ist, als ein Neudesign und eine Re-Implementierung. Ebenso können viele generelle Funktionalitäten die in den Altsystemen aufwändig individuell implementiert wurden, heute von den fachlichen Microservcie-Modulen als Services der Plattform konsumiert werden, so z.B. Services für das Caching , Workflow Engines, Berechtigungsmanagement-Services, Archivierungs- und Speicherservices, Identifikations- und Authentifikationsservices, Integrationskonnektoren, API-Repository- und Managementfunktionen, Datenvirtualisierungs-Services, Messaging Broker oder serverlose Frameworks oder Event-Bus, sodass Plattformen heute auch als Entwicklungsumgebungen angese-

hen werden können. Neuentwicklungen können sich so vollständig auf die fachlogischen Problemstellungen konzentrieren – und das vor dem Hintergrund der inzwischen verfügbaren Struktur- und Inhaltsstandards wie z.B. FHIR in Verbindung mit SNOMED.

Die Evolution hin zu Cloud Native Anwendungen muss als multidimensionaler Ansatz gesehen werden, der nicht nur die technischen Aspekte betrifft, sondern auch Kultur, Organisation und Denken in den Entwicklungsabteilungen der Softwareindustrie. "This cloud-native thing is NOT a big-bang approach and doing so will backfire incredibly hard. ... Cloud native is an adjective that describes the applications, architectures, platforms/infrastructure, and processes, that together make it *economical* to work in a way that allows us to improve our ability to quickly respond to change and reduce unpredictability. This includes things like services architectures, self-service infrastructure, automation, continuous integration/delivery pipelines, observability tools, freedom/responsibility to experiment, teams held to outcomes not output, etc."[442]

Mit Blick auf die gute Differenziertheit und Modularisierung des medizinischen Vorgehens sind viele korrespondierende IT-Funktionalitäten ebenso gut abgrenzbar und damit modular realisierbar. Eine Wunddokumentation muss nicht mit dem Rest der KIS-Welt eng verbacken sein und ist selbst sogar noch weiter zerlegbar, eine Diagnosedokumentation im Grunde bestehend aus einer Diagnoseliste und einer Diagnoseerfassung ist ebenfalls gut isolierbar und so lassen sich viele weitere Beispiel anbringen. Was für den klinischen Teil des KIS gilt, gilt auch in vielen Teilen für den administrativen Teil. Dort haben bereits große Hersteller begonnen, Cloud-Produkte auszurollen. Im Klinischen Teil ist es evident, im Zentrum ein interoperables offenes Patientenakten-Dossier zu konzipieren, das ebenfalls als Microservice dann mit den vielen notwendigen Plug-Ins interagieren bzw. diese aufrufen kann.

Dabei kann als Alternative zu einer völligen Neuentwicklung ("Big Bang"), die ein Legacy-Hersteller in der Regel organisatorisch und finanziell überfordert, auch ein schrittweises migratives Vorgehen angegeben werden, bei dem unter Aspekten des Domain-Driven Design Fachfunktionalitäten isoliert und als Microservice-Module neu entwickelt und kontextuell in das Altsystem integriert werden. Eine Liste möglicher Kandidaten findet sich in Kapitel 4.4.5. Dabei kann eine kontextsensitive Aufrufintegration von Microservices aus dem Legacy-System heraus ebenfalls gut realisiert werden, sodass für einen Übergangszeitraum die Koexistenz beider Ansätze möglich ist. Ergänzend muss ggf. ein Zugriff auf die gekapselten Daten des CMSM aus Funktionalitäten des Legacy-Systems heraus zusätzlich implementiert werden, umgekehrt kann es auch hilfreich sein, stufenweise Zugriffs-Services von CMSM auf Legacy-Daten für wichtige Shared Context zu implementieren.

Zukünftige Architekturen für eine vollumfängliche Cloud-Fähigkeit sind **Cloud Native KIS**, die auf Basis von erprobten Cloud-Plattformen und Nutzung der vorhandenen standardisierten Dienste verschiedener Schichten dieser auf der Ebene des User Layers aus fachlogischen Microservice-Modulen bestehen, die nach dem Prinzip maximale Kohäsion und lose Kopplung implementiert sind (siehe Beispiel Abb. 4-9). Dabei bieten die vielfältigen und differenzierten Standards der Health IT - so vor allem FHIR von HL7, IHE IT-Infrastructure und Profile, DICOM und die vielfältigen Semantikkataloge von ICD, ICPM über LOINC bis SNOMED, aber auch definierte medizinische Stadien und Einteilungen, eine sehr gute Basis für das Design und die

[442] Quelle: https://www.infoq.com/articles/cloud-native-panel/.

interoperable standardkonforme Implementierung von medizinischen, aber auch administrativen Microservices.

Zusammenfassend ergeben sich **folgende Lösungsvorschläge für die Legacy-Systeme/Hersteller**:

- Öffnung der Systeme durch Ergänzung um FHIR-Services zum Abruf und ggf. der Rückübergabe wesentlicher (Kontext)Daten an/von Cloud-Subsysteme und -Anwendungsmodule, damit Ermöglichung der Integration innovativer Funktionsmodule von Drittanbietern.
- Implementierung von GUI-Elementen zum Aufruf von Cloud-Anwendungsmodulen an geeigneten Stellen bzw. eine generische parametrierbare Aufruf-Bildschirmseite/ Menüleiste
- Zurverfügungstellung oder Ankopplung eines (Clinical) Contextmanagers und eines Event-Bus für System-Offenheit und moderne Interoperabilität
- Konkrete Kontextlieferungen bzw. FHIR-Services für von vielen Cloud-Modulen benötigten Kontextdaten wie Patient, Fall, Auftrag, Diagnosen usw.
- Öffnung und Interoperabilität in dem Sinne, dass Repository-Inhalte und Semantik auch aus DaaS-Instanzen bezogen/genutzt werden können.
- Anbindung von in der Cloud verfügbaren Basisdiensten wie z.B. Single Sign On, Policy- und Rechtemanagement, Kryptographiedienste, Pseudonymisierungsdienste, Zeitsynchronisationsdienste
- Sukzessive Umstellung von Anwendungsfunktionalitäten auf CMSM

Anforderungen an die CMSM und CMSM-Hersteller:

- Berücksichtigung der internationalen Standards für Domänenmodell, Semantik und Interoperabilitäts-API, vor allem von HL7, IHE und SNOMED, aber auch andere Semantikstandards
- Offengelegtes Interoperabilitäts-API
- Hohe Aufgabenangemessenheit der GUI
- Durchgehend Web-basiert und Web-nutzbar
- Responsives Verhalten
- Bezug von standardisierter Semantik und Bezugsobjekten wo möglich aus verfügbaren Cloud-Repositories (DaaS-Instanzen)
- Nutzung von Open Source Werkzeugen, Bibliotheken und Komponenten für die Implementierung

Abschließend sei hinsichtlich der Migration auf einen praxisorientierten 8-Schritte Vorschlag verwiesen[443]:

- Entwicklung einer DevOps-Kultur nebst Praktiken
- Beschleunigung bestehender Anwendungen mithilfe “schneller Monolithen”, d.h. Migration der aktuellen monolithischen Architektur zu einer modulareren, service-basierten Architektur mit API-basierten Kommunikation wo möglich

[443] Quelle: https://www.redhat.com/cms/managed-files/mi-path-to-cloud-native-apps-ebook-f12255cs-201805-a4-de.pdf.

- Nutzung von Anwendungs-Services für eine schnellere Entwicklung
- Auswahl der richtigen Tools für die richtigen Aufgaben
- Bereitstellung einer bedarfsabhängigen Self-Service-Infrastruktur
- IT-Automatisierung zwecks Beschleunigung der Anwendungsbereitstellung
- Nutzung von CD (Continuous Delivery)-Prozessen und fortschrittlichen Bereitstellungstechniken
- Entwicklung einer modulareren Architektur

6.3 Vorschläge für mehr Cloud-Souveränität in Deutschland und Europa

Aus Sicht des europäischen Datenschutzes und der deutschen Schweigepflicht samt Beschlagnahmeschutz ist es problematisch, dass die wohl leistungsstärksten Cloud-Angebote derzeit von US-Unternehmen ausgehen. Dieser Herausforderung kann man insbesondere mit den beiden im Folgenden beschriebenen Maßnahmen begegnen.

6.3.1 Entwicklung und Stärkung originär europäischer Cloud-Angebote

Im Sinne des europäischen Technologie- und Wirtschaftsstandortes könnte staatlicherseits die Entwicklung originär europäischer Cloud-Technologien und deren Vermarktung gefördert werden. Dies muss nicht zwingend durch direkte Subventionierung bzw. Anschubfinanzierung geschehen, sondern kann auch durch eine Koordination im europäischen Staatenverbund wie bei GAIA-X geschehen. Hierdurch wurde letztlich eine private Kooperation von Unternehmen angestoßen, die auch US-Anbieter nicht ausschließt,[444] aber vor allem auch der Entwicklung sowie in Zukunft dem strukturierten, transparenten und vertrauenswürdigen Angebot von Cloud-Leistungen in Europa dienen soll. Dies ist aus Sicht der Verfasser dieses Gutachtens ein Schritt in die richtige Richtung, auch wenn es zweifelsohne eine große Herausforderung sein wird, in Europa technologisch wirklich Anschluss zu finden.

6.3.2 Cloud nach dem Treuhandmodell

Eine mögliche Lösung, durch welche die technischen Vorteile der Cloud-Angebote von US-Konzernen mit den strengen europäischen Datenschutz-Anforderungen[445] vereinbart werden können, stellt das sogenannte Treuhandmodell dar. Dieses soll im Folgenden anhand eines Beispiels erläutert werden, das tatsächlich praktiziert wird und möglicherweise ausgebaut werden kann, ohne dass damit eine Einschränkung des Modells auf die hier genannten Unternehmen verbunden wäre:

Um hohen (datenschutz-)rechtlichen Anforderungen Rechnung zu tragen, ohne dass Kunden dabei auf die Angebote großer US-amerikanischer Anbieter verzichten müssen, betreibt Microsoft in Kooperation mit der Deutschen Telekom (bzw. T-Systems) seit 2015 die sogenannte Microsoft Cloud Deutschland nach dem Treuhandmodell. Dabei handelt es sich um eine isolierte, aus zwei deutschen Rechenzentren betriebene Instanz der Microsoft Azure Cloud, deren physischen und logischen Zugriff die Deutsche Telekom als Treuhänder verwaltet, steuert,

[444] Letztlich sollen über GAIA-X die Lokalisierung von Daten und die Zugriffe auf diese für den Cloud-Nutzer vorab und laufend transparent gemacht werden, so dass dieser entscheiden kann, welche Cloud-Angebote er für welche Daten nutzen möchte. Die Angebote von US-Anbietern, auch wenn sie auf US-Server zurückgreifen, sind damit nicht ausgeschlossen, der Umfang ihrer Nutzung ist durch die datenschutzrechtliche Lage jedoch eingeschränkt.

[445] Siehe dazu oben Kapitel 3, S. 49 ff., sowie zusammenfassend auch Kapitel 5.2, S. 267 ff.

überwacht und protokolliert. Ein Transfer zu Microsoft in die USA als unsicheren Drittstaat ist somit für die eigentlichen Geschäftszwecke nicht notwendig, was aber grundsätzlich auch bei jeder anderen, von Microsoft selbst in der EU gehosteten Cloud der Fall wäre. Den Unterschied macht hier der Einsatz der Deutschen Telekom als Datentreuhänder. Durch diesen Schritt wird der physische und logische Zugriff auf in der Cloud gespeicherte Daten für Microsoft ohne die Zustimmung der Deutschen Telekom praktisch nicht möglich. In der Folge kann auch kein Durchgriff auf diese Daten durch US-Behörden nach dem U.S. CLOUD Act unter Rückgriff auf Microsoft erfolgen.

Ein direkter Anspruch von US-Behörden gegenüber der Deutschen Telekom scheidet zwar auf Grundlage der einschlägigen US-amerikanischen Rechtsvorschriften nicht generell aus, da die Deutsche Telekom mit der T-Mobile US, Inc. zumindest auch über eine Tochtergesellschaft mit nicht unerheblichem Geschäft in den USA verfügt. Dies ändert jedoch nichts daran, dass die deutsche Muttergesellschaft und ihre deutschen Töchter nach deutschem Recht ausschließlich deutschem und europäischem öffentlichen Recht unterliegen.[446] Und aufgrund des Umstandes, dass Hauptgeschäft und Konzernzentrale der Deutschen Telekom nach wie vor in Deutschland liegen, besteht hier die begründete Erwartung, dass sich die Muttergesellschaft und die deutschen Töchterunternehmen vorrangig an deutsches Recht halten werden.[447]

Während ein solches Treuhandmodell also aus rechtlicher Sicht einen datenschutzkonformen Cloud-Betrieb ermöglichen kann, stehen ihm auf der anderen Seite wirtschaftliche und technische Herausforderungen entgegen. So erhöht das Telekom-Treuhandmodell z. B. im Fall der SAP-Cloud-Services, also des Betriebs eines SAP ERP-Systems in der von der Telekom administrierten Microsoft Cloud Deutschland, die Kosten gegenüber dem Betrieb in einer Cloud ohne Treuhandmodell um ca. 10-20%. Neben diesem wirtschaftlichen Nachteil machen aus technischer Sicht höhere Latenzen (Zeitverzögerungen) bei weltweiter Nutzung das Treuhand-Angebot weniger attraktiv. Diese Latenzen entstehen dadurch, dass Rechenzentren in Deutschland die weltweiten Standorte der nutzenden Großunternehmen bedienen müssen und Rechenzentren mit gespiegelten Datenbeständen in unsicheren Drittstaaten im Treuhandmodell nicht möglich sind.

Für Krankenhäuser innerhalb von Deutschland dürften jedoch keine nennenswerten Latenzen auftreten. Auch ist die hohe Skalierbarkeit einer weltweiten Cloud für Krankenhäuser mit ihren eher deterministischen Lasten nicht unbedingt erforderlich.

---

[446] Eine extraterritoriale Geltung ausländischen öffentlichen Rechts, einschließlich des Strafverfahrensrechts, wird insoweit nicht anerkannt, wenn dies auch eine Kooperation und mittelbare Wirkung im Rahmen von Rechtshilfeersuchen nicht ausschließt. Im Gegensatz zum Zivilrecht ist hier auch keine Rechtswahl per Vertrag zulässig.

[447] Der französische Conseil d'État hat im einstweiligen Rechtsschutz selbst zu Microsoft Ireland ausgeführt, dass kein Anlass bestehe, bloße Vermutungen im Hinblick auf einen Zugriff aus unsicheren Drittstaaten als Anlass für eine Untersagung der Datenverarbeitung heranzuziehen; s.o. S. 61 f. Ob man im Hinblick auf US-Konzerne wie Microsoft hier generell von bloßen Vermutungen sprechen muss, kann man anzweifeln; vgl. den öffentlich gewordenen Fall einer Herausgabeanordnung des U.S. Departments of Justice gegenüber Microsoft im Hinblick auf in Irland belegene Daten, der bis vor den obersten Gerichtshof der USA gelangte: 584 U.S. ___, 138 S. Ct. 1186 (2018). Im Fall eines Unternehmens mit Konzernzentrale und Tätigkeitsschwerpunkt in Deutschland besteht aber grundsätzlich ein berechtigtes Vertrauen dahingehend, dass deutsches und europäischen Recht eingehalten wird, s. oben S. 62, Fn. 109.

Im Fall der Microsoft Cloud Deutschland haben sich die genannten Nachteile in der Vergangenheit zwar in mangelndem Interesse der Kunden niedergeschlagen, weshalb Microsoft das Angebot für Neukunden nicht mehr anbietet. Es könnte allerdings sein, dass solche Treuhandmodelle nach der Schrems II-Entscheidung des EuGH wieder mehr in den Fokus sowohl potenzieller Anbieter als auch Nutzer gelangen, was grundsätzlich auch für Krankenhäuser zu befürworten wäre.[448]

[448] Skeptisch mit Blick auf die Kosten einer Treuhandlösung für Microsoft 365 an Schulen (Stand: 18.09.2020): https://datenschutz-schule.info/2020/09/18/microsoft-365-zukunft-fuer-schulen-ungewiss/. Je mehr Kunden eine solche Treuhandlösung im Sinne einer Community-Cloud für Anwender mit höherem Schutzbedarf hätte, desto geringer dürften allerdings die Kosten für den einzelnen Kunden ausfallen.

7 Abkürzungsverzeichnis

Abkürzung	Langtext
ABAC	Attribute Based Access Control
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AfG	Ausschuss für Gesundheit
AHA	American Hospital Association
AISEC	Fraunhofer-Institut für Angewandte und Integrierte Sicherheit
AMC	Advanced Medical Communication Holding GmbH
AMTS	Arzneimitteltherapiesicherheit
API	Application Programming Interface (Anwendungsprogrammierschnittstelle)
APIS	Arztpraxisinformationssystem
BAS	Bundesamt für soziale Sicherung
BB	Brandenburg (ISO 3166)
BCM	Business Continuity Management
BDSG	Bundesdatenschutzgesetz
BE	Berlin (ISO 3166)
BeckOK	Beck'scher Online-Kommentar
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien
BMG	Bundesgesundheitsministerium
BMP	bundeseinheitlicher Medikationsplan
BMWi	Bundesministerium für Wirtschaft und Energie
BRAO	Bundesrechtsanwaltsordnung

BSI	Bundesamt für die Sicherheit in der Informationstechnik
BW	Baden-Württemberg (ISO 3166)
BY	Bayern (ISO 3166)
BYOD	Bring Your Own Device
CCOW	Clinical Context Object Workgroup
CCRA	Cloud Computing Reference Architecture
CDA	Clinical Document Architecture
CEN	Comité Européen de Normalisation
CHIME	College of Healthcare Information Management Executives
cloudKIS	Cloud-basiertes Krankenhausinformationssystem
CMSM	Cloud MicroService Modul
CMSMS	Content-Management-System Made Simple
COPS	Common Open Policy Service
CSV	Comma-separated values
DaaS	Data as a Service
DAC	Discrenary Access Control
D-A-CH	Deutschland Österreich Schweiz
DDD	Domain Driven Design
DICOM	Digital Imaging and Communication in Medicine
DIGA	Digitale Gesundheitsanwendung
DKBFVO	Datenschutzkirchenbezirksfestlegungsverordnung
DKG	Deutsche Krankenhausgesellschaft
DRG	Diagnosis Related Group
DSDEVO	Datenschutzdurchführungs- und -ergänzungsverordnung
DSG-EKD	Datenschutzgesetz der evangelischen Kirche in Deutschland
DSGVO	Datenschutzgrundverordnung
DuD	Datenschutz und Datensicherheit (Zeitschrift)

EAV	Entity Attribute Value
ECCF	Enterprise Consistency and Conformity Framework
EDSA	Europäischer Datenschutzausschuss
EEG	Elektroencephalogramm
EGMR	Europäischen Gerichtshofes für Menschenrechte
EHR	Electronic Health Record
EIS	Enterprise Information System
EKG	Elektrokardiogramm
EMR	Electronic Medical Record
EMRAM	Electronic Medical Records Adoption Model
ENV	Europäischer Normvorschlag
EPA	Elektronische Patientenakte
ERP	Enterprise-Resource-Planning
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUV	Vertrag über die Europäische Union
EWR	Europäischer Wirtschaftsraum
FaaS	Function as a Service
FHIR	Fast Healthcare Interoperability Resources
FINK	Finanzbuchhaltung im Krankenhaus
GDSG	Gesundheitsdatenschutzgesetz
gem.	gemäß
GG	Grundgesetz
ggf.	gegebenenfalls
GKV	Gesetzliche Krankenversicherung
GKV	Gesetzliche Krankenversicherung
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie

grds.	grundsätzlich
GUI	Graphical User Interface
HB	Bremen (ISO 3166)
HE	Hessen (ISO 3166)
Hg.	Herausgeber
HH	Hamburg (ISO 3166)
HIMSS	Healthcare Information and Management Systems Society, Inc.
HL7	Health Level 7
HPD	Health Care Provider Directory
Hrsg.	Herausgeber
Hs.	Halbsatz
IaaS	Infrastructure as a Service
ICD	International Statistical Classification of Diseases and Related Health Problems
IEEE	Institute of Electrical and Electronics Engineers
IHE	Integrating the Healthcare Enterprise
IOP	Interoperabilität
ISM	Interoperabilitätsspezifiaktions-Matrizen
ISMS	Informationssicherheitsmanagementsystem
ISO	International Standards Organisation
IST	Interoperability Specification Templates
IT	Informationstechnologie
ITSVO	Verordnung zur Sicherheit der Informationstechnik
JSON	JavaScript Object Notation
juris	Rechtsportal der juris GmbH, u.a. mit einer Datenbank von Gerichtsentscheidungen

k. A.	keine Angabe(n)
KAL	Klinisches Arbeitsplatzsystem
KBV	Kassenärztliche Bundesvereinigung
KDG	Gesetz über den kirchlichen Datenschutz
KDSGO	kirchliche Datenschutzgerichtsordnung
KG	Kammergericht (Oberlandesgericht in Berlin)
KHDSG	Krankenhausdatenschutzgesetz (Bremen)
KHG	Krankenhausfinanzierungsgesetz
KHSFV	Krankenhausstrukturfonds-Verordnung
KHZG	Krankenhauszukunftsgesetz
KIM	Kommunikation im Medizinwesen
KIS	Krankenhausinformationssysteme
KOLK	Kosten- Leistungsrechnung im Krankenhaus
LDA	Bayerisches Landesamt für Datenschutzaufsicht
LDSG	Landesdatenschutzgesetz
LDt	Labordatenträger
LDT	Labordatentransfer
LfD	Landesbeauftragter für den Datenschutz
LIS	Laborinformationssystem
LKHG	Landeskrankenhausgesetz
LVwVfG	Landesverwaltungsverfahrensgesetz
MAC	Mandatory Access Control
MAIK	Materialwirtschaft im Krankenhaus
mCloud-KIS	Modulares Cloud-basiertes Krankenhausinformationssystem
MDK	Medizinischer Dienst der Krankenversicherung
MDR	Metadata Registry
MIO	Medizinische Informationsobjekte
MPI	Master Patient Index

MV	Mecklenburg-Vorpommern (ISO 3166)
NCAV	Native Cloud Applications
NI	Niedersachsen (ISO 3166)
NIST	National Institute of Standards and Technology des US Department of Commerce
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NW	Nordrhein-Westfalen
OAuth	Open Authorization
ÖGDG	Gesetz über den öffentlichen Gesundheitsdienst
OH-KIS	Orientierungshilfe Krankenhausinformationssysteme
OLG	Oberlandesgericht
OPS	Operationen- und Prozedurenschlüssel
ORM	Order Entry Result Reporting
OSGi	Open Services Gateway Initiative
PaaS	Platform as a Service
PACS	Picture Archiving and Communication System
PAP	Policy Administration Point
PAS	Patientenaktensystem
PathIS	Pathologieinformationssystem
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PRP	Policy Retrieval Point
RBAC	Role Based Access Control
Rdnr.	Randnummer
RDV	Recht der Datenverarbeitung (Zeitschrift)
RIA	Rich Internet Application

RIM	Reference Information Model
RIS	Radiologieinformationssysteme
RKI	Robert Koch-Institut
RP	Rheinland-Pfalz (ISO 3166)
RPC	Remote Procedure Call
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RZ	Rechenzentrum
SaaS	Software as a Service
SAIF	Services-Aware Interoperability Framework
SAML	Security Assertion Markup Language
SCC	Standard Contractual Clauses
SGB	Sozialgesetzbuch
SH	Schleswig-Holstein (ISO 3166)
SL	Saarland (ISO 3166)
SMC-B	Security Module Card - Betriebsstätte, kurz SMC-B
SN	Sachsen (ISO 3166)
SNOMED	Standardized Nomenclature of Medicine
SOA	Serviceorientierte Architektur
SOAP	Simple Object Access Protocol
SPOF	Single Point of Failure
SSO	Single Sign On
ST	Sachsen-Anhalt (ISO 3166)
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TCP/IP	Transmission Control Protocol/Internet Protocol
TH	Thüringen (ISO 3166)
TI	Telematik-Infrastruktur

TOM	Technisch Organisatorische Maßnahme
Unterabs.	Unterabsatz
VNA	Vendor Neutral Archive
VSSR	Vierteljahresschrift für Sozialrecht (Zeitschrift)
WHO	World Health Organization
XACML	eXtensible Access Control Markup Language

8 Abkürzungen der Bundesländer

Die deutschen Bundesländer werden im vorliegenden Gutachten nach der internationalen Norm ISO 3166 (ohne vorangestelltes Kürzel DE für Deutschland) wie folgt abgekürzt:

BW	Baden-Württemberg
BY	Bayern
BE	Berlin
BB	Brandenburg
HB	Bremen
HH	Hamburg
HE	Hessen
MV	Mecklenburg-Vorpommern
NI	Niedersachsen
NW	Nordrhein-Westfalen
RP	Rheinland-Pfalz
SL	Saarland
SN	Sachsen
ST	Sachsen-Anhalt
SH	Schleswig-Holstein
TH	Thüringen

9 Glossar

Begriff	Erläuterung
Anonymisierung	Anonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, d.h. jeglicher Personenbezug wird entfernt. Dabei muss auch berücksichtigt werden, dass Daten, die evtl. zu einer faktischen Deanonymisierung führen können, ebenfalls entfernt oder vergröbert werden.
Anwendungslandschaft	Die Summe von verschiedenen Softwareanwendungen oder Anwendungssystemen, die für einen bestimmten Zweck zusammenarbeiten und so ein funktionierendes Gesamtsystem darstellen.
Anwendungssystem	Ein anwendbares IT-System, umfasst die Hardware, Betriebssystem, notwendige Middleware, die Anwendungs-Software sowie evtl. für die Anwendung notwendige Peripherie.
Auftragsverarbeiter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen (und somit weisungsgebunden) verarbeitet (Art. 4 Nr. 8 DSGVO).
Authentifikation	Vorgang für die Überprüfung der Echtheit eines Objektes, z.B. die Identitätsprüfung eines Benutzers für die Zulassung zu einem System.
Berechtigungs-/Rechtemanagement	Alle softwaretechnischen Mechanismen und zughörige Daten, um Berechtigungen zur Nutzung von Funktionen und Daten (Sicherheitsobjekte) eines Informationssystems für eine Person oder eine Systemkomponente (Sicherheitssubjekt) zu formulieren und zur Laufzeit durchzusetzen.
Best of Breed	Eine Strategie, ein gesamtbetriebliches heterogenes Informationssystem aus bestmöglich passenden Subsystemen zusammenzusetzen.
Bezugsobjekt	Ein Datenobjekt, auf das eine Verarbeitung bzw. ein System sich beziehen muss, dass aber nicht selbst Gegenstand der eigentlichen Verarbeitung ist. Z.B. Materialien, Organisationen etc.
Bezugsobjektrepository	Eine informationstechnische Zusammenstellung aller für eine Softwareanwendung benötigten Bezugsobjekte, damit Benutzer diese referenzieren können.

Biometrische Daten	Mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten (Art. 4 Nr. 14 DSGVO).
Bounded Context	Zentrales Entwurfsmuster beim Domain Driven Design. Beschreibt den abgrenzbaren Kontext für ein Team, einen Microservice usw., in diesem Sinne der für einen funktionalen Zweck/für einen Microservice relevante Realweltausschnitt.
Boxcrypting	Verschlüsseln von Daten und Dateien in einem Container für die sichere Speicherung z.B. in der Cloud.
CDA-Dokument	Ein Dokument im Format der von HL7 definierten Clinical Document Architecture-Struktur. Besteht aus einem Header mit allen Metadaten und einem Body mit den Inhaltsdaten jeweils im XML-Format.
Client-Server	Ein Muster für eine Beziehung, in der Informatik zwischen zwei Computern, wobei der Client Ressourcen des Servers nutzt auf Basis bestimmter Anforderungen/Aufrufe.
Cloud Native Anwendung	Eine Softwaresystem, das optimiert für den Einsatz als Cloud-Anwendung auf Basis von Microservices konzipiert und realisiert wurde und dabei auch die Services einer Cloud-Plattform nutzt.
Cloud-Computing	Einerseits die Zurverfügungstellung von IT-Ressourcen wie Infrastruktur, Plattform oder Anwendungssoftware als skalierbarer Services zumeist über das Internet auf Basis spezieller Cloud-Computing Architekturen. Andererseits aber auch eine spezielle Architektur von Anwendungen, die besonders gut in Cloud-Umgebungen eingesetzt werden können.
Cloudifizierung	Die Überführung/die Migration eines Legacy-Systems/einer Altanwendung in eine Cloud Native Anwendung, um diese Cloud-fähig zu machen.
Community Cloud	Eine Cloud, in der sich - zumeist gleichartige - Unternehmen bzw. Organisationen Software und ggf. auch Daten teilen. Ziel ist die bessere Zusammenarbeit und/oder bessere Nutzung von Ressourcen und gemeinsamen Daten.

Compliance	Strategie, Maßnahmen und Sicherstellung der Einhaltung und Befolgung von betrieblichen Vorgaben zur Vermeidung von Risiken und Schadensereignissen, die aus Nichteinhaltung gesetzlicher oder sonstiger Regelungen entstehen können. IT-Compliance entsprechend, sodass der IT-Einsatz durch technisch-organisatorische Maßnahmen und inhärenten Lösungsmerkmalen z.B. der Anwendungssoftware rechtmäßig ist und rechtskonform funktioniert.
Container	Allgemeiner Begriff, um gewisse informatische Artefakte gemeinsam zu kapseln. Dies können z.B. virtuelle Maschinen sein oder Plattformen oder aber einzelne selbstständig lauffähige Microservice-Module.
Datenminimierung	Siehe Datensparsamkeit.
Datenschutzkonferenz	Konferenz der Datenschutzbeauftragen des Bundes und der Länder in der Bundesrepublik Deutschland.
Datensparsamkeit	Es werden nur genau jene Daten erhoben und gespeichert, die für die Zwecke der Verarbeitung unbedingt benötigt werden. Für jedes Datum sollte begründbar sein, warum es erhoben, gespeichert und ggf. verarbeitet wird.
Datenübertragbarkeit	Das Recht und die Möglichkeit einer Person (einer Organisation) bei Wechsel von Anbieter bzw. Software die eigenen Daten in einem transparenten offenen Format exportieren und mitzunehmen bzw. beim neuen Anbieter/in die neue Software einspielen zu können.
Deployment	Das Ausliefern/Verteilen von Software auf verschiedene Zielsysteme, auf denen diese Software dann ausgeführt werden kann. Vor allem auch im Zuge von Fehlerbehebungen und dem Aufspielen neuer Versionen.
DICOM	Kommunikations- und Interoperabilitätsstandard für Medizinische Bilddaten und Videos.
Digitales Ökosystem	Der Zusammenschluss von vielen unterschiedlichen Informationssystemen oder Anwendungen für einen bestimmten meist branchenspezifischen und regionalen Aspekt für eine effektive Zusammenarbeit verschiedenster Organisationen, auch um gemeinsam Daten und Funktionalitäten zu teilen und um Prozesse effektiv abzuwickeln.

Domain Driven Design	Spezielle Vorgehensweise, um komplexe große Softwaresysteme modular und orientiert an den in einer Domäne bestehenden fachlichen Daten- und Bearbeitungs-Erfordernissen zu entwerfen und zu realisieren. Ziele sind u.a. modulare und gut wartbare und weiterentwickelbare und zeitnah deploybare Softwaremodule, die in Summe ein System ergeben.
Drittlandübermittlung	Die Übermittlung von personenbezogenen Daten in ein Land außerhalb der EU/des EWR. Neben den allgemeinen Voraussetzungen für die Übermittlung von Daten muss nach den Art. 45 ff. DSGVO zudem ein angemessenes Datenschutzniveau beim Empfänger vorliegen. Die Angemessenheit des Datenschutzniveaus ist durch eine der in Art. 46 ff. DSGVO verankerten rechtlichen Transfertools sowie gegebenenfalls ergänzenden technischen, vertraglichen oder organisatorischen Maßnahmen nach der entsprechenden Rechtsprechung des EuGH sicherzustellen.
eHealth-Konnektor	Eine spezielle Hardware/Software-Box zur sicheren Anbindung und Interoperabilität zwischen Informationssystemen von Gesundheitseinrichtungen an die nationale Telematik-Infrastruktur.
Eigenbetrieb	Eine Organisationsform von öffentlichen Betrieben (einschließlich Krankenhäuser). Der Eigenbetrieb verfügt über keine eigene Rechtspersönlichkeit, sondern wird als Sondervermögen des öffentlichen Trägers behandelt. Im Gegensatz zum Regiebetrieb besitzt der Eigenbetrieb eigene Organe (wie eine Geschäftsführung) und führt einen Stellenplan.
Einwilligung	Eine von der betroffenen Person freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist (Art. 4 Nr. 11 DSGVO).
Elastizität	Sich an die Echtzeitlast bzw. -nachfrage anpassende Infrastruktur durch Schaffung neuer virtueller Maschinen und Container.
Elektronische Patientenakte	Digital gespeicherte medizinische Informationen beliebiger Granularität wie z.B. Befunde, Röntgenbilder, Diagnosen etc. zu einem Patienten. Wird auch oft Synonym für ein ganzes Patientenaktensystem verwendet, also für die Daten und die zugehörigen Funktionalitäten. Derzeit oft als institutionelle EPA in den Systemen der einzelnen Versorgungseinrichtungen zu finden.

Enterprise (Information) System (EIS)	Ein gesamtbetriebliches Informationssystem für alle Bereiche/Abteilungen eines Unternehmens.
Europäischer Wirtschaftsraum (EWR)	Der Europäische Wirtschaftsraum wurde 1994 eingerichtet, um die Bestimmungen des EU-Binnenmarkt auf die Länder der Europäischen Freihandelszone (EFTA) auszudehnen. Der EWR umfasst damit die Mitgliedstaaten der EU sowie die Länder der EFTA mit Ausnahme der Schweiz, letztlich also neben den EU-Staaten die Länder Norwegen, Island und Liechtenstein.
Fachfunktion	Eine Softwaredialogfunktion zur Unterstützung einer dedizierten fachlichen Aufgabe eines Benutzers.
GAIA-X	Europäisches Großprojekt bzw. Initiative zum Aufbau europäischer Cloud-Infrastrukturen für ein europäisches digitales Ökosystem. Ziel ist auch, den Technologievorsprung von US-Unternehmen auf europäischer Ebene einzuholen.
Genetische Daten	Personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden (Art. 4 Nr. 13 DSGVO).
Gesundheitsdaten	Personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (Art. 4 Nr. 15 DSGVO).
Governance	Vieldeutiger Begriff, oft verwendet für Strategie und Umsetzung und Kontrolle bestimmter Unternehmens-Prinzipien und Policies in den Unternehmensalltag.
Horizontales System/Funktion	Ein System/eine Anwendungssystemfunktion, das/die gleichartig von vielen verschiedenen oder allen Abteilungen eines Unternehmens oder von verschiedenen Unternehmen eingesetzt werden kann.
IaaS (Infrastructure as a Service)	Ein Cloud-Service bzw. Geschäftsmodell von Cloud-Unternehmen, ihren Kunden Infrastruktur wie z.B. Rechnerressourcen anzubieten bzw. zu hosten. Oft nutzungsorientierte Erstattungsmodelle, daher keine Investitionskosten für den Kunden.

Identifikation	Die Feststellung der Identität eines (Informations-)Objektes bzw. einer Person. Eindeutige Identitäten sind in vielerlei Hinsicht in verteilten Systemen nicht nur für Personen sondern auch für Geschäftsobjekte und Bezugsobjekte wichtig. Auch Implementierungs- und Laufzeitobjekte sollten eine eindeutige Identität haben.
Integrität	Die Integrität ist ein zentrales Konzept in der Informatik bedeutet allgemein die Richtigkeit und Widerspruchsfreiheit von Daten und Algorithmen. Die Sicherstellung der Integrität in einem verteilten System ist eine besondere Herausforderung, da es zum Beispiel durch nebenläufige Prozesse oder zeitliche Verzögerungen zu einer kurzzeitigen oder dauerhaften Nicht-Integrität kommen kann. Hieraus resultieren dann im ungünstigsten Fall Folgefehler.
Justitiablität	Im Kontext der Datenverarbeitung die Anforderung, dass Sachverhalte so abgelegt sind oder verarbeitet werden, dass sie im Rechtsfall gerichtlich beurteilt und entschieden werden können. Hierzu müssen in Informationssystem gewisse Mechanismen implementiert werden, um zum Beispiel die Zurechenbarkeit oder die Nichtabstreitbarkeit von Übermittlungen oder Kenntnisnahme von Daten nachweislich sicherzustellen.
Kernsystem	Im Rahmen einer Anwendungslandschaft bestehend aus vielen verschiedenen Informationssystemen jenes System, dass die Kernfunktionalität für die betriebliche Datenverarbeitung beinhaltet und dann das verschiedene andere sogenannte Subsysteme angeschlossen sind.
Klassenmodell	Ein informationstechnisches Modell eines Realweltausschnittes als Grundlage für die Implementierung von Anwendungssoftware im Rahmen der objektorientierten Analyse und Entwurfs. Auch Klassendiagramm genannt. In der Regel eine grafische Darstellung von Objekttypen und deren Beziehungen, mehr technisch orientiert dann eine Darstellung von Klassen, Schnittstellen und deren Beziehungen, wobei eine Klasse Struktur und Verhalten einer definierten Menge von konkreten Objekten beschreibt.
Kohäsion	Bei Entwurf von Anwendungssoftware bzw. Cloud Native Anwendungen das Konzept, dass eine Komponente bzw. ein Microservice so viel wie möglich von dem was er speichern und verarbeiten muss kapselt und nur wenn überhaupt notwendig anderen Komponenten bzw. Microservices über Schnittstellen zur Verfügung stellt.

Konfiguration	Das Festlegen/die Anpassung der Zusammensetzung und der Funktionalität und der Betriebsparameter eines Systems bzw. einer Anwendungssoftware zum Beispiel durch die Ausprägung bestimmter Parameter. Die Summe der festgelegten Parameter ergibt die Konfigurationseinstellung.
Kontextüberschneidung	Die von mehreren Komponenten bzw. Programmen bzw. Microservices in gleicher Weise benötigten Daten als Kontext der gekapselten Speicherung und Verarbeitung. Kontextüberschneidungen führen zu Redundanzen und es müssen Mechanismen für die kontrollierte Redundanz implementiert werden, damit die Integrität im Gesamtsystem sichergestellt werden kann.
Krankenhaus-informationssystem	Das gesamtbetriebliche Informationssystem in einem Krankenhaus zur Unterstützung aller administrativen, logistischen und medizinischen Vorgänge bis hin zum Controlling und dem Qualitätsmanagement – und dies für Krankenhäuser jeglicher Größe und Art. In diesem Sinne gehören auch viele Medizintechnikgeräte zum KIS, die zunehmend auch digital sind, integriert werden und einen Datenaustausch unterstützen.
Kryptographie	Methoden und Werkzeuge zur Verschlüsselung und damit Geheimhaltung von Informationen.
Laufzeitumgebung	Alle Ressourcen wie zum Beispiel Bibliotheken, Schnittstellen, Laufzeitvariablen aber auch Hardware und Softwarekomponenten der Middleware und des Betriebssystems die für die Ausführung eines bestimmten Anwendungsprogramms bzw. eines Anwendungssystems oder eines Microservice vorhanden sein müssen bzw. vorhanden sind. Synonyme sind auch Ausführungsumgebung oder Ablauf Umgebungen, im englischen Runtime Environment RTE.
Layer	In der Informatik für bestimmte System- bzw. Softwarearchitekturen eine Menge von Programmen oder Services, die einer gewissen Klasse von Funktionalitäten zugehören bzw. einem bestimmten Zweck folgen mit dem Ziel der Entkopplung von spezialisierten Funktionalitäten, wobei Programmen oder Services höherer Schichten jene der Schicht darunter nutzen. Bekanntestes Schichtenmodell ist das ISO/OSI- Referenzmodell aus sieben Schichten, in der Softwaretechnik auch das Drei- oder Vierschichtenmodell (bei drei Schichten: Datenhaltungsschicht, Geschäftslogikschicht, Präsentationsschicht)
Legacy-System	Eine etablierte historisch gewachsene Unternehmenssoftware, die aufgrund ihres Alters und der zugrunde liegenden Softwaretechnologien zunehmend zu einer Altlast wird und beginnt zu verrotten.

Logging	Das Aufzeichnen/Protokollieren aller Aktionen in einem Informationssystem. Mit Blick auf den Datenschutz vor allem auch das Protokollieren aller Dateneingaben, Datenveränderungen und Datenlöschungen inklusive der diese durchführenden Benutzer und der genauen Zeitpunkte und ggf. des Bearbeitungskontextes, aus dem heraus die Aktionen erfolgten (z.B. mittels welcher Anwendungsfunktion).
Lose Kopplung	Die Zusammenarbeit von Softwarebausteinen auf Basis minimaler oder keiner Abhängigkeit untereinander. Dies kann zum Beispiel durch den asynchronen Nachrichtenaustausch erreicht werden, architektonisch aber auch durch die Minimierung notwendiger Schnittstellen durch Berücksichtigung einer maximalen Kohäsion der einzelnen Bausteine/Microservices.
Mandant	Ein Kunde (englisch: Tenant für Mieter, Pächter), der in einem mandantenfähigen Laufzeitsystem in einem eigenen Datenhaltungs- und Verarbeitungszusammenhang als im datenschutzrechtlichen Sinne verantwortlichen Stelle Verarbeitungen durchführt.
Mandantenfähigkeit	Die Fähigkeit eines Informationssystems bzw. einer Anwendungssoftware innerhalb einer Laufzeitinstanz eine Verarbeitung von Daten für verschiedene Kunden getrennt vornehmen zu können. Dabei können auch je Mandant bestimmte Konfigurationseinstellungen vorgenommen werden.
Mandantentrennung	Die physische Trennung der Mandanten.
Master Patient Index	Eine Anwendungslösung in einem verteilten System, dass minimale für eine Reidentifikation notwendige demographische Daten zu einer Person (hier einem Patienten) führt und die in den verschiedenen teilnehmenden Systemen für eine Person vergebenen Identifikationsnummern. Damit kann eine eindeutige Personenidentifikation über alle Systeme hinweg gewährleistet werden, auch wenn diese intern verschiedene IDs nutzen.
Mehrfachredundanz	Mehr als zweimalige Auslegung einer Komponente oder von Daten. Beispiele: Vier physisch getrennte Leitungsverbindungen über verschiedene Netzinfrastrukturen zwischen Krankenhaus und Rechenzentrum. Redundante Speicherung von Logfiles auf verschiedenen Platten.

Microservice	Begriff für Architekturmuster und Laufzeitobjekt für kleine gekapselte Funktionalitäten eines Informationssystems, die weitgehend unabhängig gestartet und genutzt werden können. Im Unterschied zu softwaretechnische Bibliotheksfunktionen handelt es sich um anwendungs- domänenorientierte Module mit eigener Verarbeitung, Datenspeicherung und ggf. Oberfläche.
Migration	Die Überführung eines IT-Systems oder von Daten (Datenmigration) in Teilen oder insgesamt in ein anderes Informationssystem. Im Prinzip auf alle Aspekte anwendbar z.B. Migration einer Anwendungssoftware von einer Hardware-/Betriebssystemumgebung auf eine andere, die Migration von Software von einer Programmiersprache in eine andere Sprache, die Migration von Daten von einem Anwendungssystem in ein anderes Anwendungssystem bei Systemwechsel.
Modularisierung	Der Vorgang der Zerlegung/Zergliederung von etwas Ganzem in kleinere Einheiten, in der Softwaretechnik von Software in kleinere abgeschlossene Einheiten, die ggf. miteinander kooperieren.
Modulith	Ein im Prinzip geschlossenes von einem Hersteller stammendes Softwaresystem, das aber im Inneren gut modularisiert ist. Auslieferungen bzw. neue Versionen ggf. auch auf Modulebene möglich.
Monolith	Ein im Prinzip geschlossenes von einem Hersteller stammendes Softwaresystem, das aus einer gesamtheitlichen wenig modularisierten Software besteht. Auslieferung bzw. neue Versionen nur en Block.
Nicht-öffentliche Stelle	Natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, ohne dass sie Teil einer öffentlichen Stelle sind und nur soweit sie keine hoheitlichen Aufgaben der öffentlichen Verwaltung wahrnehmen (§ 2 Abs. 4 BDSG).
Objekttyp	Synonym für "Klasse". Bei der klassenbasierten bzw. objektorientierten Softwareentwicklung ein Repräsentant einer Menge von konkreten Objekten (=Instanzen des Objekttyps). Beschreibt Struktur und Verhalten. Beispiele: Person, Patient, Behandlungsfall, Diagnose. Siehe auch Klassenmodell.
Öffentliche Stelle des Bundes	Eine Behörd, ein Organ der Rechtspflege oder eine andere öffentlich-rechtlich organisierte Einrichtung des Bundes, der bundesunmittelbaren Körperschaften, der Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform (§ 2 Abs. 1 BDSG).

Öffentliche Stelle eines Landes	Eine Behörd, ein Organ der Rechtspflege oder eine andere öffentlich-rechtlich organisierte Einrichtung eines Landes, einer Gemeinde, eines Gemeindeverbandes oder sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform (§ 2 Abs. 2 BDSG).
On-Premises	Betrieb einer Anwendungslösung bzw. einer Anwendungslösungslandschaft vor Ort auf lokalen Servern z.B. im Krankenhaus.
Orchestrierung	Das flexible Kombinieren von Services zu einem sinnvollen Ganzen mit Blick auf die angestrebte Software-Lösung. Im weiteren Sinne insgesamt die Kombination von IT-Ressourcen, z.B. von Containern oder Hardwarelandschaften.
PaaS (Platform as a Service)	Die Zurverfügungstellung einer vollständigen Entwicklungs- oder Bereitstellungsumgebung für bestimmte Kundenklassen, um diesen Bundles von verschiedenartigen Ressourcen (=Plattform) zur Verfügung zu stellen.
Parametrierung	Die Einstellung von System- oder Anwendungsparametern, um Verhalten und Eigenschaften von Systemen ohne spezielle Programmierung anzupassen so z.B. das Einrichten der Parameter und Stammdaten im Rahmen der Systemeinführung zur Herstellung der für den konkreten Betrieb notwendigen Individualität. Der Vorgang selbst wird auch Customizing genannt.
Patch	Neuauslieferung von Softwareteilen oder speziellen Programmen zur Fehlerbehebung ("Bugfix") um Softwarefehler zu beheben, Sicherheitslücken zu schließen oder einzelne Funktionalitäten aufzurüsten. Im Gegensatz zu Updates von Programmsystemen oft nur einzelne Funktionalitäten betreffend.
Performance	Bezogen auf einen bestimmten Aspekt die quantitative Leistung eines Systems, so z.B. die Antwortzeit an der Oberfläche bei gegebener gleichzeitiger Benutzerzahl, der Datendurchsatz z.B. bei Massentransaktionen, mittlere Zugriffszeiten.

Personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (Art. 4 Nr. 1 DSGVO).
Plankrankenhaus	Krankenhaus in privater Trägerschaft, das in den jeweiligen Krankenhausplan eines Bundeslandes aufgenommen wurden.
Portabilität	Die Übertragbarkeit z.B. von Anwendungssoftware auf verschiedene Betriebssysteme, von Daten in verschiedene Anwendungssysteme usw.
Private Cloud	Cloud-Computing-Bereitstellungmodell, bei dem die Dienste bzw. Anwendungslösungen ausschließlich einem Kunden zur Verfügung stehen. Dies kann in Form von IaaS oder PaaS geschehen bis hin zu ganzen Anwendungslösungen. Verbindet Vorteile von eigenen Unternehmenslösungen mit denen von Cloud-Lösungen.
Pseudonymisierung	Die Pseudonymisierung wird in Art. 4 Nr. 5 DSGVO wie folgt definiert: Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Zur Umsetzung dieser Anforderungen werden die identifizierenden Merkmale einer Person, also z.B. die Namensangaben und das Geburtsdatum durch ein Pseudonym – den Code, zumeist in Form einer Buchstaben- oder Zahlenkombination – ersetzt bzw. ein Code generiert, um die Identifizierung des Betroffenen durch Personen, die nicht im Besitz der Abbildungstabelle/des Abbildungsalgorithmus (der zusätzlichen Information) sind auszuschließen. Die Bezüge verschiedener Datensätze, die auf dieselbe Art pseudonymisiert wurden, bleiben erhalten. Nutzdaten und Identifikationsmerkmale/-daten werden also getrennt aufbewahrt und können nur von Berechtigten zusammengeführt werden.

Public Cloud	Cloud-Computing-Bereitstellungmodell, bei dem die Dienste bzw. Anwendungslösungen vielen Kunden zur Verfügung stehen. Sie können zwar mit eigenen Daten arbeiten, generelle Systemeinstellungen, Lokalisierung etc. bestimmt aber der Betreiber.
Redundanz	Mehrfachauslegung von Infrastruktur-Ressourcen bzw. Mehrfachspeicherung der gleichen Daten. Bei der kontrollierten Redundanz erfolgt die Speicherung von Kopien von Daten und Dokumenten eines Anwendungssystems in einem anderen System, wobei die Synchronisation dieser Kopien bei Änderungen im Hauptsystem immer automatisch erfolgt. Die Kopie ist also immer aktuell und weicht nie vom Original ab.
Refactoring	Die Neu-Modularisierung eines Softwaresystems/Altsystems.
Regiebetrieb	Eine Organisationsform von öffentlichen Betrieben ohne eigene Rechtspersönlichkeit. Im Gegensatz zum Eigenbetrieb besitzt der Regiebetrieb keine eigenen Organe (wie eine Geschäftsführung) und wird direkt von den Organen des öffentlichen Trägers (wie dem Landrat oder dem Kreistag) gesteuert, die dort quasi die Regie führen.
Reine Privatklinik	Krankenhaus in privater Trägerschaft, das die 40%-Grenze nach § 67 AO nicht erfüllt (§ 5 Nr. 2 KHG). Danach müssen mindestens 40% der jährlichen Belegungstage oder Berechnungstage auf gesetzlich-versicherte Patienten entfallen oder auf privat-versicherte Patienten, denen kein höheres Entgelt berechnet wird.
Repository	Eine Sammlung von Informationen über „etwas“ d.h. für bestimmte Objekttypen alle bekannten/benötigten Ausprägungen. Repository ist ein allgemeiner Überbegriff. Spezialisierungen sind z.B. Daten-Diktionäre, Maßnahmenrepositories, Sammlungen von Institutionen usw.. Manchmal auch "Directory" genannt, z.B. Health Provider Directory (HPD).
Resilienz	Fähigkeit bzw. der Prozess, auf Herausforderungen und Veränderungen im Umfeld durch adäquate Verhaltensanpassungen zu reagieren. Bei Cloud-Infrastrukturen die Fähigkeit, auf Störungen und Fehlerfälle und Ausfälle von Komponenten aber auch Cyber-Angriffe "heilend" zu reagieren und die Betriebsverfügbarkeit weiter aufrecht zu erhalten.
Responsive Anwendung	Eine Anwendung, die abhängig vom genutzten Endgerät (z.B. PC, Tablet, Handy) ihr Aussehen bzw. die GUI inklusive Navigation in der Anwendung, Dialogelemente etc. automatisch anpasst. Mit einem Anwendungsprogrammcode kann so die Software also auf verschiedensten Geräten adäquat genutzt werden.

SaaS (Software as a Service)	Es wird spezielle Anwendungssoftware von einem Dienstleister angeboten und von Kunden auf der Infrastruktur dieses Anbieters auch betrieben. In der Regel nutzen alle Kunden die gleiche Software, die beim Dienstleister mandantenfähig betrieben wird.
Semantische Interoperabilität	Die Fähigkeit von zwei oder mehr Anwendungssystemen oder Komponenten davon zum Informationsaustausch sowie zur adäquaten Nutzung der ausgetauschten Information. (in Anlehnung an IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries, IEEE, 1990)
Serviceorientierte Architektur	Eine Softwarearchitektur, die auf dem Paradigma von Programmbausteinen basiert, die nur über Services zumeist über einen Enterprise Service Bus miteinander kommunizieren bzw. zusammenarbeiten.
Schichtenarchitektur	Eine Softwarearchitektur, die von mehreren gegeneinander gekapselten Schichten besteht, um die Abhängigkeiten der Funktionen der verschiedenen Schichten voneinander zu minimieren und dementsprechend Schichten austauschen zu können. Enthält zumindest eine Datenhaltungsschicht, eine Verarbeitungsschicht und eine Präsentationsschicht.
Single Point of Failure	Bestandteil eines (technischen) Systems, dessen Ausfall den Ausfall bzw. die Nichtnutzbarkeit des Gesamtsystems bewirkt. Entgegenwirken z.B. durch Mehrfachauslegung.
Skalierbarkeit	Fähigkeit eines Systems bzw. einer Infrastruktur, automatisch durch weitere Ressourcenallokationen wachsende bzw. schwankende Last mit zugesicherter Performance zu bewältigen.
Software-Architektur	Architektur eines Softwaresystems. Beschreibt die enthaltenen Anwendungsfunktionen und ihren Zusammenhang sowie die softwaretechnischen Implementierungsobjekte in Form von Programmen, Prozeduren, transienten und persistenten Klassen. Heute sind Mehrschichtarchitekturen gängig, die zumindest Datenhaltung, Datenzugriffsschicht, Verarbeitungslogik und Präsentation trennen. Cloud Native Architekturen basieren auf Microservices und haben global keine dieser klassischen Architekturschichten, sondern sind etwas anders geschichtet (hierzu siehe Kap. 4.3). Jedes Microservice-Modul kann aber ebenfalls entsprechend den vier vorangehend genannten Schichten geschichtet sein.
Softwareschicht	siehe Layer

Stammdaten	Daten eines Anwendungssystems, die nicht selbst Gegenstand der eigentlichen Verarbeitung sind, aber zur Abwicklung der lokalen oder einrichtungsübergreifenden Anwendungsfälle und Geschäftsprozesse benötigt werden. Beispiele: Krankenkassenstammdaten, Organisationsstammdaten, Rechteprofile, Abrechnungskataloge. Werden oftmals in jedem System manuell verwaltet. In Teilen Bezug aus globaleren Objektbezugsrepositories möglich.
Subsystem	Ein Anwendungssystem, das dediziert für einen betrieblichen Gegenstandsbereich betrieben wird, aber mittels semantischer Interoperabilität mit dem betrieblichen Kernsystem gekoppelt ist. Im Krankenhaus sind klassische Subsysteme das Laborinformationssystem, das Radiologieinformationssystem, das PACS, das Apothekeninformationssystem. Subsysteme werden von spezialisierten Software-Herstellern eigenständig entwickelt und lizensiert.
Terminologieserver	Ein Anwendungssystem als Infrastrukturkomponente eines heterogenen EIS, eines digitalen Ökosystems oder einer Telematikplattform, das allen Teilnehmern bzw. Teilnehmersystemen Terminologien – meist in Form kontrollierter Vokabulare – maschinenles- und verarbeitbar zur Verfügung stellt. Dadurch wird die semantische Interoperabilität in einem verteilten System unterstützt.
Übermittlung	Übertragung von personenbezogenen Daten an einen weisungsunabhängigen Empfänger. Eine Auftragsverarbeitung dann keine Übermittlung, wenn der weisungsgebundene Auftragsverarbeiter innerhalb des Europäischen Wirtschaftsraums tätig wird.
Unternehmens-informationssystem	Die Gesamtheit aller informationstechnischen Artefakte für die betrieblichen Informationsverarbeitung in einem Unternehmen. Auch Enterprise Information System EIS genannt. In manchen Definitionen werden auch die menschlichen Benutzer hinzugezählt und das EIS als Mensch-Organisation-Technik-System betrachtet.
Verantwortlicher	Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO).

Verarbeitung	Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 Nr. 2 DSGVO).
Verarbeitung besonderer Kategorien personenbezogener Daten	Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (Art. 9 Abs. 1 DSGVO).
Verfügbarkeit	Das Maß bzw. die Zusicherung für die zeitliche Verfügbarkeit eines Systems, also im Umkehrschluss für die Wahrscheinlichkeit des Ausfalls. Wird heute in Prozent angegeben, Beispiel "four 9s": 99,99 % verfügbar, d.h. maximaler Ausfall von 52,56 Minuten im Jahr bei 24/7-Betrieb.
Verschlüsselung	Die Umwandlung von Daten im Klartext unter Zuhilfenahme eines Schlüssels in ein Chiffrat, also einen Text, der keine Auskunft mehr über den ursprünglichen Inhalt gibt, aber bei Kenntnis des Schlüssels wieder zurückkonvertiert und gelesen werden kann. Dient dem Schutz und der Geheimhaltung von Daten vor Kenntnisnahme durch unbefugte Dritte.
Vertikales System/Funktion	Eine Funktion, ein System bzw. eine Anwendungssoftware, das/die speziell für einen betrieblichen Gegenstandsbereich notwendig ist und dafür realisiert wurde. So ist das Laborinformationssystem nur für das Labor nutzbar und von Interesse, das Radiologieinformationssystem nur für die Radiologie usw. In der Regel haben alle "Fachabteilungssysteme" vertikalen Charakter.
Vertraulichkeit	Eigenschaft einer Nachricht oder eines Datums, die nur einem bestimmten Personenkreis zugänglich sein darf und daher entsprechend zu schützen ist.
Viewpoint	Bezeichnet einen bzw. verschiedene Sichtweisen auf ein Informationssystem bzw. seine Zusammensetzung und Architektur. So z.B. die Sicht des Softwarearchitekten, des Programmierers, des Datenbankdesigners, des Benutzers, des Betreibers.

Virtualisierung	Abstraktionskonzept, um Kunden/Benutzern Hardware und Software zur Verfügung zu stellen ("virtuelle Maschine"), die selbst aber nicht in dieser Form materialisiert ist, sondern als Container auf der Infrastruktur des Gastsystems läuft. Dadurch einfacherer wirtschaftlicherer Betrieb, einfachere Betreuung und Skalierung vieler virtueller Maschinen und damit vieler Kunden in einem Rechenzentrum.
Webanwendung	Anwendungssoftware, die zwar nach dem Cient-Server-Prinzip funktioniert, aber keine lokale Client-Installation - außer einem Browser - erfordert. Alle Verarbeitungen erfolgen auf dem Server, die Darstellungsschicht bzw. GUI dann im "Thin Client" in der Regel in einem Browser. Es werden gängige Web-Technologien zugrunde gelegt. Es existieren auch Ansätze, Verarbeitung in den Client zu verlagern z.B. auf Basis von JAVA Script, dann sogenannte Rich Internet Applications (RIA), um das Benutzererlebnis zu verbessern und gewohnte Bedienung wie Drag&Drop etc. zu ermöglichen.
Zurechenbarkeit	Die Eigenschaft eines Datums oder einer Verarbeitung, einem Objekt - in der Regel einer Person - zugerechnet werden zu können. Dies gilt nicht nur für die Erstellung, sondern auch für Änderungen und Löschungen. Auch technische Artefakte können Daten erstellen, die dann dem entsprechenden Gerät zugerechnet werden können sollten. Beispiel: Modalitäten die DICOM-Objekte erzeugen, EKG-Geräte, die EKG-Kurven erzeugen. Zurechenbarkeit ist für die Justitiabilität von Daten unabdingbar.

10 Quellenverzeichnis

Arbeitskreise „Gesundheit und Soziales“ sowie „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2014): Orientierungshilfe Krankenhausinformationssysteme. https://www.datenschutzzentrum.de/artikel/1107-OH-KIS-Orientierungshilfe-Krankenhausinformationssysteme.html

Arbeitskreise Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Hg.) (2012): Orientierungshilfe Mandantenfähigkeit.

Armbrust, Michael et. al. (2009): Above the Clouds: A Berkeley View of Cloud Computing. Electrical Engineering and Computer Sciences University of California at Berkeley.

Auriga (Hg.): Medical Device Interoperability with Legacy Systems. Whitepaper. www.auriga.com

Bergmann, Lutz; Möhrle, Roland; Herb, Armin (2020): Datenschutzrecht, Kommentar.

Bitkom, Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien (Hg.) (2013): Wie Cloud Computing neue Geschäftsmodelle ermöglicht. https://www.bitkom.org/sites/default/files/file/import/140203-Wie-Cloud-Computing-neue-Geschaeftsmodelle-ermoeglicht.pdf

Bitkom, Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien (Hg.) (2009): Verschlüsselung von Bestandsdaten aus Rechenzentrumssicht.

Bitkom, Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien (Hg.) (2010): Cloud Computing – Was Entscheider wissen müssen. Ein ganzheitlicher Blick über die Technik hinaus Positionierung, Vertragsrecht, Datenschutz, Informationssicherheit, Compliance Leitfaden. https://www.bitkom.org/sites/default/files/file/import/BITKOM-Leitfaden-Cloud-Computing-Was-Entscheider-wissen-muessen.pdf

Bitkom, Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien (Hg.) (2015): Entwicklung erfolgreicher Webanwendungen Leitfaden Webentwicklung 2015. https://www.bitkom.org/sites/default/files/file/import/LF-Webanwendungen-150910-1.pdf

Bittner, Johannes; Haas, Peter (2017): Access granted: So lassen sich Zugriffs-Berechtigungen in Elektronischen Patientenakten flexibel und individuell regeln. https://blog.der-digitale-patient.de/zugriffsberechtigungen-elektronische-patientenakten/

Bloß, Miriam; Kühhorn, Johannes (2020): Strafrechtliche Ermittlungen gestützt auf „Corona-Gästelisten". Juristische Ausbildung 2020, S. 1036-1045.
https://www.degruyter.com/view/journals/jura/42/10/article-p1036.xml

Brynjolfsson, Erik; McAfee, Andrew; Henzler, Herbert A. (2018): The Second Machine Age. Wie die nächste digitale Revolution unser aller Leben verändern wird. Kulmbach: Plassen Verlag.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hg.) (2020): 10 Jahre KRITIS-Strategie. Einblicke in die Umsetzung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen.
www.bbk.bund.de

Bundesamt für Sicherheit in der Informationstechnik (Hg.) (2013): Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. Leitfaden.

Bundesamt für Sicherheit in der Informationstechnik (Hg.) (2014): IT-Grundschutz-Kataloge. 14. Ergänzungslieferung-2014.
www.bsi.de

Bundesamt für Sicherheit in der Informationstechnik (Hg.) (2018): Informationssicherheitsrevision. Ein Leitfaden für die IS-Revision auf Basis von IT- Grundschutz Version 3.0.

Bundesamt für Sicherheit in der Informationstechnik (Hg.) (2020): Kriterienkatalog Cloud Computing C5:2020.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf?__blob=publicationFile&v=2

Bundesministerium für Gesundheit; Bundesamt für Soziale Sicherung (2020): Richtlinie zur Förderung von Vorhaben zur Digitalisierung der Prozesse und Strukturen im Verlauf eines Krankenhausaufenthaltes von Patientinnen und Patienten.
https://www.bundesamtsozialesicherung.de/de/themen/foerdermittelrichtlinie/

Bundesministerium für Wirtschaft und Energie (BMWi) (Hg.) (2016): Cloud-Standards und Zertifizierungen im Überblick – Was Cloud-spezifisch betrachtet werden sollte. Version 1.0. 18. Februar 2016.
https://www.trusted-cloud.de/sites/default/files/beitrag-cloud-standards_und_zertifizierungen_im_ueberblick.pdf

Bundesministerium für Wirtschaft und Energie (BMWi) (Hg.) (2018): Orientierungshilfe zum Gesundheitsdatenschutz. November 2018.
https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/orientierungshilfe-gesundheitsdatenschutz.pdf?__blob=publicationFile&v=19

Busch, Dieter; Haas, Peter; Swoboda, Jessica (2017): Weboptimiertes IT-gestütztes Medikationsmanagement (IT-MM) als Teil einer einrichtungsübergreifenden elektronischen Patientenakte. Dortmund: Eigenverlag FH Dortmund (Schriftenreihe des Fachbereichs Informatik der Fachhochschule Dortmund, 3), S. 87–103.

CHIME (2020): Digital Health most wired Survey. https://chimecentral.org/chime-most-wired-2/

Cierniak, Jürgen; Niehaus, Holger, in: Joecks, Wolfgang; Miebach, Klaus (Hg.) (2017): Münchener Kommentar zum StGB, 3. Auflage.

CNIL (2020): The Council of State asks the Health Data Hub for additional guarantees to limit the risk of transfer to the United States. https://www.cnil.fr/en/council-state-asks-health-data-hub-additional-guarantees-limit-risk-transfer-united-states

Cornelius, Kai: Das Non-Legal-Outsourcing für Berufsgeheimnisträger, NJW 2017, S. 3751-3755.

Coulouris, George F.; Dollimore, Jean; Kindberg, Tim (2002): Verteilte Systeme. Konzepte und Design. 3., überarb. Aufl. München: Pearson Studium (Informatik).

Datenschutzkonferenz (2014): Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern. https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/AnlageDSKKrebsregisterNovember2014.pdf?__blob=publicationFile&v=3

Deutsche Krankenhaus Gesellschaft (2019): Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus. https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/B3S_KH_v1.1_8a_geprueft.pdf

Datenschutzkonferenz, Arbeitskreise Gesundheit sowie Technische und organisatoirsche Datenschutzfragen (2014): OH KIS – Orientierungshilfe Krankenhausinformationssysteme. 2. Fassung, Stand März 2014. https://www.datenschutzzentrum.de/artikel/1107-OH-KIS-Orientierungshilfe-Krankenhausinformationssysteme.html

Datenschutzkonferenz (2018): Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO. https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf

Dierks, Christian (unter Mitarbeit von P. Kircher, C. Husemann, K. Engelke, J. Pirk, M. Haase) (2019): Lösungsvorschläge für ein neues Gesundheitsforschungsdatenschutzrecht in Bund und Ländern, Rechtsgutachten für das Bundesministerium der Gesundheit. https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Gesundheit/Berichte/RECHTSGUTACHTEN_Gesundheitsforschungsdatenschutzrecht_BMG.pdf

Doelfs, Guntram (2020): Revolution: Wohin steuert der KIS-Markt in Deutschland?. https://www.kma-online.de/aktuelles/it-digital-health/detail/wohin-steuert-der-kis-markt-in-deutschland-a-43433

Duan, Yucong et al. (2015): Various 'aaS' of Everything as a Service. https://www.researchgate.net/publication/285236871_Various_%27aaS%27_of_everything_as_a_service

Dürbeck, Stefan; Kolter, Jan; Pernul, Günther; Schillinger, Rolf (2011): Eine verteilte Autorisierungsinfrastruktur unter Berücksichtigung von Datenschutzaspekten. In: Informatik Spektrum 34 (3), S. 265–275. DOI: 10.1007/s00287-009-0411-0.

Eisele, Jörg, in: Schönke, Adolf; Schröder (2018), Horst: Strafgesetzbuch Kommentar, 30. Auflage.

Europäischer Datenschutzausschuss (2018): Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679. https://www.datenschutzkonferenz-online.de/media/dsgvo/edpb_guidelines_2_2018_derogations_de.pdf

Europäischer Datenschutzausschuss (2020): Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

Evans, Eric (2004): Domain-driven design. Tackling complexity in the heart of software. Boston, San Francisco, New York, Toronto, Montreal, London, Munich, Paris, Madrid, Capetown, Sydney, Tokyo, Singapore, Mexico City: Addison-Wesley.

Extreme Networks (2020): Welcome to 2020! Survey says: Healthcare is Ready for Cloud Networking. https://www.extremenetworks.com/resources/infographic/welcome-to-2020-survey-says-healthcare-is-ready-for-cloud-networking/

Fischer, Thomas (2020): Strafgesetzbuch, Kommentar, 67. Auflage.

Gabriel, Roland: Definition Informationssystem, in: Enzyklopädie der Wirtschaftsinformatik Online Lexikon.
https://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/uebergreifendes/Kontext-und-Grundlagen/Informationssystem/index.html.

Garett, Peter; Seidmann, Joshua (2011): EMR vs EHR – What is the Difference?.
https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference

Gilbert, John (2018): Cloud native development patterns and best practices. Practical architectural patterns for building modern, distributed cloud-native systems. Birmingham, UK: Packt Publishing.
http://proquest.tech.safaribooksonline.de/9781788473927

Glaser, John P.; Lo, Helen G. (2006): Concepts for Building Inter-Organizational Systems in Healthcare: Lessons from Other Industries. In: Journal of healthcare information management 20 (3), S. 54–62.

GMDS e.V. (Hg.) (2014): Stellungnahme und Kommentierung der „Orientierungshilfe Krankenhausinformationssysteme".
https://www.gmds.de/de/aktivitaeten/medizinische-informatik/arbeitsgruppenseiten/datenschutz-und-it-sicherheit-im-gesundheitswesen-dig/stellungnahmen/

Gravic Inc. (Hg.) (2020): Choosing a Business Continuity Solution to Match Your Business Availability Requirements. White paper.
https://www.shadowbasesoftware.com/publications/white-papers/

Gühr, Alisha; Karper, Irene; Maseberg, Sönke (2020): Der lange Weg zur Akkreditierung nach Art. 42 DSGVO. Datenschutz- und Datensicherheit (DuD) 2020; S. 649-653.
https://www.datenschutz-notizen.de/wp-content/uploads/2020/09/Der_lange_Weg_zur_Akkreditierung_Art42DSGVO_DuD_10_2020.pdf

Haas, Peter (2005): Medizinische Informationssysteme und elektronische Krankenakten. Berlin: Springer.

Haas, Peter (2013): Informatische Artefakte für eine Gesundheitstelematikplattform. In: Chr. F.-J. Goetz und A. Grode (Hg.): Thesenpapier zur Gesundheitstelematik. Ziele, Strategien und Impulse wichtiger Stakeholder für eine funktionelle Gesundheitstelematik in Deutschland. Berlin, S. 78–84.

Haas, Peter (2013): Repositories als unabdingbare Infrastrukturelemente für telematische und telemedizinische Anwendungsszenarien. In: Peter Haas, Sebastian C. Semler, Stephan H. Schug und Johannes Schenkel (Hg.): Nutzung, Nutzer, Nutzen von Telematik in der Gesundheitsversorgung – eine Standortbestimmung. Tagungsband der TELEMED 2013 am 3. und 4. Juli 2013 in Berlin. 1. Auflage. Berlin: Akademische Verlagsgesellschaft AKA (TELEMED - Nationales Forum für Gesundheitstelematik und Telemedizin - Jahresbericht), S. 27–34.

Haas, Peter (2016): Wissensmanagement in der Medizin. In: Forum 31 (1), S. 28–32. DOI: 10.1007/s12312-015-0012-6.

Haas, Peter (2017): Elektronische Patientenakten. Einrichtungsübergreifende Elektronische Patientenakten als Basis für integrierte patientenzentrierte Behandlungsmanagement-Plattformen. Gütersloh: Bertelsmann Stiftung Eigenverlag.

Haas, Peter (2019): eLearningeinheit „Einführung in die semantische Interoperabilität (1)". https://www.ehealth-elearning.de/ilias.php?baseClass=ilSAHSPresentation-GUI&ref_id=1208

Haas, Peter; Kuhn, Klaus A. (2017): Krankenhausinformationssysteme: Ziele, Nutzen, Topologie, Auswahl. In: Rüdiger Kramme (Hg.): Informationsmanagement und Kommunikation in der Medizin. Berlin: Springer, 21 ff.

Haas, Peter; Semler, Sebastian C.; Schug, Stephan H.; Schenkel, Johannes (Hg.) (2013): Nutzung, Nutzer, Nutzen von Telematik in der Gesundheitsversorgung – eine Standortbestimmung. Tagungsband der TELEMED 2013 am 3. und 4. Juli 2013 in Berlin. 1. Auflage. Berlin: Akademische Verlagsgesellschaft AKA (TELEMED - Nationales Forum für Gesundheitstelematik und Telemedizin - Jahresbericht).

Haesen, Raf; Snoeck, Monique; Lemahieu, Wilfried; Poelmans, Stephan (2008): On the Definition of Service Granularity and its Architectural Impact. https://www.researchgate.net/publication/46430123

Hellmich, Stefanie; Hoffmann, Laura (2020): EU-Empfehlungen nach 'Schrems II', Wie lässt sich der internationale Daten-transfer retten?; Legal Tribune Online, 07.12.2020. https://www.lto.de/recht/hintergruende/h/eugh-eu-schrems-ii-internationaler-daten-transfer-scc-standardvertragsklauseln/

Hentschel, Raoul; Leyh, Christian: Cloud Computing: Status quo, aktuelle Entwicklungen und Herausforderungen, S. 3–20.

HIMSS: EMRAM: A strategic roadmap for effective EMR adoption and maturity. https://www.himssanalytics.org/emram

HL7 International (Hg.) (2014): HL7 EHR-System Functional Model Release 2. https://www.hl7.org/implement/standards/product_brief.cfm?product_id=269

HL7 International (Hg.) (2019): HL7 Service-Aware Interoperability Framework: Canonical Definition Specification, Release 2.
http://www.hl7.org/implement/standards/product_brief.cfm?product_id=3

HL7: Digitale Standards im Gesundheitswesen.
https://hl7.de/

Hübner, Ursula; Esdar, Moritz; Hüsers, Jens; Liebe, Jan-David; Rauch, Jens; Thye, Johannes; Weiß, Jan-Patrick (2018): IT-Report Gesundheitswesen. Schwerpunkt Wie reif ist die IT in deutschen Krankenhäusern? Osnabrück: Eigenverlag (IT-Report Gesundheitswesen).

Hullen, Nils; Krohm, Niclas, in: Plath, Kai-Uwe (Hg.) (2018): DSGVO, BDSG, Kommentar, 3. Auflage.

IDG Research Services (Hg.) (2020): Studie Cloud Native 2020.
https://www2.deloitte.com/content/dam/Deloitte/de/Documents/industry-operations/CloudNative_IDG-Studie_Deloitte_2020.pdf

IEEE (1990): A Compilation of IEEE Standard Computer Glossaries New York.
https://www.worldcat.org/title/ieee-standard-computer-dictionary-a-compilation-of-ieee-standard-computer-glossaries-610/oclc/2421754

IHE International (Hg.) (2020): IHE IT Infrastructure (ITI) Volume 1 (ITI TF-1) Integration Profiles.

International Standards Organisation (2014): ISO/IEC 17789 Information technology -Cloud computing - Reference architecture. Geneva.

International Standards Organisation (Hg.) (2015): ISO/IEC 17788 Information technology — Cloud computing — Overview and vocabulary.

International Standards Organisation (Hg.) (2019): ISO 22301 Security and resilience - Business continuity management systems - Requirements.

Ionos (2020): Bare-Metal-Server – dedizierte Hardware für anspruchsvolle Webprojekte.
https://www.ionos.de/digitalguide/server/knowhow/bare-metal-server-definition-und-aufbau/

Jones, Edward (2020): Arten von Cloud Computing – ein umfangreicher Leitfaden zu Cloud-Lösungen und -Technologien im Jahr 2020.
https://kinsta.com/de/blog/arten-von-cloud-computing/

Kalloniatis, Christos; mouratidis, Haralambos; Vassilis, Manousakis; Islam, Shareeful; Gritzalis, Stefanos; Kavakli, Evangelia (2014): Towards the design of secure and privacy-oriented Information Systems in the Cloud: Identifying the major concepts.

Karlstetter, Florian (2018): Was sind Hyperscaler?. https://www.cloudcomputing-insider.de/was-sind-hyperscaler-a-743368/

Kassenärztliche Bundesvereinigung (Hg.) (2019): Spezifikation für einen bundeseinheitlichen Medikationsplan (BMP) gemäß § 31a SGB V. https://www.kbv.de/media/sp/Medikationsplan_Anlage3.pdf

Kircher, Philipp (2016): Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen. Nomos.

Klauber, Jürgen; Geraedts, Max; Friedrich, Jörg; Wasem, Jürgen (2019): Krankenhaus-Report 2019. Das digitale Krankenhaus: Springer Open.

Kramme, Rüdiger (2017): Informationsmanagement und Kommunikation in der Medizin. Berlin, Heidelberg: Springer Berlin Heidelberg.

Kuhlemann, Martin (2006.): Moderne Modularisierungstechniken und ihre Bedeutung für qualitativ hochwertige Software. Diplomarbeit an der Fakultät für Informatik Institut für Technische und Betriebliche Informationssysteme der Universität Magdeburg.

Liu, Fang; Tong, Jin; Mao, Jian; Bohn, Robert; Messina, John; Badger, Lee; Leaf, Dawn (2011): NIST Cloud Computing Reference Architecture. Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology U.S. Department of Commerce. Gaithersburg.

Mau, Jens (2016): KIS-Hersteller Cerner: Der US-Gigant und die German Angst. https://www.kma-online.de/aktuelles/it-technik/detail/der-us-gigant-und-die-german-angst-a-30967

Mau, Jens (2018): Nervöser KIS-Markt: Spannung um mögliche Konsolidierung des Marktes steigt. https://www.kma-online.de/aktuelles/it-digital-health/detail/spannung-um-moegliche-konsolidierung-des-marktes-steigt-a-37293

Mell, Peter; Grance, Timothy (2011): The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. Hg. v. NIST. National Institute of Standards and Technology U.S. Department of Commerce. Gaithersburg. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Melzer, Ingo (2010): Service-orientierte Architekturen mit Web Services. Konzepte - Standards - Praxis. 4. Aufl. Heidelberg, Neckar: Spektrum Akademischer Verlag.

Meyer, Wilfried; Hein, Franziska (2016): Business Continuity Management. Hg. v. pwc.

Mützner, Robert (2020): Anforderungen und Lösungsansätze für wissensbasierte kontext-sensitiv-reaktive medizinische Informationssysteme. I n a u g u r a l - D i s s e r t a t i o n zur Erlangung des Doktorgrades der Naturwissenschaften in der Medizin (rer. medic.) durch die Medizinische Fakultät der Universität Duisburg-Essen.

Mützner, Robert; Haas, Peter (2015): Health Provider Directory - eine standardkonforme Trial Implementierung. Tagungsbandeinreichung. Berlin.

Niedernhuber, Tanja (2020): Die Verwendung von Corona-Gästelisten zur Strafverfolgung. https://kripoz.de/2020/11/26/die-verwendung-von-corona-gaestelisten-zur-strafverfolgung.pdf

Palandt (Begründer) (2021): Bürgerliches Gesetzbuch; Beck'scher Kurz-Kommentar, 80. Auflage 2021.

Parnas, David Lorge (1972): On the criteria to be used in decomposing systems into modules. In: Commun. ACM 15 (12), S. 1053–1058.

Piltz, Carlo (2020): Schrems II: US CLOUD Act kein Problem? Zumindest nach Ansicht der Landesregierung NRW. Stand: 26.10.2020. https://www.delegedata.de/2020/10/schrems-ii-us-cloud-act-kein-problem-zumindest-nach-ansicht-der-landesregierung-nrw/

Reinheimer, Stefan (Hg.) (2018): Cloud Computing. Die Infrastruktur der Digitalisierung. Wiesbaden: Springer Vieweg (Edition HMD). http://dx.doi.org/10.1007/978-3-658-20967-4

Reng, Carl-Michael; Debold, P.; Specker, Ch.; Pommerening, Klaus (2006): Generische Lösungen der TMF zum Datenschutz für die Forschungsnetze in der Medizin. Berlin: Med. Wiss. Verl.-Ges (Schriftenreihe der Telematikplattform für Medizinische Forschungsnetze, [Bd. 1]).

Rost, Cristina; Brink, Stefan; Birk, Tobias (2020): Cloud Computing und Datenschutz; Recht der Datenverarbeitung 2020: S. 240-245.

Schaaf, Michael; Stäubert, Sebastian; Winter, Alfred (7): The 3LGM2-tool to support information management in health care. In: GMS Medizinische Informatik Biometrie Epidemiologie 2011 (2). https://www.researchgate.net/publication/268510623

Schäfer, Gutzeit: Der Weg zu einer Cloud-nativen Architektur. 2017. https://m.heise.de/developer/artikel/Der-Weg-zu-einer-Cloud-nativen-Architektur-4588019.html?seite=all

Scheer, August-Wilhelm (1995): Wirtschaftsinformatik. Referenzmodelle für industrielle Geschäftsprozesse. Studienausg. Berlin, Heidelberg, New York, Barcelona, Budapest, Hongkong, London, Mailand, Paris, Santa Clara, Singapur, Tokio: Springer.

Schmidt, Georg; Seiler, Christoph; Maier, Petra; Vollmöller, Thomas (2004): Praxis der Kommunalverwaltung – Das Krankenhausrecht in Thüringen.

Schneider, Berthold; Schönenberger, Rolf (Hg.) (1976): Datenverarbeitung im Gesundheitswesen. Erreichtes und Geplantes. Berlin, Heidelberg: Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-642-66480-9

Schneider, Uwe K. (2014): Einrichtungsübergreifende elektronische Patientenakten – Zwischen Datenschutz und Gesundheitsschutz.

Schneider, Uwe K. (unter Mitarbeit von M. Klar und J. Bernhardt) (2015): Sekundärnutzung klinischer Daten – Rechtliche Rahmenbedingungen. https://mwv-open.de/site/books/10.32745/9783954663224/download/3141/

Schneider, Uwe K., in: Krauskopf, Dieter (Begr.) (2019): Soziale Krankenversicherung, Pflegeversicherung, SGB V, § 295, Kommentar.

Schneider, Uwe K., in: VSSR 5/2009: Abrechnungsstellen und Datenschutz in der GKV – Das Urteil des BSG vom 10.12.2008 und die Folgeänderungen im Rahmen der 15. AMG-Novelle.

Schwanke-Seer, Michael; Helling, Andreas (2020): Cloud Networking im Gesundheitswesen. https://www.krankenhaus-it.de/modules/publisher/index.php/item.403/cloud%20networking%20im%20gesundheitswesen.html

Seliger, Robert; Fusari, David; Rusell, Michael; Seegmüller, Kevin; Staggs, David (2016): HL7 Context Management Specification Version 1.6. Technology- and Subject-Independent Component Architecture. Hg. v. HL7 International (HL7 Context Management Specification Version 1.6).

Spitta, Thorsten; Bick, Markus (2008): Informationswirtschaft. Berlin, Heidelberg: Springer Berlin Heidelberg.

Streitberger, Erner; Ruppel, Angelika (2009): Cloud Computing. Schutzziele. Taxonomie. Marktübersicht. Hg. v. Fraunhofer AISC. München. https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/deutsch/studie-CloudComputingSicherheit.pdf

Tanck Hajo, Heinlein Michael (2011): Fusion von Medizintechnik und Informationstechnologie Struktur, Integration und Prozessoptimierung. In: Rüdiger Kramme (Hg.): Medizintechnik. Verfahren - Systeme – Informationsverarbeitung. Berlin: Springer, 2011, S. 763–770.

Vernon, Vaughn (2017): Domain-Driven Design kompakt. 1. Auflage. Heidelberg: dpunkt.verlag.

Weidemann, Matthias, in: Heintschel-Heinegg, Bernd von (Hg.) (2020): Beck'scher Online-Kommentar (BeckOK) StGB, 48. Edition.

Wels-Maug, Cornelia (2020): Cloud-Nutzung im Krankenhaus. https://www.healthcareitnews.de/cloud-nutzung-im-krankenhaus

Winter, Alfred (7): The 3LGM2-tool to support information management in health care. In: GMS GMS Med Inform Biom Epidemiol 2011 (2), S. 1–7. https://www.researchgate.net/publication/224703041_The_3LGM2-Tool_to_Support_Information_Management_in_Health_Care

Würtenberger, Thomas; Altschwager, Martin, in: Dettling, Heinz-Uwe; Gerlach, Alice (Hg.) (2018): Krankenhausrecht, Kommentar, 2. Auflage 2018.

ZVEI (Hg.) (2017): Whitepaper Integrität von Daten, Systemen und Prozessen als Kernelement der Digitalisierung. ZVEI.